EX 1002

PTO/SB/05 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	ROCK1150-3
First Inventor	Patrick Turley
Title	Dynamically Adaptive Network ...
Express Mail Label No.	N/A

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☑ **Fee Transmittal Form** (e.g., PTO/SB/17)
   (Submit an original and a duplicate for fee processing)
2. ☑ **Applicant claims small entity status.** See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages* 25]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☑ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 3]
5. **Oath or Declaration** [*Total Sheets* 2]
   a. ☐ Newly executed (original or copy)
   b. ☑ A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO:
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers** (cover sheet & document(s))
   Name of Assignee_____
10. ☐ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☑ **Power of Attorney**
11. ☐ **English Translation Document** *(if applicable)*
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (Should be specifically itemized)
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☑ Other: Cert. of Transmission

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☑ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: 12/579,566

Prior application information: *Examiner* Dinh, Minh *Art Unit:* _____

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 44654 ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	Katharina Schuster	Date	April 22, 2011
Name (Print/Type)	KATHARINA W. SCHUSTER	Registration No. (Attorney/Agent)	50,000

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of, and claims a benefit of priority under 35 U.S.C. 120 of the filing date of U.S. Patent Application No. 12/579,566, filed October 15, 2009, now allowed, entitled “DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME,” which claims priority from U.S. Patent Application No. 11/076,719, filed March 10, 2005, issued as U.S. Patent No. 7,610,621, entitled “SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING,” which claims priority from Provisional Application No. 60/551,698, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING." This application also relates to U.S. Patent Application No. 10/683,317, filed October 10, 2003, pending, entitled "SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL," and Provisional Application No. 60/551,703, entitled "SYSTEM AND METHOD FOR PROVIDING A CENTRALIZED DESCRIPTION/ CONFIGURATION OF CLIENT DEVICES ON A NETWORK ACCESS GATEWAY," filed March 10, 2004. All applications referenced herein are hereby fully incorporated by reference.

TECHNICAL FIELD

[0002] Embodiments disclosed herein relate generally to network firewall designs and methodologies and more specifically to network firewalls that can dynamically adapt to changing conditions and operator requirements.

BACKGROUND

[0003] The communication of data over networks has become an important, if not essential, way for many organizations and individuals to communicate. The Internet is a global network connecting millions of computers using a client-server architecture in which any computer connected to the Internet can potentially receive data from and send data to any other computer connected to the Internet. The Internet provides a variety of methods in which to communicate data, one of the most ubiquitous of which is the World Wide

Web. Other methods for communicating data over the Internet include e-mail, usenet newsgroups, telnet and FTP.

[0004] Users typically access the Internet either through a computer connected to an Internet Service Provider ("ISP") or computer connected to a local area network ("LAN") provided by an organization, which is in turn connected to an ISP. The network service provider provides a point of presence to interface with the Internet backbone. Routers and switches in the backbone direct data traffic between the various ISPs.

[0005] As the number of networked devices has increased, so too has the amount and nature of network traffic. One unfortunate side effect is the evolution of destructive or unauthorized access to the data or operations of networked devices. As a result, technological advances have produced a general class of network service known as a "firewall", which can block or limit access to computers, networks and services "inside" the firewall, from access by any network devices "outside" the firewall. Representation of "inside" and "outside" a firewall is analogous to physical security and protection, where something "inside" is protected from something "outside". Hence, firewall technology and services normally have one network interface connected to the general internet or an unprotected segment of any network and the protected computer and network assets are located behind another network interface controlled by the firewall that is a different, protected network segment.

[0006] Typically, network firewalls are configured in a static manner, wherein the firewall's configuration is established and changes infrequently.

[0007] Firewalls are potentially complicated structures that are generally maintained manually by a skilled professional. Firewall owners must therefore limit themselves to simple and inflexible features provided by typical network applications/devices, or they must invest in professionals who are skilled enough to construct and maintain firewalls to their specifications. In other words, the skilled firewall professional provides the intelligence, decision-making and flexibility that is lacking in static firewall technology.

[0008] Previous firewall implementations are typically limited in two ways: (1) they are embedded in an inflexible hardware platform with no ability to expand and/or (2) they offer only a very simple set of user-visible features both because they have no expandability and because they lack the conceptual model to express more advanced

features in a way that is convenient for customers to use. These solutions are inadequate because they limit the power of the features available to customers.

[0009] While statically configured firewalls serve a purpose for protecting static network and computing assets, the ability to dynamically reconfigure firewalls in a changing network environment represents a significant evolutionary step in network firewall technology. Dynamic firewalls can monitor transient network client connections and adjust themselves to optimally serve and protect a dynamically changing network client population on both "sides" of a firewall.

SUMMARY

[0010] Embodiments disclosed herein expose a conceptual model of firewall structure that makes it far easier to construct an automated system to bridge the gap between the desires of users and the technical implementation of those desires.

[0011] One embodiment of the automated system provides a new level of flexibility including, but not limited to, dynamically adding new network interface abstractions or groupings of interface abstractions and tailoring the behavior of those abstractions to the network client devices' specific needs. The automated system enables the firewall owner to generally describe how the firewall should behave, and the automated system can automatically produce the requisite, specific firewall configuration, without detailed manipulation by a human operator.

[0012] One embodiment models sources and destinations of network traffic (e.g., client, Virtual Private Network, and Wide Area Network-side devices) as "nodes" that exhibit particular sets of behaviors. Network interface devices (including virtual devices) can then be associated with one of the nodes and assigned the same behaviors/rules as all other devices in that particular node. In this way, the data flows between devices can be monitored and controlled according to the behaviors and rules of each device.

[0013] Another embodiment extends the aforementioned behavior description and configuration to modeling the connections between nodes and not just the devices (virtual or physical) of a particular node. That is to say, not only do the devices belonging to a node can exhibit particular behaviors, but the connections between each node can also exhibit particular behaviors.

[0014] Another embodiment defines a conceptual framework of the firewall and elucidates the flow of traffic through the gateway and provides a level of abstraction that can be understood and manipulated by human operators to tailor the system's behaviors to their needs.

[0015] Another embodiment enables the firewall to react dynamically to important changes such as, but not limited to, the addition or removal of physical or virtual network interfaces. This can be especially important for certain applications because the embodiment permits the deployment of unsophisticated, general implementation technologies (i.e., off-the-shelf hardware) and does not require a custom hardware platform.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] A more complete understanding of the invention and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings in which like reference indicates like features and wherein:

[0017] FIG. 1 illustrates a set of nodes for a firewall model;

[0018] FIG. 2 illustrates a set of firewall rules; and

[0019] FIG. 3 illustrates aspects of behaviors applied to packet traversal through the firewall model.

DETAILED DESCRIPTION

[0020] The following applications are hereby fully incorporated by reference herein in their entirety: United States Application No. 10/683,317, filed October 10, 2003, pending, entitled “SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL”; Provisional Application No. 60/551,698, filed March 10, 2004, entitled “SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING”; Provisional Application No. 60/551,754, filed March 10, 2004, entitled “SYSTEM AND METHOD FOR COMPREHENSIVE CODE GENERATION FOR SYSTEM MANAGEMENT,” which converted into United States Application No. 11/078,223, filed March 10, 2005, entitled “SYSTEM AND METHOD FOR COMPREHENSIVE CODE GENERATION FOR SYSTEM MANAGEMENT,” issued as U.S. Patent No. 7,509,625; Provisional Application No. 60/551,703, filed March 10, 2004 entitled “SYSTEM AND METHOD FOR PROVIDING A CENTRALIZED DESCRIPTION/CONFIGURATION OF CLIENT

DEVICES ON A NETWORK ACCESS GATEWAY"; Provisional Application No. 60/551,702, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR ACCESS SCOPE CONTROL ("WALLED GARDENS") FOR CLIENTS OF A NETWORK ACCESS GATEWAY," which converted into United States Application No. 11/076,591, filed March 10, 2005, pending, entitled "METHOD AND SYSTEM FOR CONTROLLING NETWORK ACCESS"; Provisional Application No. 60/551,699, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR DYNAMIC BANDWIDTH CONTROL"; Provisional Application No. 60/551,697, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR DETECTION OF ABERRANT NETWORK BEHAVIOR BY CLIENTS OF A NETWORK ACCESS GATEWAY," which converted into United States Application No. 11/076,652, filed March 10, 2005, issued as U.S. Patent No. 7,590,728, entitled "SYSTEM AND METHOD FOR DETECTION OF ABERRANT NETWORK BEHAVIOR BY CLIENTS OF A NETWORK ACCESS GATEWAY"; Provisional Application No. 60/551,705, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR DOUBLE-CAPTURE/DOUBLE-REDIRECT TO A DIFFERENT LOCATION," which converted into United States Application No. 11/076,646, filed March 10, 2005, issued as U.S. Patent No. 7,665,130, entitled "SYSTEM AND METHOD FOR DOUBLE-CAPTURE/DOUBLE-REDIRECT TO A DIFFERENT LOCATION"; Provisional Application No. 60/551,704, filed March 10, 2004, entitled "SYSTEM AND METHOD FOR NETWORK MANAGEMENT XML ARCHITECTURAL ABSTRACTION," which converted into United States Application No. 11/076,672, filed March 10, 2005, abandoned, entitled "SYSTEM AND METHOD FOR NETWORK MANAGEMENT XML ARCHITECTURAL ABSTRACTION"; and Provisional Application No. 60/551,703, filed March 10, 2005, entitled "SYSTEM AND METHOD FOR PROVIDING A CENTRALIZED DESCRIPTION/ CONFIGURATION OF CLIENT DEVICES ON A NETWORK ACCESS GATEWORK."

[0021] The invention considers the firewall as implemented within a device, service or server at the nexus of two network segments but, at a conceptual level, it appears more like any other network traffic origination or destination device; i.e., while the functional aspects of a firewall may differentiate itself from other network infrastructure devices or services, at a conceptual level it inspects, marks, prioritizes and routes traffic similar to other network packet handling service.

[0022] Embodiments disclosed herein seek to abstract the diverse set of network and firewall operations into a generalization of activities amongst "nodes" in the firewall model. With

a basic conceptual model, all firewall behavior can be characterized as high-level operations on network traffic flowing through the firewall.

[0023] The firewall is the nexus in a fully-interconnected graph (FIG. 1) with four nodes. Each node in FIG. 1 is simultaneously a source of and destination for network packets. Packets travel between nodes over intra-firewall connections within the firewall model. Implementations of intra-firewall connections can be software, in-memory implementations or can be hardware, signaling implementations. A non-limiting example of a software, in-memory implementation can be realized through a computer program product comprising a computer readable storage medium storing computer program code executable by a computer. As one of ordinary skill in the art can appreciate, a computer memory is a non-limiting example of a computer readable storage medium.

[0024] There are three essential stages to a packet's journey through the firewall model:

- Arriving, node-specific behaviors. Where network traffic is inspected upon arrival at a node in the firewall model and the model acts upon this traffic, based on its configuration at the time of the traffic arrival and the processing node's capabilities.
- Connection-specific behaviors. Some behaviors are contextually important when considered as part of a connection between two nodes in the firewall model. When network traffic flows over the connection it can be inspected and handled at one or both of the node endpoints of the connection.
- Departing, node-specific behaviors. Where network traffic is inspected prior to departure from a node and the firewall acts upon this traffic, based on its configuration at the time of the traffic departure and the processing node's capabilities.

[0025] Embodiments disclosed herein can employ existing operating system mechanisms to implement the concepts. For example, the Linux operating system has a subsystem known as "iptables" (for Internet Protocol Tables) that offers a "rule" syntax for representing the logic of packet handling through the Linux system.

[0026] As illustrated in FIG. 2, and described below, the firewall employs dynamic chains of rules (serialized sequences of one or more rules) to "tap" into the main firewall chains and offer isolated, well-defined places for specific behavior to be introduced. One reason for functional extensions is to enrich the firewall rule predicate or antecedent

functionality to provide more functionality as domain-specific applications require or as general network technology evolves.

[0027] To dynamically integrate devices or interfaces, the firewall defines the following objects:

- Device--Represents a source or sink of network traffic. In the firewall conceptual framework, a "device" can be mapped to a physical device or network interface, or it can be mapped to a virtual device; e.g., a virtual private network (VPN) is an abstraction of routes, keys and permissions that represent a virtual network segment, the firewall can manipulate the facets of a VPN through a VPN device in the firewall abstraction nomenclature. Devices always belong to nodes when they are active.
- Chain--Represents a list of one or more firewall rules. A firewall rule has the normal predicate/antecedent format, where elements of the predicate must match before the actions of the antecedent are enacted. Chains of firewall rules are linear and serial, as the name implies.
- Node--Could be any one of the nodes represented in FIG. 1. A Node can have any number of Services or Devices.
- Service--Represents a node-specific or connection-specific behavior. A service may be a collection of atomic behaviors that are cohesive in their functionality and represent a larger piece of utility to the system. Any node or connection may have one or more services.

[0028] When a new device is introduced to the firewall system, a new Device object is created and placed in the Null node, which has no services (behaviors) and is not connected to any other node. The new device is then moved to the Node to which it belongs. A Device can be moved from one node to another. The process of "moving" a device from one node to another deletes existing behaviors and states and associates new ones.

[0029] When a device is deleted from the system, its Device object is moved to the Null node and then left to die (e.g., at object cleanup). In one implementation, a Java Virtual Machine provides garbage collection for null-ed firewall objects.

[0030] Connections between nodes, as represented in FIG. 1, are also created dynamically and can migrate or redefine their endpoints as the firewall system deems necessary.

[0031] One of the strengths of the firewall is its careful identification and segmentation of traffic flows. Each such flow is represented by the concept of a connection between nodes. Just as nodes have behaviors, so do connections. Some of the transformations applied to a packet depend entirely on the node through which the packet arrives or departs. Additional transformations can be associated with the connection through which the packet travels, without regard to the nodes between which the packet is traveling. FIG. 3 illustrates the salient aspects of behaviors applied to packet traversal through the firewall model. Thus, in a generic and customizable way, basic facilities can be adjusted by tailoring the specific behaviors of the various connections.

[0032] One important example of this is the connection between the Clients node and the WAN node. Packets that bear the mark of a client that is authorized to use the WAN connection are permitted to flow along this connection and arrive at the WAN node. Packets from clients that don't have this authorization are blocked. Network communications port blocking is typically a Client-specific behavior; i.e., in this embodiment's conceptual model, port blocking is germane only to network client device traffic and, hence, network port blocking is only considered when network client traffic is considered (i.e., traffic from the client node).

[0033] Network port forwarding is specific to the connection from the WAN node to the Clients node. In other words, packet processing is performed based on rules associated with the connection rather than the nodes. The nature of network port forwarding is that "outside" traffic--meaning, network traffic originating on the outside of the firewall, from the Wide-Area Network--will be addressed to a particular port as received by the firewall, whereupon the firewall will pass that network traffic, but may change the port as seen by the packet destination device.

[0034] Network Address Translation (NAT), is a WAN-specific behavior. NATed network packets have source and/or destination addresses translated to/from an internal network address that is not publicly available on the general network (or Internet). NATing is a mechanism for employing a single, public Internet Protocol Address (IPADDR) to represent a number of client devices behind a NATing service. NATed packets present a slightly different form of forwarding problem for firewalls, but it is akin to port forwarding or port translation, as the firewall must maintain a state table to keep track of NATed addresses or translated ports.

[0035] Every packet that arrives at the firewall receives a 32-bit mark (or other mark depending on implementation) that identifies how that packet is attributed. This is fundamental to accounting and authorization models, where network client traffic must be tracked. The firewall uses marks to, among other things, decide if packets are permitted to reach their destinations.

[0036] FIG. 2 illustrates the experience of a network packet as it travels through the firewall from its arriving node to its departing node. FIG. 2B is an extension of the tree graph of FIG. 2A as indicated. The path the tree graph takes is a depth-first, in-order traversal of the tree depicted in FIG. 2. In FIG. 2, the node (clients) corresponds to the defined nod LAN in FIG. 1.

[0037] To help reflect the structure of the firewall, rule chains are given names in a hierarchical name space. Immediately below the root are subtrees with names "A", "M", "D" and "X". These character identifiers provide a namespace separate for rules governing the firewalls behavior.

[0038] Rule chains essentially represent predicate/antecedent rule logic and can be classified as classic production rules systems as known in the Artificial Intelligence community. The tree nodes of a rule chain is a specific representation of a more general Boolean logic structure where each node in a chain tree that is traversed represented AND'd predicate logic in Boolean form. Additionally, exits from a rule chain (i.e., reaching leaf nodes) or jumps to other rule chains represent the antecedent portion of the rule.

[0039] Said differently, rule chains represent classic "If-Then" logic, as might be supported by the syntax of a software programming language.

[0040] FIG. 2 illustrates a representative set of firewall rules that handles NAT'd, MASQUERAD'd, VPN'd, port blocked, port forwarded and client authenticated traffic. While not an exhaustive list of firewall capabilities, these firewall functions are relatively standard and basic capabilities that can be found in most firewall implementations. These basic capabilities serve as an example from which to explain the dynamic firewall rule chain logic and are not meant to be an exhaustive or limiting list of capabilities. One main embodiment of the invention is the ability to dynamically extend, prune or otherwise modify these firewall rule chain sets as functional requirements or the network operating environment changes.

[0041] The arriving (:A) sub-tree (represented at 202) prepares packets to enter the matrix. This is where packets are marked, de-NATed (if Network Address Translation has occurred), de-MAQUERADEd and redirected. Since the purpose of this sub-tree is packet "conditioning", its rules only change network packets, and do not drop or accept them. Along with the :D sub-tree (see below), these rules implement the behaviors of nodes.

[0042] In the rule chain represented by 218, the antecedent portion of the :A rule chain redirects a network packet based on a port forwarding rule. Specifically, this rule (218) rewrites a portion of the network packet header, either changing the destination address or port, so that the packet arrives at an alternate location, once the packet departs the firewall, than originally addressed. In this example, the packet header contents are modified as a result of this :A rule chain.

[0043] In the :A rule chain represented by 224, a packets protocol is detected and "captured", before a determination is made as to where the packet may next proceed. This particular rule chain represents a common manner for capturing unauthorized network clients and either forcing them to authenticate themselves (usually against an authentication server like LDAP) or simply redirecting them to a constrained location on the network where their ability to view network resources is limited.

[0044] It is important to note, at this point, that the rule chains represented by FIG. 2 are composite rules chains of the entire firewall model and do not describe rule chains at any particular node or attached to any particular inter-node connection. For certain rules, especially those annotated as departing to or arriving from Clients or the WAN, there are likely logically constrained attachment points so that they work properly; e.g., A: chains dealing with incoming Client packets are likely attached to the LAN interface (logical, physical or virtual), since network Clients connect to a firewall via the LAN interface. Attachment points for other rule chains may be deferred to implementation details, based on the implementation technology or optimization requirements (speed, memory or cost).

[0045] In the matrix (:M) sub-tree (represented at 204), packets are routed through different chains depending on their source and destination nodes. The main purpose of this sub-tree is to decide if packets deserve to arrive at their destination, so the rules in this sub-tree only accept or drop packets, not change them. These rules implement the behaviors of the connections between nodes. More specifically, :M chains can be attached to the

incoming/outgoing interfaces of nodes themselves, or attached to the inter-node connections.

[0046] The departing (:D) sub-tree (represented at 206), post-processes packets that have successfully navigated the matrix. Packets that arrive here deserve to be transmitted, so the rules in this sub-tree only change packets, not drop or accept them. This is where packets are NATed and MASQUERADEd. Along with the :A sub-tree, these rules implement the behaviors of nodes. :D chains are normally associated with nodes that have interfaces (logical, physical, virtual) with network segments outside of the firewall model.

[0047] The :X subtree contains chains that are compact, well-identified places where rules can be inserted and deleted dynamically. Packets arrive at these chains from well-identified "taps" in the main pathway. These taps are indicated throughout FIG. 2 by "=>" pointing at the name of the :X chain that will receive packets. This is shown, for example, at 208. :X chains exist for extensibility and may be provided, a priori, as part of the firewall implementation or may be dynamically loaded as part of a firewalls configuration or runtime reconfiguration.

[0048] In any tree structure, there are ultimately "leaves" of the tree, from which there are no child nodes. FIG. 2 demonstrates leaf chains, which have suffixes that indicate how they behave. ":Accept" chains, such as that represented at 210, have rules with ACCEPT targets. When a packet matches an ACCEPT target, the packet immediately jumps out of the current sub-tree, and moves to the next. Accept chains are useful for forming Boolean OR constructs. For example, the following series of rules might appear in a chain that needs to accept packets that match any of the tests "A", "B" or "C", each of which are implemented in their own chain. As an example, the "iptables" utility available from the Linux Operating System environment uses the following syntax to enable rules:

```
iptables -t filter -A ExampleChain -j TestA:Accept
iptables -t filter -A ExampleChain -j TestB:Accept
iptables -t filter -A ExampleChain -j TestC:Accept
```

[0049] According to one embodiment, the default policy in the :M sub-tree is DROP. That is, if a packet traverses the entire :M sub-tree and never matches an ACCEPT target, it will be dropped.

[0050] ":Drop" chains, such as that represented at 212, have rules with DROP targets. When a packet encounters a DROP target, it is discarded and will never be delivered to its destination.

[0051] ":Pass" chains, such as that represented at 214, have rules with RETURN targets, and a single DROP target at the end. A RETURN target causes the packet to jump out of the current chain and resume its path through the "calling" chain. Each rule other than the final DROP describes a packets that should be "passed" on to further processing. Packets that match none of the RETURN rules encounter the DROP rule and are discarded. Since the DROP target in a pass chain must stay at the end of the chain, new rules, according to one embodiment, must be inserted, rather than appended.

[0052] Pass chains are useful for forming Boolean AND constructs. For example, the following series of rules might appear in a chain that needs to pass only packets that match all the tests "A", "B" and "C", each of which are implemented in their own chain. As an example, the "iptables" utility available from the Linux Operating System environment uses the following syntax to enable rules:

```
iptables -t filter -A ExampleChain -j TestA:Pass
iptables -t filter -A ExampleChain -j TestB:Pass
iptables -t filter -A ExampleChain -j TestC:Pass
```

[0053] ":Mark" chains, such as that represented at 216, have rules with MARK targets. These rules write packet marks according to various criteria. These chains appear only in the :A sub-tree because packets must be accounted for as soon as they arrive.

[0054] ":Redirect" chains, like that shown at 218, have rules with REDIRECT targets. These rules usually change a packet's destination address and/or port.

[0055] ":Skip" chains (e.g., shown at 220) are like pass chains, these chains have rules with RETURN targets. Unlike pass chains, skip chains have something other than a DROP target at the end. Each rule other than the final one describes packets that should skip whatever processing the final rule offers. Packets that match none of the RETURN rules are processed by the final rule. Since the final rule must stay at the end of the chain, new rules, according to one embodiment, must be inserted, rather than appended.

[0056] ":S (:J)" chains are "services" (described below). The names of nodes that subscribe to a service are shown in parentheses after the chain. For each :S chain (e.g., shown at 222), there is a :J chain that is not shown.

[0057] A "service" is a set of rules that operate on packets in a very specific way (e.g., masquerading outgoing packets, or capturing incoming packets). Every service has two chains. The first chain has a name ending with :S. This chain appears in the packet pathway in a specific place and is guaranteed to see all packets flowing through the firewall. The second chain has a name ending with :J and contains the rules that actually implement the service. Packets that need the service are directed through the second chain by a "jumper" in the first chain. This is analogous to a hardware jumper used to enable a feature.

[0058] For example, HTTP requests arriving from the Clients node must be captured if the given client is not authorized. Thus, the :A:Redir:HTTPCap:S (shown at 224) can contain a rule that causes packets coming from eth0 to the :A:Redir:HTTPCap:J chain. The rules in the :A:Redir:HTTPCap:J chain arrange for the capture of unauthorized packets.

[0059] One example of Mark Space Allocation employs a 32-bit number that travels with the packet when it's in the system--it is lost as soon as the packet enters a device. Marks can be read and written by rules in the firewall. They can also be read (but not written) by the routing and bandwidth control systems. Thus, firewall rules can be used to control how packets are routed and scheduled for transmission.

[0060] It can be noted from FIG. 2 that rules can be applied to nodes or connections between nodes. For example, rule 208 is applied to the node "clients" (represented by the (clients) in the rule). A rule associated with the clients node will be applied to packets to/from devices or services associated with the clients node in the firewall model. Rules can also be associated with connections. For example, for the chain shown in FIG. 2B:

```
M:X:WAN-x-Clients  =>:X:Network:Accept
                   =>:X:PortForwarding:Accept
                   =>:X:PortXlation:Accept
```

The rules are applied to packets flowing on the connection between the WAN node and the clients node.

[0061] When a packet arrives at the firewall, it is automatically assigned a mark of zero (the "unmarked" mark). As quickly as possible, the firewall attempts to assign a mark that attributes the packet to whichever party is best accountable for it. This is important for two reasons:

[0062] It tells the firewall, bandwidth control and routing systems how to treat a packet. For example, priority channel packets are passed immediately by the firewall, and then transmitted by the bandwidth control system as soon as they arrive. Packets with client marks are passed conditionally, depending on whether or not the owning client has the proper authorization, and then scheduled for transmission by the bandwidth control system in accordance with the client's provisioning.

[0063] It also tells the firewall how to account for a packet. In order for the firewall to send proper accounting reports, it must be able to match a packet to a client or other accounting entity. When the firewall marks a packet, it enables the firewall to do this.

[0064] The table below shows one embodiment of how the mark name space is allocated:

Mark (hex)	Description
0000	Unmarked
0001 – 0fff	RESERVED
1xxx 1000 1001 1002 1003 – 1fff	System traffic marks (4K marks) Unattributed Firewall VPN RESERVED
2xxx	Static clients (4k marks)
3xxx	Dynamic clients (4k marks)
4000 – fffe	Per-IP Bandwidth Control
Ffff	MAC address bypass

[0065] The mark ranges are in order of numerical value, but are also in order of "mark priority". For example, a dynamic client mark has a higher priority than the firewall mark. This is why a packet traveling from a client to the firewall merits both marks, but will receive the client's mark. Notice that the priority channel has the highest priority mark. This means that packets from a client that travels over the priority channel will be attributed to the priority channel - not the client from which it came.

[0066] All packets get "0x0000" mark automatically when they enter the firewall. A packet will receive a more informative mark if it can be attributed. These packets have limited permission to travel through the firewall and are very susceptible to being captured.

[0067] The "0x1xxx" range (where xxx is a 3-digit hexadecimal range from 000 to fff) is used to mark packets that cannot be specifically attributed with a higher mark, but can be

identified by the node to/from which they are traveling. Currently, there are only two marks in this range: firewall and VPN. There is no Clients mark because all packets traveling to/from the Clients node are given the appropriate client mark. There is no WAN mark because all packets traveling to/from the WAN node are given other marks.

[0068] An important use for this range is exemplified by the VPN mark. When packets depart through the ipsec0 pseudo-device, they generate new packets that emerge from the firewall and leave through the physical eth1 device. Thus, tunneled VPN traffic competes with clients and other elements of the system to consume bandwidth on the eth1 device. For that reason, these packets must be marked so they can be accounted for.

[0069] According to one embodiment, new nodes can be dynamically generated for new pseudo-devices that, like the VPN, will generate packets that must flow out through a physical device. Each such node will be allocated a mark from this range. :D rule chains implement packet handling for pseudo devices as the packets depart the firewall.

[0070] Packets receive the "0x1000" firewall mark if they are arriving from or destined for the firewall and do not already have a higher-priority mark.

[0071] Packets receive the "0x1001" VPN mark if they are carrying tunnel traffic for a VPN node.

[0072] Marks for static clients are allocated from the "0x2xxx" range (where xxx is the hexadecimal range 000 to fff). Notice that this is a lower priority range than dynamic clients. That is, if a packet merits both a static and dynamic client mark, it will receive the dynamic client mark.

[0073] Marks for dynamic clients are allocated from range 0x3xxx, where xxx is the hexadecimal range 000 to fff.

[0074] The "0xfxxx" range is used to mark packets belong to various unaccounted categories.

[0075] The mark "0xf000" applies to packets that qualify for MAC Address Bypass.

[0076] The "0xffff" mark applies to packets in the priority channel.

[0077] Packets departing from the router node receive marks in this order:

- Apply a client's mark to packets departing through a device owned by the client.
- Apply a client's mark to packets with a destination IP address owned by the client.

[0078] For any packets that don't yet have a mark:

- Apply the VPN mark to unmarked IPv6-Crypt protocol packets.
- Apply the firewall mark to unmarked packets.

[0079] If the packet can be attributed to a network client, it will be. Otherwise, it will be attributed to the firewall. Since the firewall doesn't participate in VPN tunnels with clients, the VPN mark will never apply.

[0080] VPN tunnel traffic will be IPv6-Crypt protocol, and will receive the VPN mark. All other traffic will receive the firewall mark.

[0081] Packets destined for the router node receive additional marks in this order:

- Apply the VPN mark to unmarked IPv6-Crypt protocol packets.
- Apply the firewall mark to unmarked packets.

[0082] Packets arriving from the Clients node receive marks in this order:

- Apply a client's mark to packets arriving from a device owned by the client.
- Apply a client's mark to packets with a source IP address owned by the client.
- Apply the MAC address bypass mark to qualifying packets.
- Apply the priority channel mark to qualifying packets.

[0083] Apply additional marks in this order:

- Apply the VPN mark to unmarked IPv6-Crypt protocol packets.
- Apply the firewall mark to unmarked packets.

[0084] Packets arriving from the VPN node receive marks in this order:

- Apply a client's mark to packets departing through a device owned by the client.
- Apply a client's mark to packets with a destination IP address owned by the client.

[0085] Apply additional marks in this order:

- Apply the VPN mark to unmarked IPv6-Crypt protocol packets.
- Apply the firewall mark to unmarked packets.

[0086] Client marks, according to one embodiment, will never apply to this traffic. Tunnel within tunnel traffic will receive the VPN mark, just like tunnel traffic through the WAN node. All remaining traffic will receive the firewall mark.

[0087] Packets arriving from the WAN node receive marks in this order:

- Apply a client's mark to packets departing through a device owned by the client.
- Apply a client's mark to packets with a destination IP address owned by the client.

[0088] Apply additional marks in this order:

- Apply the VPN mark to unmarked IPv6-Crypt protocol packets.
- Apply the firewall mark to unmarked packets.

[0089] According to one embodiment, client marks will never apply to this traffic. Tunnel traffic will receive the VPN mark. All remaining traffic will receive the firewall mark.

[0090] If the packet can be attributed to a client, it will be. Otherwise, it will be unmarked. Note that port forwarded and port translated traffic that is not directed at a specific client will be unmarked. One way to insure that this traffic is marked and accounted for would be to set up a static client.

[0091] One embodiment includes a conceptual model representing a network firewall that separates firewall functionality into individually configurable and controllable components.

[0092] Another embodiment includes the conceptual model, wherein the hardware or component technology used to host a firewall model's implementation is indistinct from commercial off-the-shelf components and, therefore, the firewall is driven by a dynamically reconfigurable implementation of the firewall model. A non-limiting example of a dynamically reconfigurable implementation of the firewall model can be realized through a computer program product comprising a computer readable storage medium storing computer program code executable by a computer. One of ordinary skill in the art can appreciate that many suitable computer readable storage media exist.

[0093] Yet another embodiment includes a conceptual model, where a set of firewalls can be dynamically reconfigurable and managed as a cohesive group of firewall nodes in a network implementation comprised of several LAN and WAN segments needing firewall protection. In a system of firewalls, each protecting a separate network segment, system-wide policies can be implemented by downloading identical sets of rule chains to each firewall, as a representation of common firewall configurations. It may also be desirable to "clone-n-hone" firewall configurations, which occurs with a common rule chain configuration is provided to each firewall in a system of firewalls and individual

firewalls receive localized customizations, tailoring their behavior to the needs of a particular network segment. Localized rule chain modifications make it possible to extend/modify an individual firewall's behavior, based on a general behavior policy.

[0094] According to one embodiment, the firewall behaviors can be described as predicate/antecedent rule logic acting upon dynamic data from both the configuration space of the firewall as well as changing network state and client connectivity. The rule chain predicates ("If" portions of a rule) act on data that is potentially available from multiple sources:

- Configuration data of the firewall (e.g., its Internet Protocol Address, its local identification string, the version of the firewall rule chain set, etc.)
- Data arriving in the network packet itself (e.g., the origination or destination address, the protocol, portions of the payload data, etc.)
- Data available through firewall extensions (:X rule chains) that may be monitoring network traffic flows for activity spikes or lulls or, perhaps, a device monitoring extension that polls a timer or instrumentation device for time-sensitive data.

[0095] While the invention has been described with reference to particular embodiments, it should be understood that the embodiments are illustrative and that the scope of the invention is not limited to these embodiments. Many variations, modifications, additions and improvements to the embodiments described above are possible. It is contemplated that these variations, modifications, additions and improvements fall within the scope of the invention as detailed in the following claims.

WHAT IS CLAIMED IS:

1. A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:

defining at least one node, wherein the at least one node is associated with two or more network interfaces;

associating a set of firewall rules with the at least one node;

receiving a packet at a first node of the at least one node; and

accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically configurable.

2. A method according to claim 1, wherein the set of firewall rules being dynamically configurable further comprises dynamically updating the set of firewall rules during runtime.

3. A method according to claim 2, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules.

4. A method according to claim 1, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

5. A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.

6. A method according to claim 5, wherein the at least one node further comprises a second node, further comprising associating a second subset of the set of firewall rules with the second node.

7. A method according to claim 6, wherein the first subset of firewall rules is same as or at least partially different from the second subset of firewall rules.

8. A method according to claim 6, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.

9. A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.

10. A method according to claim 9, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

11. A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.

12. A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.

13. A device for controlling data through a firewall, comprising:

a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices;

a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically configurable; and

a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:

define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces; and

when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules.

14. A device according to claim 13, wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime.

15. A device according to claim 14, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

16. A device according to claim 13, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

17. A device according to claim 13, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

18. A device according to claim 17, wherein the at least one node further comprises a second node, and wherein the data controlling computer program code is further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

19. A device according to claim 18, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

20. A device according to claim 18, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

21. A device according to claim 13, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.

22. A device according to claim 21, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet .

23. A device according to claim 13, wherein each of the at least one node is associated with at least two network interfaces.

24. A device according to claim 13, wherein each of the plurality of network interfaces is connected with at least one physical device.

25. A device according to claim 13, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces.

26. A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:

define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;

associate a set of firewall rules with the at least one node;

receive a packet at a first node of the at least one node; and

accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically configurable.

27. A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime.

28. A data controlling computer program product according to claim 27, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

29. A data controlling computer program product according to claim 27, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

30. A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

31. A data controlling computer program product according to claim 30, wherein the at least one node further comprises a second node, and wherein the computer instructions are further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

32. A data controlling computer program product according to claim 31, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

33. A data controlling computer program product according to claim 31, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

34. A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.

35. A data controlling computer program product according to claim 34, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet .

36. A data controlling computer program product according to claim 26, wherein each of the at least one node comprises at least two network interfaces.

37. A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is connected with at least one physical device.

38. A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is physically connected to every other network interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

ABSTRACT

[0096] A system, method, and computer program product for controlling data through a firewall which may be dynamically configurable. The method may comprise defining at least one node, wherein the at least one node is associated with two or more network interfaces; associating a set of firewall rules with the at least one node; receiving a packet at a first node of the at least one node; and accepting or denying the packet based on the set of firewall rules. The firewall rules include dynamic chains of rules having defined places where firewall rules may be dynamically inserted into or deleted from the firewall while the firewall is operating on one or more machines connected to network segments where the nodes reside.

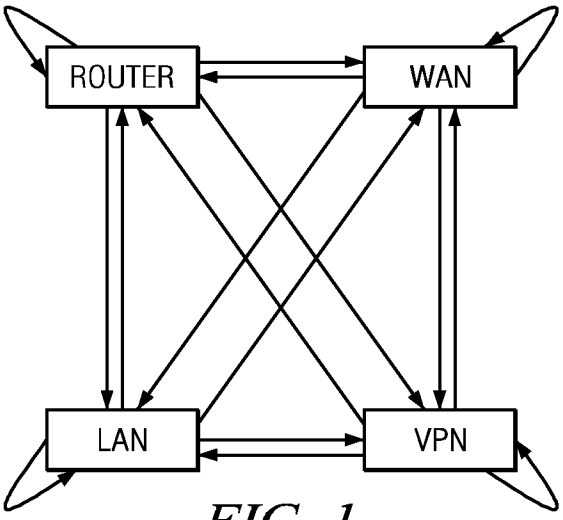

ROUTER
WAN
LAN
VPN

FIG. 1

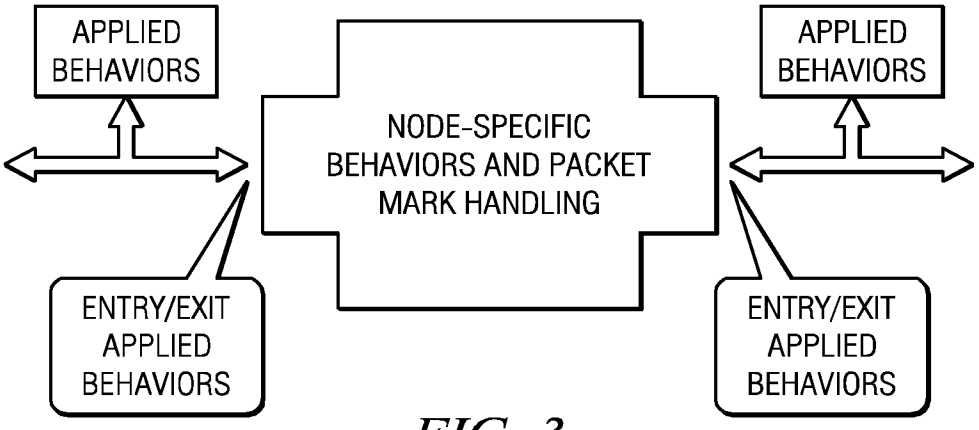

APPLIED BEHAVIORS
NODE-SPECIFIC BEHAVIORS AND PACKET MARK HANDLING
APPLIED BEHAVIORS
ENTRY/EXIT APPLIED BEHAVIORS
ENTRY/EXIT APPLIED BEHAVIORS

FIG. 3

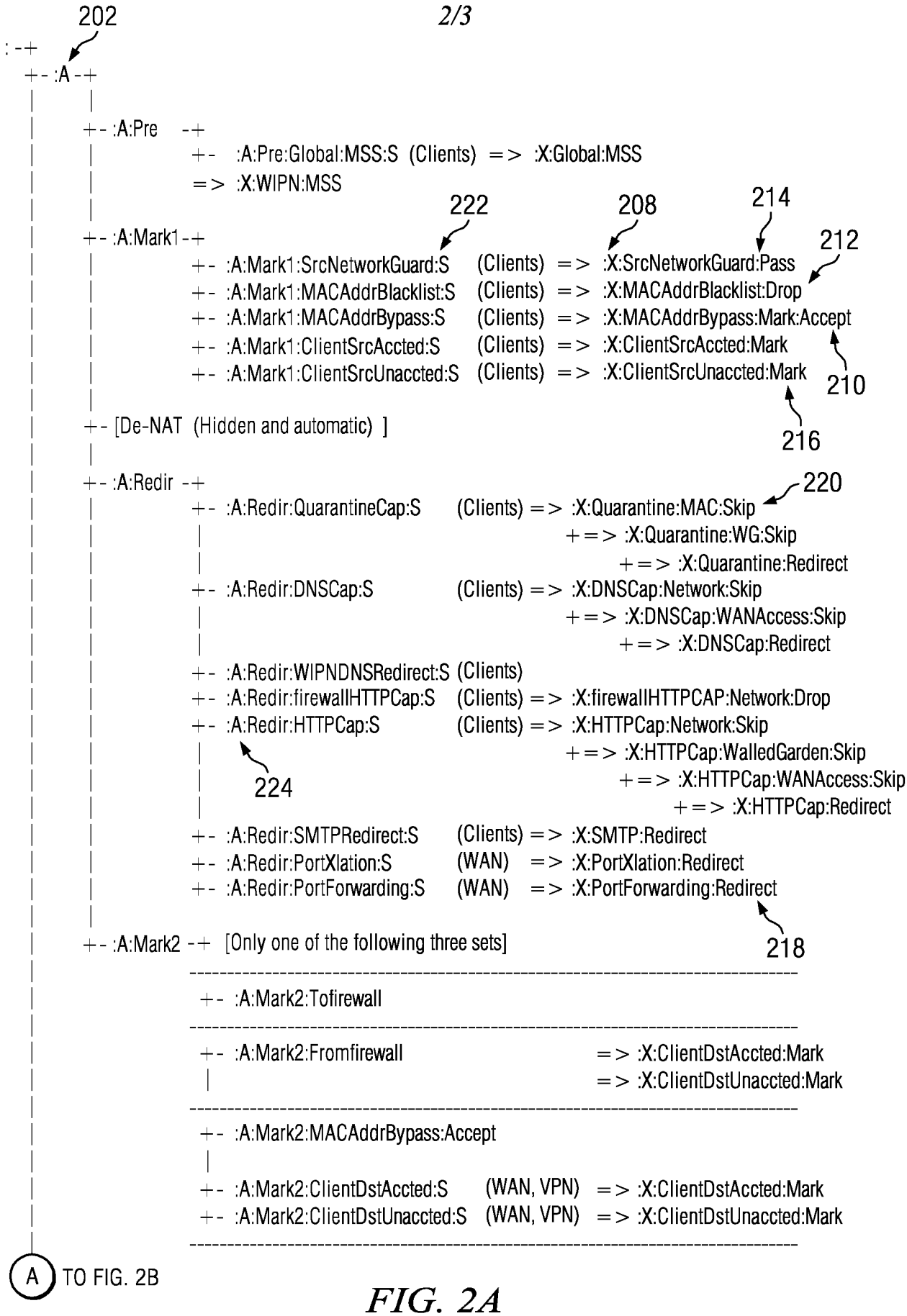

202
:-+
+- :A -+
|
+- :A:Pre -+
+- :A:Pre:Global:MSS:S (Clients) => :X:Global:MSS
=> :X:WIPN:MSS
222
208
214
212
+- :A:Mark1 -+
+- :A:Mark1:SrcNetworkGuard:S (Clients) => :X:SrcNetworkGuard:Pass
+- :A:Mark1:MACAddrBlacklist:S (Clients) => :X:MACAddrBlacklist:Drop
+- :A:Mark1:MACAddrBypass:S (Clients) => :X:MACAddrBypass:Mark:Accept
+- :A:Mark1:ClientSrcAccted:S (Clients) => :X:ClientSrcAccted:Mark
+- :A:Mark1:ClientSrcUnaccted:S (Clients) => :X:ClientSrcUnaccted:Mark
210
216
+- [De-NAT (Hidden and automatic)]
220
+- :A:Redir -+
+- :A:Redir:QuarantineCap:S (Clients) => :X:Quarantine:MAC:Skip
+=> :X:Quarantine:WG:Skip
+=> :X:Quarantine:Redirect
+- :A:Redir:DNSCap:S (Clients) => :X:DNSCap:Network:Skip
+=> :X:DNSCap:WANAccess:Skip
+=> :X:DNSCap:Redirect
+- :A:Redir:WIPNDNSRedirect:S (Clients)
+- :A:Redir:firewallHTTPCap:S (Clients) => :X:firewallHTTPCAP:Network:Drop
+- :A:Redir:HTTPCap:S (Clients) => :X:HTTPCap:Network:Skip
224
+=> :X:HTTPCap:WalledGarden:Skip
+=> :X:HTTPCap:WANAccess:Skip
+=> :X:HTTPCap:Redirect
+- :A:Redir:SMTPRedirect:S (Clients) => :X:SMTP:Redirect
+- :A:Redir:PortXlation:S (WAN) => :X:PortXlation:Redirect
+- :A:Redir:PortForwarding:S (WAN) => :X:PortForwarding:Redirect
218
+- :A:Mark2 -+ [Only one of the following three sets]
+- :A:Mark2:Tofirewall
+- :A:Mark2:Fromfirewall => :X:ClientDstAccted:Mark
=> :X:ClientDstUnaccted:Mark
+- :A:Mark2:MACAddrBypass:Accept
+- :A:Mark2:ClientDstAccted:S (WAN, VPN) => :X:ClientDstAccted:Mark
+- :A:Mark2:ClientDstUnaccted:S (WAN, VPN) => :X:ClientDstUnaccted:Mark
A TO FIG. 2B

FIG. 2A

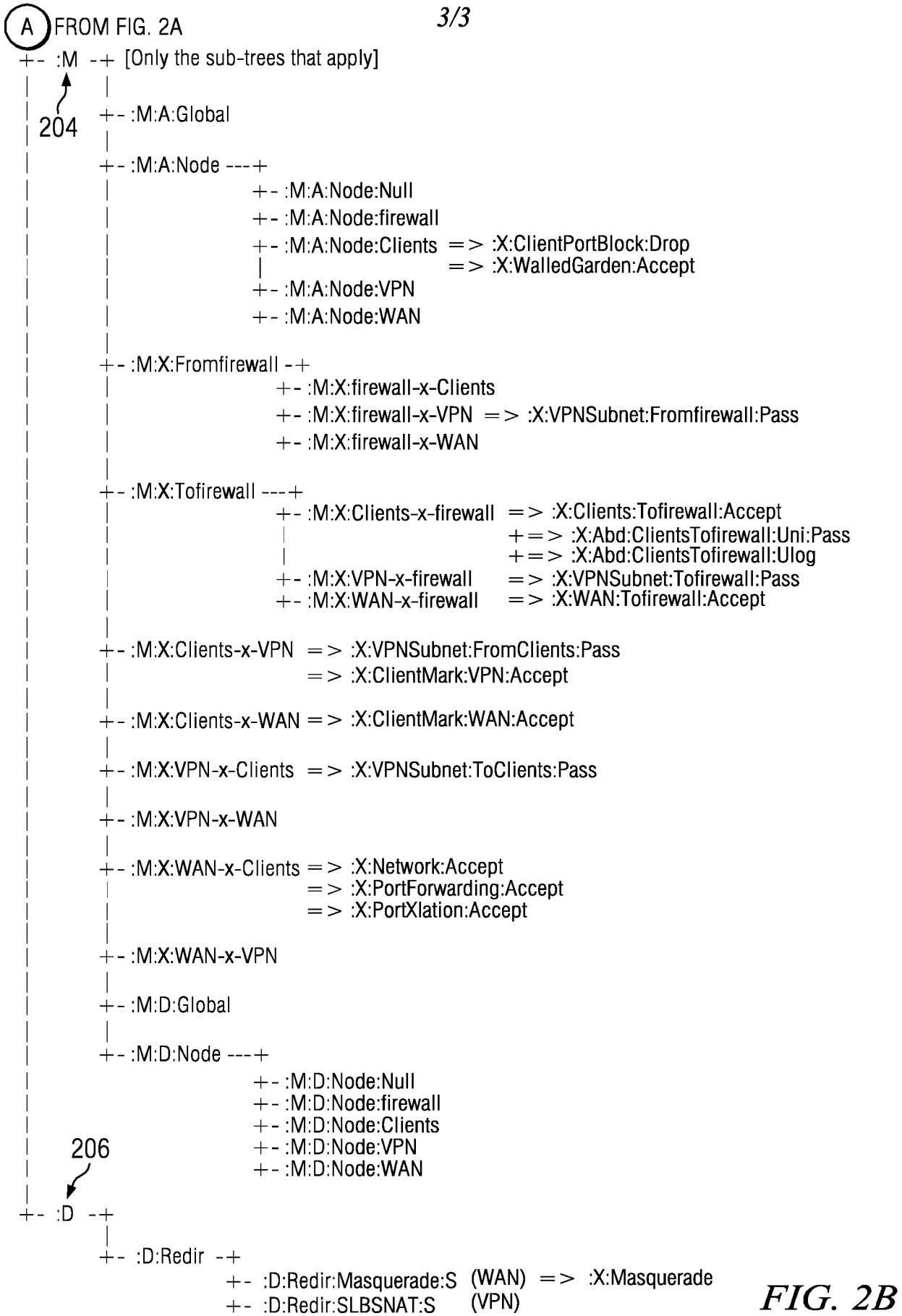

A FROM FIG. 2A
+- :M -+ [Only the sub-trees that apply]
204
+- :M:A:Global
+- :M:A:Node ---+
+- :M:A:Node:Null
+- :M:A:Node:firewall
+- :M:A:Node:Clients => :X:ClientPortBlock:Drop
=> :X:WalledGarden:Accept
+- :M:A:Node:VPN
+- :M:A:Node:WAN
+- :M:X:Fromfirewall -+
+- :M:X:firewall-x-Clients
+- :M:X:firewall-x-VPN => :X:VPNSubnet:Fromfirewall:Pass
+- :M:X:firewall-x-WAN
+- :M:X:Tofirewall ---+
+- :M:X:Clients-x-firewall => :X:Clients:Tofirewall:Accept
+=> :X:Abd:ClientsTofirewall:Uni:Pass
+=> :X:Abd:ClientsTofirewall:Ulog
+- :M:X:VPN-x-firewall => :X:VPNSubnet:Tofirewall:Pass
+- :M:X:WAN-x-firewall => :X:WAN:Tofirewall:Accept
+- :M:X:Clients-x-VPN => :X:VPNSubnet:FromClients:Pass
=> :X:ClientMark:VPN:Accept
+- :M:X:Clients-x-WAN => :X:ClientMark:WAN:Accept
+- :M:X:VPN-x-Clients => :X:VPNSubnet:ToClients:Pass
+- :M:X:VPN-x-WAN
+- :M:X:WAN-x-Clients => :X:Network:Accept
=> :X:PortForwarding:Accept
=> :X:PortXlation:Accept
+- :M:X:WAN-x-VPN
+- :M:D:Global
+- :M:D:Node ---+
+- :M:D:Node:Null
+- :M:D:Node:firewall
+- :M:D:Node:Clients
206
+- :M:D:Node:VPN
+- :M:D:Node:WAN
+- :D -+
+- :D:Redir -+
+- :D:Redir:Masquerade:S (WAN) => :X:Masquerade
+- :D:Redir:SLBSNAT:S (VPN)

FIG. 2B

Copy From Parent

Please type a plus sign (+) inside this box [+] PTO/SB/01

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)		
	Attorney Docket No.	ROCK1150-1
	First Named Inventor	Patrick Turley
	COMPLETE IF KNOWN	
	Application Number	Unknown
	Filing Date	March 10, 2005
[X] Declaration Submitted with Initial Filing [ ] Declaration Submitted after Initial Filing	*Group Art Unit*	Unknown
	Examiner Name	Unknown

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING

(Title of Invention)

the specification of which was filed on (MM/DD/YYYY)	Herewith
as United States Application Number or PCT International Application Number	Herewith
and was amended on (MM/DD/YYYY) *(if applicable)*	

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me which is material to the patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO

Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below:

Application Number(s)	Filing Date (MM/DD/YYYY)	
60/551,698	03/10/2004	[ ] Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto

DECLARATION -- Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States Application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number *(If applicable)*

Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the registered practitioner(s) assigned to **Customer No. 44654** to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole/First Inventor:							
Given Name (first and middle [if any])		Family Name or Surname					
Patrick		**Turley**					
Inventor's Signature	P. Turley			Date	3/8/2005		
Residence: City	AUSTIN	State	TX	Country	USA	Citizenship	USA
Residence Address	1820 TREADWELL STREET AUSTIN, TX 78704						
Post Office Address	3903 SOUTH CONGRESS AVE. AUSTIN, TX 78704						

Name of Sole/First Inventor:							
Given Name (first and middle [if any])		Family Name or Surname					
Eric		**White**					
Inventor's Signature	E White			Date	9 March 2005		
Residence: City	Austin	State	TX	Country	USA	Citizenship	USA
Residence Address	1717 Bandcliff Drive, Austin TX 78704						
Post Office Address	same as residence						

Direct all correspondence to
Customer No. 44654

Name	John L. Adair	Sprinkle IP Law Group			
Address	1301 W. 25th Street, Suite 408				
City	Austin	*State*	TX	*Zip*	78705
Country	U.S.A.	*Telephone*	512.637.9220	*Fax*	512.371.9088

FORTINET EX1002 Page 31

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
CERTIFICATE OF TRANSMISSION VIA EFS-WEB SYSTEM	Atty Docket No. **ROCK1150-3**

In the Application of: **Patrick Turley**
Date Filed: **Herewith**
Title: **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**

Mail Stop: Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

I hereby certify that the attached Continuation Patent Application Transmittal Form (1 page), executed Declaration and Power of Attorney (copy from parent, 2 pages), Patent Application Specification and Claims (25 pages), and Drawings (3 sheets) are being deposited electronically using the United States Patent and Trademark Office EFS-Web System on April 22, 2011.

Respectfully submitted,
Sprinkle IP Law Group

Betty Caldwell
Betty Caldwell

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Filer:	Katharina W. Schuster/Betty Caldwell
Attorney Docket Number:	ROCK1150-3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Claims:				
Claims in excess of 20	2202	18	26	468
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**930**

Electronic Acknowledgement Receipt

EFS ID:	9937651
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Katharina W. Schuster/Betty Caldwell
Filer Authorized By:	Katharina W. Schuster
Attorney Docket Number:	ROCK1150-3
Receipt Date:	22-APR-2011
Filing Date:	
Time Stamp:	14:50:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$930
RAM confirmation Number	942
Deposit Account	503183
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	ROCK1150-3_Patent_Application_Transmittal.pdf	72498 7ac570b94dcd90fd15c5727834317d81dcd32e3b	no	1
Warnings:					
Information:					
2		ROCK1150-3_Application.pdf	113006 2bede3e2f576ec321bd69ba035e3eca71cdb922f	yes	25

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	18
Claims	19	24
Abstract	25	25

Warnings:					
Information:					
3	Drawings-only black and white line drawings	ROCK1150-3_Drawings.pdf	144929 4f75435c4541b8f24fb86586ae9c76f94fbd056f	no	3
Warnings:					
Information:					
4	Oath or Declaration filed	ROCK1150-3_Declaration_Parent.pdf	2751050 0574776cd59305c68d43e24ade1be2ad025ccda0	no	2
Warnings:					
Information:					
5	Miscellaneous Incoming Letter	ROCK1150-3_Certificate_Transmission.pdf	26495 e158ff66f1fd61de12ce11594bd9a4f3ff68eb16	no	1
Warnings:					
Information:					
6	Fee Worksheet (PTO-875)	fee-info.pdf	37036 5c5e80c8c94af494078a61d3dc1558c99c02a146	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	3145014

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/092,488	04/22/2011	2431	930	ROCK1150-3	38	3

CONFIRMATION NO. 6667

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

FILING RECEIPT

OC00000047524177

Date Mailed: 05/09/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 44654

Domestic Priority data as claimed by applicant

This application is a CON of 12/579,566 10/15/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 05/05/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/092,488**

Projected Publication Date: 08/18/2011

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/092,488

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	82		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	270		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	110		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	38 minus 20 =	* 18	x 26 =	468	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 110 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	930		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

RECEIVED
CENTRAL FAX CENTER
MAY 23 2011

sprinkle IP LAW GROUP

FAX COVER SHEET

TO:	Commissioner for Patents	**Fax#:**	571-273-8300
		Group Art Unit	2431
FROM:	Katharina W. Schuster	**Client Matter #:**	ROCK1150-3
		Serial #:	13/092,488
DATE:	May 23, 2011	**# of Pages:**	8
RE:	Request for Corrected Filing Receipt		

Please contact 512.637.9220 if there is a problem with this transmission.

See Following request for corrected filing receipt

CONFIDENTIALITY NOTICE

This communication is ONLY for the person named above. Unless otherwise indicated, it contains information that is confidential, privileged or exempt from disclosure under applicable law. If you are not the person named above, or responsible for delivering it to that person, be aware that disclosure, copying, distribution or use of this communication is strictly PROHIBITED. If you have received it in error, or are uncertain as to its proper handling, please immediately notify us by telephone and mail the original to us at the above address. Thank you.

1301 W. 25th STREET, SUITE 408
AUSTIN, TX 78705
[o] 512.637.9220 [f] 512.371.9088

RECEIVED
CENTRAL FAX CENTER
MAY 23 2011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
REQUEST FOR CORRECTED FILING RECEIPT	Atty. Docket No. **ROCK1150-3**
In re Application of: **Patrick Turley**	
Application Number: **13/092,488**	Filed: **April 22, 2011**
For: **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit: **2431**	Confirmation No. **6667**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Certificate of Mailing Via Facsimile

I hereby certify that this document is being transmitted via facsimile to the U.S. Patent Office, Office of Initial Patent Examinations, Fax No. 571-273-8300 on May 23, 2011.

Betty Caldwell
Betty Caldwell

1. Attached is a copy of the official filing receipt received from the PTO in the above application for which issuance of a corrected filing receipt is respectfully requested.
2. There is an error with respect to the following data, which is:

☐	Incorrectly entered and/or
☒	Omitted: **Domestic Priority data as claimed by applicant. Please see Specification filed April 22, 2011, page 1, paragraph 0001**

		Error In		*Correct data*
A.	☒	Priority Information	A.	This application is a CON of 12/579,566 filed 10/15/2009 Which is a CON of 11/076,719 filed 3/10/2005 Which claims benefit of 60/551,698 filed 3/1/2004
B.	☐	Inventor's Info.	B.	
C.	☐	Title	C.	
D.	☐	Filing Date	D.	
E.	☐	Other	E.	

May 23, 2011
Date

Katharina W. Schuster
Reg. No.: 50,000

RECEIVED
CENTRAL FAX CENTER
MAY 23 2011

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE RECD	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/092,488	04/22/2011	2431	930	ROCK1150-3	38	3

CONFIRMATION NO. 6667

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

FILING RECEIPT



Date Mailed: 05/09/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 44654

Domestic Priority data as claimed by applicant

This application is a CON of 12/579,566 10/15/2009 which is a CON of 11/076,719 3/10/2005 which claims benefit of 60/551,698 3/1/2004

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 05/05/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/092,488**

Projected Publication Date: 08/18/2011

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

FORTINET EX1002 Page 44

Title

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

PAGE 4/8 * RCVD AT 5/23/2011 3:59:41 PM [Eastern Daylight Time] * SVR:W-PTOFAX-001/35 * DNIS:2738300 * CSID: * DURATION (mm-ss):02-27

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PAGE 5/8 * RCVD AT 5/23/2011 3:59:41 PM [Eastern Daylight Time] * SVR:W-PTOFAX-001/35 * DNIS:2738300 * CSID: * DURATION (mm-ss):02-27

FORTINET EX1002 Page 46

RECEIVED
CENTRAL FAX CENTER
MAY 23 2011

COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/092,488	04/22/2011	2431	930	ROCK1150-3	38	3

CONFIRMATION NO. 6667

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

FILING RECEIPT



Date Mailed: 05/09/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 44654

Domestic Priority data as claimed by applicant

This application is a CON of 12/579,566 10/15/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 05/05/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/092,488**

Projected Publication Date: 08/18/2011

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

COPY

Title

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an International application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

COPY

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/092,488	04/22/2011	2431	930	ROCK1150-3	38	3

CONFIRMATION NO. 6667

CORRECTED FILING RECEIPT

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

OC000000047942119

Date Mailed: 06/01/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 44654

Domestic Priority data as claimed by applicant

This application is a CON of 12/579,566 10/15/2009
which is a CON of 11/076,719 03/10/2005 PAT 7,610,621
which claims benefit of 60/551,698 03/10/2004 *
(*)Data provided by applicant is not consistent with PTO records.

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 05/05/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/092,488**

Projected Publication Date: 09/08/2011

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

Title

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	229	US 7216173	05-08-2007	Clayton et al.	
	230	US 20020165949	11-07-2002	Na et al.	
	231	US 20030069955	04-10-2003	Gieseke et al.	
	232	US 6643260	11-04-2003	Kloth et al.	
	233	US 6789118	09-07-2004	Rao	
	234	US 6798746	09-28-2004	Kloth et al.	
	235	US 6816903	11-09-2004	Rakoshitz et al.	
	236	US 6876668	04-05-2005	Chawla et al.	
	237	US 6976089	12-13-2005	Na et al.	
	238	US 7185073	02-27-2007	Gai et al.	
	239	US 7257833	08-14-2007	Parekh et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C83	Office Action for U.S. Patent Application No. 12/579,566, mailed 10/06/2010, 7 pgs.	
	C115	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 03/23/2011, 12 pgs.	
	C116	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 05/13/2011, 8 pgs.	
	C117	Office Action for U.S. Patent Application No. 10/683,317, mailed 06/08/2011, 15 pgs.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	10275675
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Katharina W. Schuster/Delia Narvaiz
Filer Authorized By:	Katharina W. Schuster
Attorney Docket Number:	ROCK1150-3
Receipt Date:	10-JUN-2011
Filing Date:	22-APR-2011
Time Stamp:	10:40:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	ROCK_Ref_115.pdf	661527 abfa5008ecd1804d304c1665fc2c6cd489d96f47	no	12

Warnings:	
Information:	

2	Non Patent Literature	ROCK_Ref_C116.pdf	405088 d59310938272288fca0e57a0be4aba12e23bab48	no	8
Warnings:					
Information:					
3	Non Patent Literature	ROCK_Ref_C117.pdf	570455 859be8b5ab7d462ca0a0bb65502c23ac6adef8dd	no	15
Warnings:					
Information:					
4	Non Patent Literature	ION_Ref_C83.pdf	228147 dbe6e6b529f40b3e94157b5fcfa2a86947f5fd66	no	7
Warnings:					
Information:					
5		ROCK1150-3_IDS_061011.pdf	174285 5e815a9e856a2334af22638ae27aff5843b62640	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	5

Warnings:	
Information:	
Total Files Size (in bytes):	2039502

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371(c) Date **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2431**	Examiner **Not Yet Assigned**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on June 10, 2011.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

Applicant respectfully requests the Examiner considers information cited in parent application No. 12/579,566 filed October 15, 2009, from of which the present application is a continuation.

☒ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a final action under 37 C.F.R. § 1.113, a notice of allowance under 37 C.F.R. § 1.311, or an action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application. Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information.

Applicant does not believe any fees are due for filing this Information Disclosure Statement; however, if Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

Katharina W. Schuster
Reg. No. 50,000

Dated: June 9, 2011

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

EFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**



Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371(c) Date **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2431**	Examiner **Not Yet Assigned**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on 8/17 2011.

Signature

K. Jacobson

Printed Name

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. A copy of foreign patent documents as well as the information listed on the attached SB08B form is enclosed for the convenience of the Examiner. An English translation is not readily available for References C13, C17 and C18, however, an English abstract is included therein.

In addition to the attached references, Applicant respectfully requests consideration of references cited in parent applications including application serial numbers 08/816,174 and 09/458,602.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☒ This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a first Office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a final action under 37 C.F.R. § 1.113, a notice of allowance under 37 C.F.R. § 1.311, or an action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application. Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information.

Applicant does not believe any fees are due for filing this Information Disclosure Statement; however, if Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust
Patent Agent
Reg. No. 51,032

Dated: August 17, 2011

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

OPAP
AUG 2 9 2011
PATENT & TRADEMARK OFFICE
TAP21

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 1 of 12

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A1	US 5673393	09-30-1997	Marshall et al.	
	A2	US 5706427	01-06-1998	Tabuki	
	A3	US 5748901	05-05-1998	Afek et al.	
	A4	US 5901148	05-04-1999	Bowen et al.	
	A5	US 5936542	08-10-1999	Kleinrock et al.	
	A6	US 5987134	11-16-1999	Shin et al.	
	A7	US 5996013	11-30-1999	Delp et al.	
	A8	US 6085241	07-04-2000	Otis	
	A9	US 6108782	08-22-2000	Fletcher et al.	
	A10	US 6130892	10-10-2000	Short et al.	
	A11	US 6131116	10-10-2000	Riggins et al.	
	A12	US 6157953	12-05-2000	Chang et al.	
	A13	US 6173331	01-09-2001	Shimonishi	
	A14	US 6176883	01-23-2001	Holloway et al.	
	A15	US 6185567	02-06-2001	Ratnaraj et al.	
	A16	US 6194992	02-27-2001	Short et al.	
	A17	US 6212558	04-03-2001	Antur et al.	
	A18	US 6233607	05-15-2001	Taylor et al.	
	A19	US 6243815	06-05-2001	Antur et al.	
	A20	US 6295294	09-25-2001	Odlyzko	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B1	EP 0 587 522 A2	03-16-1994	Int'l Business Mach. Corp.	
	B2	WO 01/077787 A3	10-18-2001	Siebel Systems, US	
	B3	WO 02/09458 A2	01-31-2002	Bluesocket, Inc., US	
	B4	WO 02/023825 A1	03-21-2002	WP Media Inc.	
	B5	WO 02/041587 A2	05-23-2002	Bluesocket, Inc., US	
	B6	WO 02/077820 A1	10-03-2002	Bluesocket, Inc., US	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	2	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A21	US 6321339	11-20-2001	French et al.	
	A22	US 6324648	11-27-2001	Grantges, Jr.	
	A23	US 6404743	06-11-2002	Meandzija	
	A24	US 6421319	07-16-2002	Iwasaki	
	A25	US 6463474	10-08-2002	Fuh et al.	
	A26	US 6473793	10-29-2002	Dillon et al.	
	A27	US 6473801	10-29-2002	Basel	
	A28	US 6535879	03-18-2003	Behera	
	A29	US 6539431	03-25-2003	Sitaraman et al.	
	A30	US 20010039576	11-08-2001	Kanada	
	A31	US 20020013844	01-31-2002	Garrett et al.	
	A32	US 20020021665	02-21-2002	Bhagavath et al.	
	A33	US 20020023160	02-21-2002	Garrett et al.	
	A34	US 20020035699	03-21-2002	Crosbie	
	A35	US 20020042883	04-11-2002	Roux et al.	
	A36	US 20020046264	04-18-2002	Dillon et al.	
	A37	US 20020052950	05-02-2002	Pillai et al.	
	A38	US 20020055968	05-09-2002	Wishoff et al.	
	A39	US 20020059408	05-16-2002	Pattabhiraman et al.	
	A40	US 20020085719	07-04-2002	Crosbie	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B7	WO 03/021890 A1	03-13-2003	The Boeing Co., US	
	B8	WO 03/098461 A1	11-27-2003	Polcha et al.	
	B9	WO 04/034229 A2	04-22-2004	Rocksteady Networks, Inc.	
	B10	WO 04/036371 A2	04-29-2004	Rocksteady Networks, Inc.	
	B11	WO 05/020035 A2	03-03-2005	Rocksteady Networks, Inc.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	3	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A41	US 20020087713	07-04-2002	Cunningham	
	A42	US 20020091944	07-11-2002	Anderson et al.	
	A43	US 20020112183	08-15-2002	Baird, III et al.	
	A44	US 20020120741	08-29-2002	Webb et al.	
	A45	US 20020124078	09-05-2002	Conrad	
	A46	US 20020124103	09-05-2002	Maruyama et al.	
	A47	US 20020129143	09-12-2002	McKinnon, III et al.	
	A48	US 20020133581	09-19-2002	Schwartz et al.	
	A49	US 20020133589	09-19-2002	Gubbi et al.	
	A50	US 20020136226	09-26-2002	Christoffel et al.	
	A51	US 20020138762	09-26-2002	Horne	
	A52	US 20020143964	10-03-2002	Guo et al.	
	A53	US 20020152284	10-17-2002	Cambray et al.	
	A54	US 20020162030	10-31-2002	Brezak et al.	
	A55	US 20020164952	11-07-2002	Singhal et al.	
	A56	US 20020165990	11-07-2002	Singhal et al.	
	A57	US 20020169867	11-14-2002	Mann et al.	
	A58	US 20020174227	11-21-2002	Hartsell et al.	
	A59	US 20020178282	11-28-2002	Mysore et al.	
	A60	US 20030043846	03-06-2003	Purpura et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	4	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A61	US 20030087629	05-08-2003	Juitt et al.	
	A62	US 5953506	09-14-1999	Kalra et al.	
	A63	US 6336133	01-01-2002	Morris et al.	
	A64	US 6502131	12-31-2002	Vaid et al.	
	A65	US 5878231	03-02-1999	Baehr et al.	
	A66	US 6088451	07-11-2000	He et al.	
	A67	US 6275693	08-14-2001	Lin et al.	
	A68	US 20020112186	08-15-2002	Ford et al.	
	A69	US 20020123335	09-05-2002	Luna et al.	
	A70	US 20020138763	09-26-2002	Delany et al.	
	A71	US 6205552	03-20-2001	Fudge	
	A72	US 6477143	11-05-2002	Ginossar	
	A73	US 6092200	07-18-2000	Muniyappa et al.	
	A74	US 6516417	02-04-2003	Pegrum et al.	
	A75	US 20030135753	07-17-2003	Batra et al.	
	A76	US 6735691	05-11-2004	Capps et al.	
	A77	US 20020199007	12-01-2002	Clayton et al.	
	A78	US 20030149751	08-07-2003	Bellinger et al.	
	A79	US 20030159072	08-21-2003	Bellinger et al.	
	A80	US 20030217126	11-20-2003	Polcha et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	5	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A81	US 20040049586	03-11-2004	Ocepek et al.	
	A82	US 20050193103	09-01-2005	Drabik, John	
	A83	US 5896499 A	04-20-1999	McKelvey	
	A84	US 6804783	10-12-2004	Wesinger et al.	
	A85	US 7181017	02-20-2007	Nagel et al.	
	A86	US 20020075844	06-01-2002	Hagen	
	A87	US 20040199635	10-07-2004	Ta et al.	
	A88	US 20050204168	09-15-2005	Johnston et al.	
	A89	US 20030212800	11-01-2003	Jones et al.	
	A90	US 6757740	06-01-2004	Parekh et al.	
	A91	US 20020029260	03-01-2002	Dobbins et al.	
	A92	US 20030069956	04-01-2003	Gieske et al.	
	A93	US 20030163603	08-01-2003	Fry et al.	
	A94	US 20030177477	09-01-2003	Fuchs	
	A95	US 20040268234	12-01-2004	Sampathkumar et al.	
	A96	US 6708212	03-16-2004	Porras et al.	
	A97	US 7272646	09-18-2007	Cooper et al.	
	A98	US 6785252	08-31-2004	Zimmerman et al.	
	A99	US 6823385	11-23-2004	McKinnon et al.	
	A100	US 6917622	07-12-2005	McKinnon et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	6	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A101	US 20010038639	11-08-2001	McKinnon et al.	
	A102	US 20010038640	11-08-2001	McKinnon et al.	
	A103	US 20010038645	11-08-2001	McKinnon et al.	
	A104	US 20010039582	11-08-2001	McKinnon et al	
	A105	US 7013331	03-14-2006	Das	
	A106	US 20030055994	03-20-2003	Herrmann et al.	
	A107	US 7143283	11-28-2006	Chen et al.	
	A108	US 7146639	12-05-2006	Bartal et al.	
	A109	US 6636894	10/21/2003	Short et al	
	A110	US 6789110	09-07-2004	Short et al.	
	A111	US 7120934	10-10-2006	Ishikawa	
	A112	US 7185368	02-27-2007	Copeland III	
	A113	US 7266754	09-04-2007	Shah	
	A114	US 7454792	11-18-2008	Cantrell et al.	
	A115	US 20030061506	03-27-2003	Cooper	
	A116	US 20030154399	08-14-2003	Zuk	
	A117	US 20040015719	01-22-2004	Lee	
	A118	US 20040047356	03-11-2004	Bauer	
	A119	US 20040085906	09-19-2008	Ohtani	
	A120	US 20040093513	05-13-2004	Cantrell	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	7	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A121	US 20040172557	09-02-2004	Nakae et al.	
	A122	US 20050044422	02-24-2005	Cantrell	
	A123	US 20050091303	04-28-2005	Suzuki	
	A124	US 20050149721	07-07-2005	Lu	
	A125	US 20060168229	07-27-2006	Shim, et al.	
	A126	US 6732179	05-04-2004	Brown et al.	
	A127	US 6678733	01-13-2004	Brown et al.	
	A128	US 7324947	01-29-2008	Jordan et al	
	A129	US 7325042	01-29-2008	Soscia et al.	
	A130	US 7406530	07-29-2008	Brown et al.	
	A131	US 7420956	09-02-2008	Karaoguz et al.	
	A132	US 20020131404	09-19-2002	Mehta et al.	
	A133	US 20030041104	02-27-2003	Wingard et al.	
	A134	US 20030070170	04-10-2003	Lennon	
	A135	US 20030078784	04-24-2003	Jordan et al.	
	A136	US 20030126608	07-03-2003	Safadi et al.	
	A137	US 20040064836	04-01-2004	Ludvig et al.	
	A138	US 20040073941	04-15-2004	Ludvig et al.	
	A139	US 20040103426	05-27-2004	Ludvig et al.	
	A140	US 20040122956	06-24-2004	Myers et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	8	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A141	US 20040179822	09-16-2004	Tsumagari et al.	
	A142	US 20040181816	09-16-2004	Kim et al.	
	A143	US 20040210633	10-21-2004	Brown et al.	
	A144	US 20050195854	09-08-2005	Agmon et al.	
	A145	US 20060184618	08-17-2006	Kurup et al.	
	A146	US 20070073718	03-29-2007	Ramer et al.	
	A147	US 20070186113	08-09-2007	Cuberson et al.	
	A148	US 20070208936	09-06-2007	Ramos Robles	
	A149	US 20070268878	11-22-2007	Clements	
	A150	US 20080066096	03-13-2008	Wollmershauser et al.	
	A151	US 20080120661	05-22-2008	Ludvig et al.	
	A152	US 20080147840	06-19-2008	Roelens et al.	
	A153	US 20080276305	11-06-2008	Chan et al.	
	A154	US 20060173992	08-03-2006	Weber et al.	
	A155	US 20030046370	03-06-2003	Courtney	
	A156	US 20050021686	01-27-2005	Jai et al.	
	A157	US 20030059038	03-27-2003	Meyerson et al.	
	A158	US 20030172167	09-11-2003	Judge et al.	
	A159	US 20040177276	09-05-2004	MacKinnon et al.	
	A160	US 20050044350	02-24-2005	White et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	9	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A161	US 20050204022	09-15-2005	Johnston et al.	
	A162	US 20050204031	09-05-2005	Johnston et al.	
	A163	US 20050204050	09-15-2005	Turley	
	A164	US 20050204402	09-15-2005	Turley et al.	
	A165	US 20060036723	02-16-2006	Yip et al.	
	A166	US 20050138416	06-23-2005	Qian et al.	
	A167	US 20050204169	09-15-2005	Tonnesen	
	A168	US 20020090089	07-11-2002	Branigan	
	A169	US 6199113	03-06-2001	Alegre et al.	
	A170	US 7509625	03-24-2009	Johnston et al.	
	A171	US 6219706	04-17-2001	Fan et al.	
	A172	US 7624438	11-24-2009	White	
	A173	US 7587512	09-08-2009	Ta et al.	
	A174	US 7610621	10-27-2009	Turley et al.	
	A175	US 7590728	09-15-2009	Tonnesen et al.	
	A176	US 20020138631	09-26-2002	Friedel et al.	
	A177	US 7665130	02-16-2010	Johnston et al.	
	A178	US 6226752	05-01-2001	Gupta et al.	
	A179	US 6631416	10-07-2003	Bendinelli et al.	
	A180	US 6763468	07-13-2004	Gupta et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	10	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A181	US 7085854	08-01-2006	Keane et al.	
	A182	US 7143435	11-28-2006	Droms et al.	
	A183	US 7181542	02-20-2007	Tuomenoksa et al.	
	A184	US 7181766	02-20-2007	Bendinelli et al.	
	A185	US 7194554	03-20-2007	Short et al.	
	A186	US 7290288	10-30-2007	Gregg et al.	
	A187	US 7316029	01-01-2008	Parker et al.	
	A188	US 7324551	01-29-2008	Stammers	
	A189	US 7448075	11-04-2008	Morand et al.	
	A190	US 20020023210	02-21-2002	Tuomenoksa et al.	
	A191	US 20020026503	02-28-2002	Bendinelli et al.	
	A192	US 20020026531	02-28-2002	Keane et al.	
	A193	US 20020029276	03-07-2002	Bendinelli et al.	
	A194	US 20020053031	05-02-2002	Bendinelli et al.	
	A195	US 20020056008	05-09-2002	Keane et al.	
	A196	US 20020091859	07-11-2002	Tuomenoksa et al.	
	A197	US 20020099829	07-25-2002	Richards et al.	
	A198	US 20030115247	06-19-2003	Simpson et al.	
	A199	US 20030182420	09-25-2003	Jones et al.	
	A200	US 20040083295	04-29-2004	Amara et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 11 of 12

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A201	US 20040215957	10-28-2004	Moineau et al.	
	A202	US 20050021975	01-27-2005	Liu	
	A203	US 7310613	12-18-2007	Briel et al.	
	A204	US 20030110073	06-12-2003	Briel et al.	
	A205	US 20100192213	07-29-2010	Ta et al.	
	A206	US 20040268149	12-30-2004	Aaron	
	A207	US 20030212900	11-13-2003	Liu et al.	
	A208	US 20020133586	09-12-2002	Shanklin et al.	
	A209	US 7386888	06-10-2008	Liang et al.	
	A210	US 6266774	07-24-2001	Sampath et al.	
	A211	US 6502135	12-31-2002	Munger et al.	
	A212	US 6839759	01-04-2005	Larson et al.	
	A213	US 7188180	03-06-2007	Larson et al.	
	A214	US 7418504	08-26-2008	Larson et al.	
	A215	US 7490151	02-10-2009	Munger et al.	
	A216	US 20040064351	04-01-2004	Mikurak	
	A217	US 20040064560	04-01-2004	Zhang et al.	
	A218	US 6834341	12-21-2004	Bahl et al.	
	A219	US 20050066200	03-24-2005	Bahl et al.	
	A220	US 20050138358	06-23-2005	Bahl et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	12	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A221	US 20060168454	07-27-2006	Venkatachary et al.	
	A222	US 7092727	08-15-2006	Li et al.	
	A223	US 7444669	10-28-2008	Bahl et al.	
	A224	US 7185358	02-27-2007	Schreiber et al.	
	A225	US 7085385	08-01-2006	Frantz et al.	
	A226	US 6907530	06-14-2005	Wang	
	A227	US 5623601	04-22-1997	Vu	
	A228	US 20030123442	07-03-2003	Drucker et al.	
	240	US 6996625	02-07-2006	Kaplan et al.	
	241	US 20040107290	06-03-2004	Kaplan et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

OPAP
AUG 2 9 2011
IAP21
PATENT & TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 11

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C1	LINGBLOM, MARIE, "Bluesocket's New Gateway Based on Open Standards -- WGX-4000 Switch Wireless Gateway, CRN, Burlington, MA, found at www.crn.channelsupersearch.com, 4-21-2003, 2 pgs.	
	C2	"Boingo Wireless Service Installed at LaGuardia Airport," 06/17/2003, Copyright 2003 M2Communications Ltd., found at www.findarticles.com, 12-08-2003, 1 pg.	
	C3	"West Point Unwired: the Military Academy at West Point Continues to Lead the Way in High-Tech Curriculum with Wireless Classroom Networking," Communication News, June 2003, Copyright 2003 M2 Communications Ltd., found at www.findarticles.com, 5 pgs., printed 12/8/03.	
	C4	MOLTA, DAVE, "Wireless Hotspots Heat Up," Mobile & Wireless Technology, pp.1-8, 05/15/2003, Copyright 2003 M2Communications Ltd., found at www.networkcomputing.com, printed 12/08/2003, 8 pgs..	
	C5	JACKSON, WILLIAM, "Wireless at West Point: Officers of the Future Use IT in Class Now, in the Field Later (Technology Report)," 04/21/2003, GCN, pp.1-3, www.gcn.com.	
	C6	LINGBLOM, MARIE, "Cranite Develops SMB Strategy, CRN, San Jose, CA, June 23, 2003, 2 pgs.	
	C7	DORNAN, ANDY "Wireless LANs: Freedom vs. Security?" Network Magazine, July 2003, pps. 36-39, www.networkmagazine.com.	
	C8	O'SHEA, DAN, "PCTEL looks past patent suit toward fusion of Wi-Fi, PC" Telephony.online, 06/02/2003, pp. 1-2, found at www.telephonyonline.com, Primedia Business Magazines and Media, printed 12/08/2003.	
	C9	O'SHEA, DAN, "Boingo to Launch Initiative Aimed at Carrier Market" Telephony.online, 03/10/2003, 1 pg., found at www.telephonyonline.com, Primedia Business Magazines and Media, printed 12/08/2003.	
	C10	International Search Report for International Patent Application No. PCT/US03/32912, completed 03/22/2004, mailed 04/08/2004, 6 pgs.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	2	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C11	International Search Report for International Patent Application No. PCT/US03/32268, completed 10/17/2004, mailed 10/29/2004, 6 pgs.	
	C12	FAN, CHEN, et al, "Distributed Real Time Intrusion Detection System for 3G," Proceedings of ICCC2004, 2004, pp. 1566-70.	
	C13	YU, ZHAO-xu et al., "Fuzzy Logic Based Adaptive Congestion Control Scheme for High-Speed Network," Vol. 33, No. 4, Information and Control, August 2004, pp. 389-93 (with English abstract).	
	C14	HAMANO, TAKAFUMI et al., "A Redirection-Based Defense Mechanism Against Flood-Type Attacks in Large Scale ISP Networks," 10th Asia-Pacific Conf. on Comm. and 5th Int'l Symposium on Multi-Dimensional Mobile Comm., 2004, pp. 543-547, IEEE #07803-8601-09/04.	
	C15	SAROLAHTI, PASI, "Congestion Control on Spurious TCP Retransmssion Timeouts," Globecom 2003, pp. 682-686, IEEE #0-7803-7974-8.	
	C16	ESTEVEZ-TAPIADOR, JUAN M., et al., "Measuring Normality in HTTP Traffic for Anomaly-Based Intrusion Detection," Computer Networks 45 (2004), pp. 175-193, available at www.sciencedirect.com, El Sevier 2004 #13891286.	
	C17	XING, XU-JIA, et al., "A Survey of Computer Vulnerability Assessment," Chinese Journal of Computers, Vol. 27, No. 1, Jan. 2004, pp. 1-11 (with English abstract).	
	C18	WEN et al. "Development of a Snort-Based Security Network Management and Real-Time Intrusion Detection System," Journal of Beijing Normal Univ. (Natural Science), Vol. 40, No. 1, February 2004, pp. 40-43 (with English abstract).	
	C19	THOTTETHODI, METHUNE, et al., "Exploiting Global Knowledge to Achieve Self-Tuned Congestion Control for k-Ary n-Cube Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 15, No. 3, March 2004, pp. 257-272, IEEE #1045-9219/04.	
	C20	TRABELSI, ZOUHEIR, et al., "Malicious Sniffing Systems Detection Platform," 2004 IEEE, pp. 201-207, IEEE #0-7695-2068-5/04.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	3	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C21	GUANGZHI, QU, et al., "A Framework for Network Vulnerability Analysis," Proceedings of the IASTED Int'l Conf., Comm., Internet & Information Tech., November 18-20, 2004, St. Thomas, US Virgin Islands, pp. 289-294.	
	C22	ALBUQUERQUE, CELIO, et al., "Network Border Patrol: Preventing Congestion Collapse and Promoting Fairness in the Internet," IEEE/ACM Transactions on Networking, Vol. 12, No. 1, February 2004, pp. 173-186, IEEE #1063-6692/04.	
	C23	WIRBEL, LORING, "Security Stampede Could Flatten IPSec," Network Magazine, January 2004, p. 12, available at www.networkmagazine.com.	
	C24	MACLEOD, CALUM, "Freeing the Shackles with Secure Remote Working," Comtec, October 2003, pp. 66-67.	
	C25	FISHER, DENNIS, "SSL Simplifies VPN Security," IT Week, 11/10/2003, pg. 40, available at www.eweek.com/security.	
	C26	CONRY-MURRAY, ANDREW, "SSL VPNs: Remote Access for the Masses," Network Magazine, October 2003, pp. 26-32, available at www.networkmagazine.com.	
	C27	"Permeo Supports Microsoft Network Access Protection for Simplified Secure Remote Access; Permeo's Base5 Support of Microsoft Technology Provides "Zero Touch" Policy Enforcement", 04/25/2005, 2 pgs., Newswire, found at www.nerac.com. #NDN-121-0552-8254-9.	
	C28	"Permeo Drives Out Operational Costs, Simplifies Secure Remote Access, 03/25/2005, 2 pgs., Newswire, found at www.nerac.com. #NDN-121-0549-5967-5.	
	C29	"Netilla Lauches SSL VPN for Citrix. (Industry Briefs) (Virtual Private Networks) (Brief Article)," 09/20/2004, 2 pgs., Computer Reseller News, found at www.nerac.com. #NDN-218-0991-7652-9.	
	C30	"Netilla Lauches Secure Gateway Appliance Family of Application-Specific SSL VPN Products; Initial SGA-C Model Provides Secure Remote Access to Citrix MetaFrame Presentation Server Installations..." 09/13/2004, 3 pgs., PR Newswire, found at www.nerac.com. #NDN-218-0987-0667-2.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	4	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C31	"Secure Remote Access.(Network Security) (VPN Gateway 4400 Series) (Brief Article)," March 1, 2004, 2 pgs., Communication News, Vol. 41, found at www.nerac.com. #NDN-218-0925-2711-6.	
	C32	"Fortinet and Aventail Deliver Joint Solution for Clientless Remote Access with High-Performance Antivirus Protection; Integrated SSL VPN and Antivirus Offering Provides Clientless Remote Access with Complete Content Security", 01/05/2004, 3 pgs., PR Newswire, found at www.nerac.com. #NDN-218-0845-8319-2	
	C33	HAMBLEN, MATT, "Cisco Targets SSL VPN Vendors, Adds Support for Clientless Security Protocol: Installed Base of VPN Devices May Give it an Edge, Despite Late Entry," 11/17/2003, 3 pgs., Computerworld, Vol. 37, No. 46, found at www.nerac.com. #NDN-218-0841-5076-0.	
	C34	HAMZEH, K., et al., "Point-to-Point Tunneling Protocol--PPTP RFC 2637" Network Working Groups, July 1999, pp. 1-54, Microsoft Corporation.	
	C35	International Search Report and Written Opinion for International Patent Application No. PCT/US04/29249, completed 11/28/2005, mailed 12/15/2005, 10 pgs.	
	C36	PFLEEGER, CHARLES P., Computer Network Security, Security in Computing, 1989, pp. 364-415, Ch. 10, PTR Prentice-Hall, Inc., Englewood Cliffs, NJ.	
	C37	Office Action for U.S. Patent Application No. 10/922,041, mailed 07/13/2007, 20 pgs.	
	C38	STONE, DAVID, "Securing Wireless LANs with VPN", Intel Information Technology White Paper, Intel Corp., May 2006, 8 pgs. Order N#313185-001US.	
	C39	Office Action for U.S. Patent Application No. 10/683,317, mailed 10/09/2007, 20 pgs.	
	C40	Office Action for U.S. Patent Application No. 10/687,002, mailed 10/18/2007, 10 pgs.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	5	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C41	Office Action for U.S. Patent Application No. 11/078,223, mailed 10/31/2007, 8 pgs.	
	C42	Office Action for U.S. Patent Application No. 11/076,652, mailed 01/25/2008, 9 pgs.	
	C43	Office Action for U.S. Patent Application No. 10/687,002, mailed 04/17/2008, 12 pgs.	
	C44	Office Action for U.S. Patent Application No. 10/683,317, mailed 06/09/2008, 15 pgs.	
	C45	Office Action for U.S. Patent Application No. 11/076,672, mailed 07/09/2008, 12 pgs.	
	C46	Office Action for U.S. Patent Application No. 11/076,652, mailed 07/22/2008, 8 pgs.	
	C47	Office Action for U.S. Patent Application No. 11/076,591, mailed 08/13/2008, 10 pgs.	
	C48	Office Action for U.S. Patent Application No. 11/076,719, mailed 09/04/2008, 7 pgs.	
	C49	SBC TECHNOLOGY RESOURCES, INC., XNMP-XML Network Management Protocol and Interface, 07-19-2002, pp.1-9, http://www.ietf.org/proceedings/02jul/slides	
	C50	Shim, Choon B., " XNMP for IP Telephony Management," Enterprise Networks & Servers, June 2, 2006, 7 pgs.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	6	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C51	Office Action for U.S. Patent Application No. 11/076,652, mailed 12/11/2008, 8 pgs.	
	C52	Office Action for U.S. Patent Application No. 10/687,002, mailed 01/07/2009, 14 pgs.	
	C53	Office Action for U.S. Patent Application No. 11/076,672, mailed 02/03/2009, 10 pgs.	
	C54	Oh, et al., "Interaction Translation Methods for XML/SNMP Gateway," July 11, 2003, retrieved from http://web-archive.org/web/20030711162412/http://dpnm.postech.ac.kr/papers/DSOM/02/xml-snmp-gateway/xml-snmp-gateway.pdf, pgs. 1-12.	
	C55	Office Action for U.S. Patent Application No. 10/683,317, mailed 02/11/2009, 17 pgs.	
	C56	Office Action for U.S. Patent Application No. 11/076,591, mailed 02/13/2009, 26 pgs.	
	C57	International Preliminary Report on Patentability for International Patent Application No. PCT/US03/032268 completed 1/4/2005, 3 pgs.	
	C58	International Preliminary Report on Patentability for International Patent Application No. PCT/US03/032912 completed 06/28/2004, 3 pgs.	
	C59	International Preliminary Report on Patentability (Ch. I) of the International Searching Authority for International Patent Application No. PCT/US04/029249 issued 02/21/2006, 6 pgs.	
	C60	Office Action for U.S. Patent Application No. 11/076,719, mailed 03/17/2009, 8 pgs.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	7	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C61	Office Action for U.S. Patent Application No. 10/922,041, mailed 12/06/2005, 10 pgs.	
	C62	Office Action for U.S. Patent Application No. 10/922,041, mailed 03/30/2006, 18 pgs.	
	C63	Office Action for U.S. Patent Application No. 10/922,041, mailed 08/11/2006, 19 pgs.	
	C64	Office Action for U.S. Patent Application No. 10/922,041, mailed 01/30/2007, 20 pgs.	
	C65	Office Action for U.S. Patent Application No. 10/683,317, mailed 04/05/2007, 6 pgs.	
	C66	Office Action for U.S. Patent Application No. 10/687,002, mailed 05/02/2007, 10 pgs.	
	C67	Office Action for U.S. Patent Application No. 10/922,041, mailed 05/08/2009, 13 pgs.	
	C68	Office Action for U.S. Patent Application No. 11/076,672, mailed 07/21/2009, 11 pgs.	
	C69	Notice of Allowability for U.S. Patent Application No. 11/076,646, mailed 07/24/2009, 7 pgs.	
	C70	CRANDELL ET AL., "A Secure and Transparent Firewall Web Proxy," October 2003, USENIX, Retrieved from the internet on 7/15/09: <URL: http://www.usenix.org/event/lisa03/tech/full_papers/crandell/crandell.pdf>	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	8	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C71	SOMMERLAD, "Reverse Proxy Patterns," 2003 Retrieved from the Internet on 7/15/09, 27 pages; <URL: http://www.modsecurity.org/archive/ReverseProxy-book-1.pdf>	
	C72	Office Action for U.S. Patent Application No. 11/076,591, mailed 08/06/2009, 29 pgs.	
	C73	Office Action for U.S. Patent Application No. 10/683,317, mailed 08/18/2009, 17 pgs.	
	C74	RASHTI et al, "A Multi-Dimensional Packet Classifier for NP-Based Firewalls," Proceedings of the 2004 Int'l Symposium on Applications and the Internet, January 2004, 5 pages, from the internet, printed 08/12/2009: <URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1266123&isnumber=28312>.	
	C75	WILLIAMSON, Matthew, "Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code," Proceedings of the 18th Annual Computer Security Applications Conference, 2002 IEEE, 8 pages.	
	C76	WILLIAMSON, et al, "Virus Throttling," Virus Bulletin Research Feature 1, March 2003, 4 pgs.	
	C77	Office Action for U.S. Patent Application No. 11/076,672, mailed 01/07/2010, 9 pgs.	
	C78	Office Action for U.S. Patent Application No. 11/076,591, mailed 02/02/2010, 34 pgs.	
	C80	Office Action for U.S. Patent Application No. 11/076,591, mailed 07/20/2010, 33 pgs.	
	C81	Office Action for U.S. Patent Application No. 10/683,317, mailed 07/23/2010, 9 pgs.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	9	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C82	Office Action for U.S. Patent Application No. 12/506,140, mailed 09/01/2010, 11 pgs.	
	C90	"Discussion of Conceptual Difference Between Cisco IOS Classic and Zone-Based Firewalls," October 2007, Cisco Systems, Inc., San Jose, CA, 4 pgs.	
	C91	Cisco IOS Firewall Zone-Based Policy Firewall, Release 12.4(6)T, Technical Discussion, February 2006, 77 pgs., Cisco Systems, Inc., San Jose, CA.	
	C92	Zone-Based Policy Firewall Design and Application Guide, Document ID: 98628, 09/13/2007, 49 pgs., Cisco Systems, Inc., San Jose, CA	
	C93	SP MAJ, W MAKAIRANONDH, D VEAL, "An Evaluation of Firewall Configuration Methods," IJSCSNS International Journal of Computer Science and Network Security, Vol. 10, No. 8, August 2010, 7 pgs.	
	C94	Using VPN with Zone-Based Policy Firewall, May 2009, Cisco Systems, Inc., San Jose, CA, 10 pgs.	
	C95	Cisco IOS Firewall Classic and Zone-Based Virtual Firewall Application Configuration Example, Document ID: 100595, February 12, 2008, 20 pgs., Cisco Systems, Inc., San Jose, CA.	
	C96	Class-Based Policy Provisioning: Introducing Class-Based Policy Language (CPL), August 2008, 36 pgs., Cisco Systems, Inc., San Jose, CA.	
	C97	Cisco IOS Zone Based Firewall Example, at http://www.linickx.com/archives/2945/cisco-ios-zon..., printed 12/07/2010, 6 pgs., LINICKX.com.	
	C98	Zone-Based Policy Firewall, Published 02/22/2006, Updated 06/19/2006, 46 pgs., Cisco Systems, Inc., San Jose, CA.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	10	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C99	Applying Zone-based Firewall Policies in Cisco Security Manager, Published March 2009, Revised September 2009, Cisco Systems, Inc., San Jose, CA.	
	C100	"FreeBSD Handbook, Chapter 30 Firewalls," 2003, found at www.freebsd.org/doc/handbook/firewalls-ipfw.html, printed 12/27/2010, 13 pgs.	
	C101	WATTERS, Paul, "Solaris 8 Administrator's Guide, Chapter 4, Network Configuration," O'Reilly & Associates, Inc., January 2002, 17 pgs.	
	C102	SPITZNER, Lance, "Configuring network interface cards; getting your interfaces to talk," March 23, 2004, 4 pgs.	
	C103	GITE, Vivek, "Redhat/CentOS/Fedora Linux Open Port," September 13, 2007, found at www.cyberciti.biz/faq/howto-rhel-linux-open-port-using-iptables/ printed 01/03/2011, 7 pgs.	
	C105	Office Action for U.S. Patent Application No. 10/683,317, mailed 01/03/2011, 12 pgs.	
	C106	Office Action for U.S. Patent Application No. 12/617,211, mailed 02/03/2011, 14 pgs.	
	C107	"Managing Firewall Services," User Guide for Cisco Security Manager 3.3.1, October 2009, Ch. 11, 90 pgs., Cisco Systems, Inc., San Jose, CA.	
	C108	"Cisco Common Classification Policy Language," Cisco Router and Security Device Manager 2.4 User's Guide, Ch. 34, 2007, 32 pgs., Cisco Systems, Inc., San Jose, CA.	
	C109	Guide to User Documentation for Cisco Security Manager 4.0, June 18, 2010, Cisco Systems, Inc., San Jose, CA.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	11	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C110	Cisco Configuration Professional: Zone-Based Firewall Blocking Peer to Peer Traffic Configuration Example, Document ID: 112237, Updated 12/03/2010, 25 pgs., Cisco Systems, Inc., San Jose, CA	
	C111	Tuning Cisco IOS Classic and Zone-Based Policy Firewall Denial-of-Service Protection, 2006, 10 pgs., Cisco Systems, Inc., San Jose, CA.	
	C112	HOLUSKA, Marty, Using Ciscos IOS Firewalls to Implement a Network Security Policy, Fort Hays State University/INT 490, printed 12/06/2010, 5 pgs., http://quasarint.com/Capstone/zb_policy.php	
	C113	Cisco Feature Navigator, Cisco Systems, Inc., San Jose, CA, printed on 12/02/2010, 4 pgs., at http://tools.cisco.com/ITDIT/CFN/Dispatch.	
	C114	Office Action for U.S. Patent Application No. 12/506,140, mailed 02/18/2011, 13 pgs.	
	C118	Office Action for U.S. Patent Application No. 12/617,211, mailed 07/19/2011, 18 pgs.	
	C119	Office Action for U.S. Patent Application No. 12/506,140, mailed 08/04/2011, 18 pgs.	

Examiner Signature		Date Considered	

OPAP
AUG 2 9 2011
IAP21
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
CERTIFICATE OF MAILING	Atty Docket No. **ROCK1150-3**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In the Application of: **Patrick Turley**
Filing or 371(c) Date: **April 22, 2011**
Title: **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**

Certification Under 37 C.F.R. §1.8

I hereby certify that the Information Disclosure Statement with references is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: MAIL STOP Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **August** 17**, 2011.**

Signature

K. Jacobson

Printed Name

B1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 587 522 A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 93480121.8

(22) Date of filing: 24.08.93

(51) Int. Cl.[5]: H04L 12/56

(30) Priority: 10.09.92 US 943097

(43) Date of publication of application:
16.03.94 Bulletin 94/11

(84) Designated Contracting States:
DE FR GB

(71) Applicant: International Business Machines Corporation
Old Orchard Road
Armonk, N.Y. 10504 (US)

(72) Inventor: Ahmadi, Hamid
156 Mitchell Road
Somers, New York 10589 (US)
Inventor: Guerin, Roch A.
Rochambeau Drive, Scenic View No. 4H
Yorktown Heights, New York 10598 (US)
Inventor: Derby, Jeffrey Haskell
104 Foxridge Court
Chapel Hill, North Carolina 27514 (US)
Inventor: Gun, Levent
4324 Swarthmore Road
Durham, North Carolina 27707 (US)
Inventor: Marin, Gerald Arnold
3704 Sweeten Creek Road
Chapel Hill, North Carolina 27514 (US)
Inventor: Naghshineh, Mamoud
74 Mountain View Road
Fishkill, New York 12524 (US)
Inventor: Sohraby, Khosrow
9 Oakridge Circle
Mahopac, New York 10598 (US)

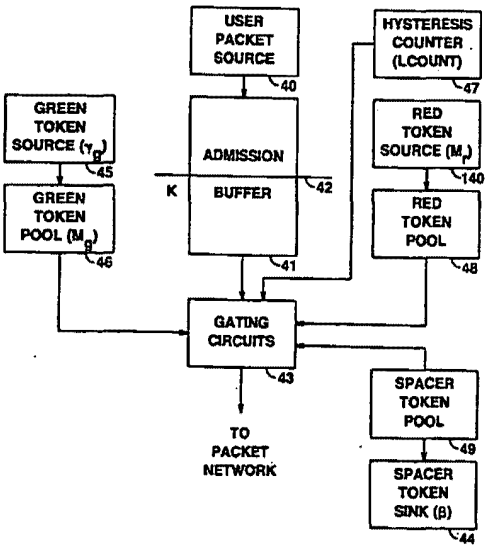
(74) Representative: de Pena, Alain
Compagnie IBM France Département de Propriété Intellectuelle
F-06610 La Gaude (FR)

(54) Rate-based congestion control in packet communications networks.

(57) A congestion control system for packet communications networks in which access to the network is controlled to prevent such congestion. Packets within the pre-specified statistical description of each packet source are marked as high priority ("green" packets) while packets exceeding the pre-specified characteristics are marked with a lower priority ("red" packets). The overall red packet rate is limited to prevent red packet saturation of the network. The introduction of red packets into the network is subjected to a degree of hysteresis to provide better interaction with higher layer error recovery protocols. The amount of hysteresis introduced into the red packet marking can be fixed or varied, depending on the statistics of the incoming data packets at the entry point to the network.

FIG. 3

LEAKY BUCKET ACCESS CONTROL WITH STATIC HYSTERESIS



EP 0 587 522 A2

TECHNICAL FIELD

This invention relates to packet communications networks and, more particularly, to the control of user access to the network in order to minimize congestion in such networks.

BACKGROUND OF THE INVENTION

In high-speed packet switching networks, several classes of traffic share the common resources of the network. Multimedia services such as text, image, voice and video generate traffic at widely varying rates. The traffic characteristics of such different sources, moreover, vary dramatically over time. The transport network must nevertheless guarantee a bandwidth and a quality of service to each connection regardless of these differences. Managing the available bandwidth to avoid congestion and to provide such guaranteed Grades of Service (GOS) for connections with potentially dramatic differences in their statistical behavior is therefore of extreme importance in such networks. For example, while data traffic can usually be slowed down in order to cope with network congestion, real time traffic, such as voice, video or image, has an intrinsic rate determined by external factors; the ability to slow down such sources is usually very limited. Real time traffic therefore requires some level of guaranteed service and hence the allocation of resources for such connections is mandatory. The traffic must be managed, not only to guarantee the availability of resources such as link bandwidth, buffer space, switch capacity, processing resources, and so forth, but also to allocate these resources among the contending traffic streams in a "fair" manner. Network resources are finite, valuable and must be utilized in an optimal manner.

Conventional mechanisms for controlling congestion in a network rely on end-to-end control messages for regulating the flow of traffic. In high speed networks, however, the propagation delays across the network typically dominate the switching and queuing delays. The congestion control feedback messages from the network are therefore usually so outdated that any action taken by the source in response to such messages is too late to resolve the congestion which caused the messages to be initiated in the first place. Conventional end-to-end congestion control mechanisms are simply incapable of dealing realistically with congestion in today's high speed global networks.

Due to the stochastic nature of the packet arrival process, for transitory periods during the connection, the parameters of a source vary from the values determined at the connection setup time. In addition, congestion may arise in the network for brief periods during the course of the connection due to statistical variances in the multiplexing process. It is therefore important not only to regulate the access to the network at the source, but also to regulate traffic flow within the network by buffer management and scheduling functions. These traffic regulation mechanisms enforce the pre-specified classes of service. Since all congestion control procedures used in high speed networks must be available in real time, however, such procedures must be computationally simple.

In order to achieve these goals, the network must regulate the rate of traffic flow from each source into the network. Such rate-based access control mechanisms are preferable over link-by-link flow controls because such access control mechanisms maximize the speed of information transfer over the network. One well-known congestion preventive rate-based access control technique is based on the so-called buffered "leaky bucket" scheme. Such leaky bucket schemes restrict the data transmission, on the average, to the allowable rate, but permit some degree of burstiness diverging from the average. Leaky bucket schemes are disclosed in "Congestion Control Through Input Rate Regulation," by M. Sidi, W-Z. Liu, I. Cidon and I. Gopal, Proceedings of Globecom '89, pages 49.2.1-49.2.5, Dallas, 1989, "The 'Leaky Bucket' Policing Method in the ATM (Asynchronous Transfer Mode) Network," by G. Niestegge, International Journal of Digital and Analog Communications Systems, Vol. 3, pages 187-197, 1990, and "Congestion Control for High Speed Packet Switched Networks," by K. Bala, I. Cidon and K. Sohraby, Proceedings of Infocom '90, pages 520-6, San Francisco, 1990. Some of these leaky bucket congestion control schemes involve the marking of packets entering the network to control the procedures used in the network in handling those packets.

In the Bala et al. article, for example, packets leaving a source are marked with one of two different "colors," red and green. Green packets represent traffic that is within the connection's reserved bandwidth, and are guaranteed a pre-specified grade of service based on some level of delay and loss probability within the network. The green packets are therefore transmitted at a rate determined at call setup time. Red packets, on the other hand, represent traffic sent over and above the reserved rate and can be viewed as an emergency relief mechanism coming into play during an overload period where the instantaneously offered traffic is above the reserved bandwidth. In other words, the amount of traffic in excess of the allocated bandwidth is marked red and sent into the network, instead of being dropped at the source. Red packets allow a source to exploit any unused network bandwidth in order to improve the efficiency of the statistical multiplexing.

The network nodes operate to store and forward packets. Green and red packets are treated differently, however. The intermediate nodes will discard red packets first at times of congestion, using a low dis-

FORTINET EX1002 Page 88

card threshold. As a result, red packets have a higher loss probability at the intermediate nodes, and, moreover, do not degrade the performance of the green packets to any significant extent.

One leaky bucket mechanism is described in detail in the copending application of the present EP-A-No. 93480099.6, filed on 16 July 1993 and assigned to applicants' assignee. It is of considerable importance in leaky bucket access control schemes that the red packets do not degrade the performance of the green packets. Moreover, it is also desirable that the red packets make as much use as possible of the available bandwidth on the network. For example, if the amount of red traffic is not controlled, it is possible that the red packets can destructively interfere with each other, resulting in a lower red packet throughput than the network would have otherwise permitted. These problems are of extreme concern in very large national or international networks where traffic is heavy, demand great and the efficiency of the network of paramount importance.

SUMMARY OF THE INVENTION

In accordance with the illustrative embodiment of the present invention, a buffered leaky bucket access control mechanism is provided for access to a packet network using a packet marking scheme. Packets within the reserved bandwidth of the connection are marked with a high ("green") priority marking while packets not within the reserved bandwidth of the connection are marked with a lower ("red") priority marking. More particularly, in accordance with the illustrative embodiment of the present invention, the bandwidth available to the red packets in the leaky bucket access control mechanism is controlled for every connection to prevent saturation of the network with such red packets. Such saturation would cause the red packets to interfere with each other and with the higher priority green packets. Furthermore, in order to improve interaction with higher layer error recovery protocols, a certain amount of hysteresis is built into the packet marking mechanism. That is, it is arranged such that several low priority red packets are transmitted back-to-back instead of continuously alternating between red and green packets.

In accordance with a first embodiment of the present invention, a spacer is also used to introduce some spacing between packets and achieve some level of smoothing. At the same time, a red traffic limiter limits the number of red packets which can be transmitted during a given time interval. Meanwhile, a hysteresis counter insures that, once red packet marking is initiated, that such red packet marking continues for a fixed number of data units to form a continuous red packet train. Green packets are, of course, transmitted when enough green tokens are present in a fixed-size green token pool into which green tokens are introduced at a fixed rate. The red traffic limiter prevents the network links from being saturated with red packets while the hysteresis counter avoids too frequent alternations of red and green marking periods.

In accordance with a second embodiment of the present invention, the hysteresis mechanism is made dynamic by substituting a variable number of successive red data units for the fixed number in the first embodiment. The number of such successive red data units, moreover, is dependent on the distribution of the incoming packets. This avoids certain problems that might arise in the first embodiment. For example, if the number of successive red data units is too short, there will not be a sufficient accumulation of green tokens to permit a green packet to be transmitted between bursts of red packets. On the other hand, if the number of successive red data units is too large, the loss probability of the red packets at the intermediate nodes increases.

Another problem can arise with a fixed amount of hysteresis. If the number is large enough to permit adequate green token accumulation and thereby permit adequate separation of red packet bursts, it is possible that the red marking interval will continue after the green token pool is full. In accordance with the second embodiment of the invention, the red marking process is turned off when the number of green tokens has reached a threshold (the green resume threshold) to insure that green packets can be transmitted when the green token pool reaches the threshold. Both embodiments of the present invention have the advantage of optimizing the use of red packets by assembling trains of such red packets while, at the same time, limiting the total number of such red packets in any given period of time.

BRIEF DESCRIPTION OF THE DRAWINGS

A complete understanding of the present invention may be gained by considering the following detailed description in conjunction with the accompanying drawings, in which:

FIG. 1 shows a general block diagram of a packet communications system in which the buffered leaky bucket mechanisms in accordance with the present invention might find use;

FIG. 2 shows a more detailed block diagram of typical decision point in the network of FIG. 1 at which packets enter the network or are forwarded along the route to a destination for that packet, and at which a leaky bucket mechanism in accordance with the present invention would be located;

FIG. 3 shows a general block diagram of a buffered leaky bucket access mechanism in accordance with the present invention using a fixed value of hysteresis in the red packet marking

FORTINET EX1002 Page 89

process, to be used in the network access controller of FIG. 2;

FIG. 4 shows a flow chart of the operation of the leaky bucket access control mechanism of FIG. 3;

FIG. 5 shows a general block diagram of a buffered leaky bucket access control mechanism in accordance with the present invention using a variable amount of hysteresis in the red packet marking process, to be used in the network access controller of FIG. 2; and

FIG. 6 shows a flow chart of the operation of the leaky bucket access control mechanism of FIG. 5.

To facilitate reader understanding, identical reference numerals are used to designate elements common to the figures.

DETAILED DESCRIPTION

Referring more particularly to FIG. 1, there is shown a general block diagram of a packet transmission system 10 comprising eight network nodes 11 numbered 1 through 8. Each of network nodes 11 is linked to others of the network nodes 11 by one or more communication links A through L. Each such communication link may be either a permanent connection or a selectively enabled (dial-up) connection. Any or all of network nodes 11 may be attached to end nodes, network node 2 being shown as attached to end nodes 1, 2 and 3, network node 7 being shown as attached to end nodes 4, 5 and 6, and network node 8 being shown as attached to end nodes 7, 8 and 9. Network nodes 11 each comprise a data processing system which provides data communications services to all connected nodes, network nodes and end nodes, as well as decision points within the node. The network nodes 11 each comprise one or more decision points within the node, at which incoming data packets are selectively routed on one or more of the outgoing communication links terminated within that node or at another node. Such routing decisions are made in response to information in the header of the data packet. The network node also provides ancillary services such as the calculation of routes or paths between terminal nodes, providing access control to packets entering the network at that node, and providing directory services and maintenance of network topology data bases used to support route calculations and packet buffering.

Each of end nodes 12 comprises either a source of digital data to be transmitted to another end node, a utilization device for consuming digital data received from another end node, or both. Users of the packet communications network 10 of FIG. 1 utilize an end node device 12 connected to the local network node 11 for access to the packet network 10. The local network node 11 translates the user's data into packets formatted appropriately for transmission on the packet network of FIG. 1 and generates the header which is used to route the packets through the network 10.

In order to transmit packets on the network of FIG. 1, it is necessary to calculate a feasible path or route through the network from the source node to the destination node for the transmission of such packets. To avoid overload on any of the links on this route, the route is calculated in accordance with an algorithm that insures that adequate bandwidth is available for the new connection, using statistical multiplexing techniques. That is, given the statistical properties of each data source, a plurality of signals from such sources are multiplexed on the transmission links A-L, reserving sufficient bandwidth to carry each signal if that signal stays within its statistically described properties. One such algorithm is disclosed in the copending application, Serial Number 07/874,917, filed April 28, 1992, and assigned to applicants' assignee. Once such a route is calculated, a connection request message is launched on the network, following the computed route and updating the bandwidth occupancy of each link along the route to reflect the new connection.

In FIG. 2 there is shown a general block diagram of a typical packet network decision point such as is found in the network nodes 11 of FIG. 1. The decision point of FIG. 2 comprises a high speed packet switching fabric 33 onto which packets arriving at the decision point are entered. Such packets arrive over transmission links via transmission adapters 34, 35, ..., 36, or originate in user applications in end nodes via application adapters 30, 31, ..., 32. It should be noted that one or more of the transmission adapters 34-36 can be connected to intranode transmission links connected to yet other packet switching fabrics similar to fabric 33, thereby expanding the switching capacity of the node. The decision point of FIG. 2 thus serves to connect the packets arriving at the decision point to a local user (for end nodes) or to a transmission link leaving the decision point (for network nodes and end nodes). The adapters 30-32 and 34-36 may include queuing circuits for queuing packets prior to or subsequent to switching on fabric 33. A route controller 37 is used to calculate optimum routes through the network for packets originating at one of the user application adapters 30-32 in the decision point of FIG. 2. Network access controllers 39, one for each connection originating at the decision point of FIG. 2, are used to regulate the launching of packets onto the network so as to prevent congestion. That is, if the transient rate of any connection exceeds the statistical values assumed in making the original connection, the controllers 39 slow down the input to the network so as to prevent congestion. Both route controller 37 and access controllers 39 utilize the statistical description of the new connection in calculating routes or controlling access. These descriptions are stored in topology data base 38. Indeed, network topology data base 38 contains information about all of

FORTINET EX1002 Page 90

the nodes and transmission links of the network of FIG. 1 which information is necessary for controller 37 to operate properly.

The controllers 37 and 39 of FIG. 2 may comprise discrete digital circuitry or may preferably comprise properly programmed digital computer circuits. Such a programmed computer can be used to generate headers for packets originating at user applications in the decision point of FIG. 2 or connected directly thereto. Similarly, the computer can also be used to calculate feasible routes for new connections and to calculate the necessary controls to regulate access to the network in order to prevent congestion. The information in data base 38 is updated when each new link is activated, new nodes are added to the network, when links or nodes are dropped from the network or when link loads change due to the addition of new connections. Such information originates at the network node to which the resources are attached and is exchanged with all other nodes to assure up-to-date topological information needed for route and access control calculations. Such data can be carried throughout the network on packets very similar to the information packets exchanged between end users of the network.

The incoming transmission links to the packet decision point of FIG. 2 may comprise links from local end nodes such as end nodes 12 of FIG. 1, or links from adjacent network nodes 11 of FIG. 1. In any case, the decision point of FIG. 2 operates in the same fashion to receive each data packet and forward it on to another local or remote decision point as dictated by the information in the packet header. The packet network of FIG. 1 thus operates to enable communication between any two end nodes of FIG. 1 without dedicating any transmission or node facilities to that communication path except for the duration of a single packet. In this way, the utilization of the communication facilities of the packet network is optimized to carry significantly more traffic than would be possible with dedicated transmission links for each communication path.

Referring more particularly to FIG. 3, there is shown a general block diagram of the major components of an access control module in accordance with the present invention which may comprise special purpose circuitry, but preferably is embodied in a programmed computer. The access control module of FIG. 3 comprises a user packet source 40 which generates packets of data having a given set of statistical characteristics. These packets are entered into an admission buffer 41 having a length marker 42 which is used to initiate red marking when insufficient green tokens are available. Packets at the head (bottom) of admission buffer 41 leave buffer 41 through gating circuits 43 under the control of green token pool 46, hysteresis counter 47, red token pool 48 and spacer token pool 49. More particularly, the access control circuit of FIG. 3 operates to launch packets into the packet network with green tags so long as the source 40 remains within the statistical parameters originally assigned to source 40, and transmits packets with red tags whenever the source 40 exceeds the originally assigned statistical parameters. To this end, green bucket 46 is loaded with green tokens at a fixed rate from green token source 45 until the green token pool is full. As an added protection, spacer token pool 49 is loaded with a number of spacer tokens proportional to the length of the packet just launched. Spacer tokens are removed from spacer token pool 49 by spacer token sink 44 at a fixed rate (beta). Only when spacer token pool 49 is empty is the next packet allowed to be launched into the packet network, thereby adding a certain level of smoothing of the packet transmission process. When red marking is initiated, hysteresis counter 47 insures that a fixed number of data units are marked as red packets to form a continuous train of red packets in order to better interact with higher layer error recovery protocols. Red token source 140 loads Mr red tokens into red token pool 48 every T period. The limited token count in red token pool 48 limits the number of red data units transmitted during a given time interval to the preselected value Mr, thereby insuring that the red traffic does not saturate the transmission links of the network.

The various parameters used and identified in FIG. 3 can be defined as follows:

- T: The time interval after which the red token pool is refreshed.
- γ_g: The green token generation rate.
- M_g: The size of the green token pool. M_g depends upon the burstiness of the traffic from source 40 and is typically chosen to achieve transparency of the leaky bucket to the user traffic. In general, a large M_g will let more packets enter the network as they arrive (limited only by the rate allowed by the spacer). For a given input traffic, the output green traffic will be smoother as M_g becomes smaller. A small M_g, however, will introduce larger admission delays, or cause a larger number of packets to be marked red. M_g must always be large enough to hold sufficient tokens to permit the transmission of the maximum sized packet. M_g is chosen heuristically to best satisfy these contending requirements.
- β: The rate of emptying the spacer packet pool. β determines the peak rate that the packets may enter the network, and thus affects the smoothness of the packet launching process. If β is equal to the peak input rate, the user packets from source 40 will only be queued in admission buffer 41 if no transmission tokens (red or green) are available. However, in order to protect the network, β may be chosen to be no higher than the slowest link speed in the

FORTINET EX1002 Page 91

packet path. β can be further reduced beyond this level, however, to achieve any desired level of smoothing and reserved bandwidth.

M_r: The total number of red tokens available in time interval T. M_r therefore forms the upper bound on the amount of the user traffic which is marked red when launched on the packet network during the time interval T.

K: The threshold 42 in admission buffer 41 used to initiate red marking when insufficient green tokens are available.

L: The number of tokens which determines the total number of data units that are marked red once red marking is initiated.

Using the definitions given above and the components shown in FIG. 3, the operation of the access control procedure with fixed hysteresis is shown in the flow chart of FIG. 4. In FIG. 4, the leaky bucket access control mechanism with static hysteresis is initiated, starting at start box 50, whenever a user packet reaches the head (bottom) of admission buffer 42. At that time, decision box 51 is entered to determine if the spacer pool 49 is empty. If not, decision box 51 is repeatedly re-entered until the spacer pool 49 is empty. At that time, decision box 52 is entered where it is determined if the red marking flag is off. If so, decision box 53 is entered where it is determined whether enough green tokens have been accumulated in green token pool 46 to accommodate the packet at the head of admission buffer 41. If enough green tokens have been accumulated in green pool 46, box 54 is entered where the packet is marked green and, in box 66, the green pool 46 is updated by subtracting the number N of tokens from the green pool 46 necessary to account for the data units in the green packet. Box 55 is then entered where the green packet is transmitted on the network and the process terminated for that packet in terminal box 56. Start box 50 is re-entered when the next packet arrives at the head of admission buffer 41.

If it is determined in decision box 53 that a sufficient number of green tokens are not available in green pool 46 to accommodate this packet, decision box 57 is entered to determine if the buffer 41 length is less than K, the red marking threshold. If the length of buffer 41 is less than the threshold K, decision box 53 is re-entered to wait for either enough green tokens to be accumulated to accommodate the packet (decision box 53) or the length of the buffer 41 to exceed threshold K (decision box 57). If enough green tokens are accumulated to accommodate the packet before the buffer threshold length K is reached, box 54 is entered to mark the packet green, update the green pool 46 (box 66) and transmit the green packet (box 55). If, however, the buffer length threshold K is reached before enough green tokens are accumulated, box 58 is entered to subtract a fixed hysteresis value L from the red token pool 48. That is, the red token pool is reduced by the number of red tokens needed to transmit the next desired serial train of red packets.

After decrementing the red token pool 48 in box 58, decision box 59 is entered to determine if the red token count Mr has been decremented to below zero. If so, decision box 53 is re-entered to await the accumulation of sufficient green tokens or the refreshing of the red token pool 48. That is, if there are insufficient accumulated red tokens to accommodate the next serial train of red packets, the system recycles to await the accumulation of enough green tokens to mark the packet green or the refreshing of the red token pool.

If the red count Mr is not less than zero, as determined in decision box 59, box 60 is entered to turn the red marking flag on and box 61 entered to preset the count in the hysteresis counter 47 to the fixed value L, representing the number of red tokens necessary to transmit the desired serial sequence of red packets. Box 62 is then entered to reduce the hysteresis count in counter 47 by the value N, representing the number of tokens required to accommodate the current packet at the head of admission buffer 41. In decision box 63, the value of the remaining count in hysteresis counter 47 is compared to zero. If the value in hysteresis counter 47 is less than zero, box 64 is entered to turn the red marking flag off since the tokens in counter 47 are insufficient to accommodate another red packet. Box 65 is then entered to mark the current packet red. If the value in hysteresis counter 47 is not less than zero, box 65 is entered directly, without turning the red flag off, but marking the current packet red. Box 67 is then entered to re-initialize the spacer pool 49 and then box 55 is entered to transmit the red packet. The process is terminated in terminal box 56 for the current packet. Start box 50 is re-entered when the next packet reaches the head of admission buffer 41.

If it is determined in decision box 52 that the red flag is not off, box 62 is entered to decrement the hysteresis count by N and continue on through boxes 63, 64, 65, 67 and 55 to transmit the next packet as a red packet. The red flag is thus on long enough to exhaust the hysteresis counter 47 (via box 62) and thus transmit the desired train of red packets. Note that the count in hysteresis counter 47 is eventually decremented below zero in box 62 and hence the red packet train is always somewhat longer than the length suggested by the value L.

It can be seen that the procedure outlined in the flow chart of FIG. 4 operates to transmit green packets so long as the arrival of source packets is equal to or less than the green token generation rate in green token source 45. When the arrival rate of source packets exceeds the green token generation rate, there will not be sufficient green tokens to transmit green packets and the red marking flag will be

FORTINET EX1002 Page 92

turned on. Once turned on, the red marking flag remains on until the hysteresis count in counter 47 is exhausted, thus insuring a continuous train of red packets of sufficient length to accommodate error recovery protocols. Meanwhile, at the same time that green and red packet marking is taking place, the spacer pool 49 insures a reasonable smoothing to the packet launching process. In addition, the red packet pool 48 limits the number of red data units launched in a fixed period of time. Together, these procedures insure that congestion will not occur in the network due to the launching of excessive numbers of packets from one or more packet sources.

The procedure described in connection with FIGS. 3 and 4 can be summarized as follows. Each packet at the head of the admission buffer 41 is serviced as follows:

1. Each packet waits until the spacer token pool 49 is empty.
2. If there are enough green tokens in the green token pool 46 and if the red marking flag is off, then the packet is marked green and the green token pool 46 is updated.
3. If there are not enough green tokens in green token pool 46 to service the packet and if the admission buffer length is less than K and if red marking is not turned on, then the packet must wait until enough green tokens are accumulated.
4. If there are not enough green tokens in green token pool 46 to service the packet, and if the admission buffer 41 length >K and Mr>L, then red marking is turned on and the packet is marked red. The hysteresis counter 47 is initialized to L and decremented by the number of tokens needed to accommodate this packet. When the value (LCOUNT) in hysteresis counter 47 =<0, then red marking is turned off.
5. If the number of green tokens in green token pool 46 is insufficient to service this packet and the admission buffer 41 length > K and Mr<0, then the packet waits until there are enough tokens available to mark the packet one color or the other.

The number of red data units launched in a serial train of packets in FIGS. 3 and 4 is close to and determined by the value L. This number may be too high for some rates of input source packets and may be too low for other rates of input source packets. That is, the lower the input source rate, the more time is available for transmitting red packets and hence the longer the serial red packet train can be. Similarly, the higher the input source rate, the less time is available for transmitting the serial red packet train. On the other hand, the shorter the serial red packet train, the less time available to accumulate green tokens while the red packet train is being transmitted, and sufficient green tokens may not be accumulated to transmit a green packet between bursts of red packets. Moreover, if the number of red packets in the train is too large, the probability of losing red packets at intermediate nodes is larger. These contending requirements for the length of the red packet train can be resolved by making the length of the red packet train vary in response to the rate of arrival of input source packets. A congestion control scheme utilizing such a variable amount of hysteresis is disclosed in FIGS. 5 and 6.

Referring more particularly to FIG. 5, there is shown a general block diagram of the major components of another access control module in accordance with the present invention utilizing variable hysteresis in the red packet marking process. As with FIG. 3, FIG. 5 can be realized with special purpose circuitry, but is preferably embodied in a programmed digital computer. The access control module of FIG. 5 comprises a user packet source 70 which generates input packets of data units having a given set of statistical characteristics. These packets are entered into admission buffer 71. Although admission buffer 71 may have a red-initiating threshold K like threshold 42 in buffer 41 in FIG. 3, such a threshold has been omitted in FIG. 71 for simplicity. Green token source 75 feeds a green token pool 76 having a green resume threshold 72 (Roff) which is used to turn off red marking when the number of green tokens approaches a number sufficient to allow green packet marking. As in the arrangement of FIG. 3, a red token source 74 loads Mr red tokens into red token pool 78 every T period, thus limiting the number of red data units which can be transmitted in the time period T. A spacer pool 79, emptied by spacer token sink 77, insures a minimum space between packets launched into the packet network. The only new parameter in the access control module of FIG. 5 is the green resume threshold Roff. This parameter can be defined as follows:

R(off): The green resume threshold Roff is a fraction of Mg and provides a dynamic hysteresis between the red and green marking of packets. This is accomplished by turning off red marking if the number of green tokens exceeds a preselected threshold R(off) and thus limiting the length of the red packet train in dependence on the number of green tokens available. Roff, of course, has to be large enough to exceed the number of tokens necessary to transmit a maximum-sized packet.

Using the definition of R(off) given above and the definitions of the other parameters given in connection with FIG. 3, the operation of the dynamic hysteresis access control arrangements of FIG. 5 is shown in the flow chart of FIG. 6. In FIG. 6, the dynamic hysteresis access control arrangement of FIG. 5 is started whenever a user packet reaches the head (bottom) of the admission buffer 71. Starting at start box 80, decision box 81 is entered to determine if the spacer pool 79 is empty. If not, decision box 81 is continually re-entered until spacer pool 79 is empty, thus

FORTINET EX1002 Page 93

insuring the minimum space between successive packets launched into the network.

When the spacer pool 79 is empty, as determined by decision box 81, decision box 82 is entered to determine if the packet at the head of the admission buffer 71 has been premarked green. This green premarking capability is built into the system of FIGS. 5 and 6 to allow the packet source 70 to mark specified packets as "green" (and hence to be transmitted with guaranteed delay or loss probabilities) regardless of the access control mechanism of FIG. 5. It is possible, of course, to provide the same premarking capability in the access control arrangements of FIGS. 3 and 4. If the packet is premarked green, decision box 96 is entered to determine if sufficient green tokens have been accumulated to transmit the packet. If not, box 88 is entered to await the accumulation of more tokens, and decision box 82 re-entered to check for preset green marking and decision box 96 is re-entered to check for the accumulation of sufficient green tokens. When sufficient green tokens have been accumulated to transmit the preset green packet, box 97 is entered where the packet is marked green and, in box 98, the green token pool 76 is updated by subtracting the number of tokens necessary to accommodate the preset green packet. The spacer pool is reinitialized in box 93 and the packet transmitted onto the packet network in box 94. The process terminates for that packet in terminal box 95.

If the packet at the head of the packet buffer 71 is not preset green, as determined by decision box 82, decision box 83 is entered to determine if the red marking flag is off. If the red marking flag is off, as determined by decision box 83, decision box 84 is entered to determine if sufficient green tokens have been accumulated to accommodate this packet. If so, box 97 is re-entered to mark this packet green, update the green token pool 76 in box 98, reinitialize the spacer pool 79 in box 93, transmit the green packet in box 94 and terminate the process for this packet in terminal box 95.

If the red marking flag is turned on, as determined by decision box 83, decision box 84 is entered to determine whether a sufficient number of green tokens have been accumulated in green token pool 76 to accommodate this packet. If sufficient green tokens are available, as determined by decision box 84, box 97 is entered as described above to mark the packet green (box 97), decrement the green token pool 76 (box 98), initialize the spacer pool 79 (box 93), transmit the packet (box 94) and terminate the process for this packet (box 95). If, on the other hand, sufficient green tokens have not been accumulated to accommodate this packet, as determined by decision box 84, decision box 87 is entered to determine if sufficient red tokens are available to transmit the packet. The procedure which takes place in decision box 87 will be described below.

If the red marking flag is not turned off, as determined by decision box 83, decision box 85 is entered to determine if the number of tokens in green token pool 76 (Ng) is equal to or greater than the green resume threshold 72 (Roff). If the number of green tokens equals or exceeds the green resume threshold 72 (Roff), box 86 is entered to turn the red marking flag off. Decision box 84 is then entered to determine if sufficient green tokens have been accumulated to accommodate the transmission of this packet. At this time, the answer in decision box 84 should always be "YES" since the number of green tokens is greater than Roff, as determined in decision box 85. Box 97 is therefore entered to mark this packet green, update the green pool in box 98, initialize the spacer pool in box 98, transmit the packet in box 94 and terminate the process in box 95.

If the number of green tokens in pool 72 is below the green resume threshold 72, as determined by decision box 85, or if sufficient green tokens are not available to transmit this packet, as determined by decision box 84, decision box 87 is entered to determine if sufficient red tokens have been accumulated in red token pool 78 to accommodate this packet. If so, box 90 is entered to turn the red marking flag on, box 91 is entered to mark this packet red, and box 92 is entered to update the red token pool 78 by subtracting the number of tokens necessary to accommodate this packet. Thereafter, box 93 is entered to reinitialize the spacer token pool 79 and box 94 is entered to transmit the red packet. The procedure for this packet then terminates in terminal box 95. Note that the red flag may already be turned on when box 90 is entered, due to previous traversals of the flow chart when processing a previous packet. In that case, the red flag is left on and box 91 is entered as before.

If insufficient red tokens have been accumulated in red token pool 78 to accommodate this packet, as determined by decision box 87, box 89 is entered to turn the red marking flag off. Box 88 is then entered to await the accumulation of more green or red tokens. Decision box 82 is thereafter entered to reinitiate the red-green marking process of FIG. 6, as described above, for this packet.

It can be seen that the flow chart of FIG. 6 details the procedure for utilizing a variable amount of hysteresis in the red marking process. More particularly, the green resume threshold 72 (Roff) terminates the red marking process if the packet source process produces packets sufficiently slowly so that the green token pool 76 reaches the green resume threshold 72 by the time the next packet is available at the head of buffer register 71. This allows red marking to be initiated and to continue only until the green resume threshold is reached.

The procedure carried out in the flow chart of FIG. 6 can be summarized as follows:

1. A packet at the head of the input buffer 78 first

FORTINET EX1002 Page 94

looks to see if the spacer token pool is empty. If not, it waits in the buffer until the token pool becomes empty.

2. Upon finding (or waiting for) an empty spacer token pool, a packet checks if there are enough green tokens in the green token pool to allow its transmission into the network.

3. In case there are not enough green tokens when the spacer pool is empty, the actions to be taken depend on whether or not the packet at the head of the admission buffer 78 is premarked green.

- If the packet is premarked green, the packet waits at the head of the admission buffer 78 until enough green tokens have been generated, thereby possibly holding other unmarked packets waiting behind it in the admission buffer 78.
- If the packet is not premarked green, red tokens can be used for its transmission. The red marking is then turned on, if it was not already on, and the packet is sent as red if there are enough red tokens left. After the red marking has been turned on, all the successive unmarked packets are sent marked red until either R(off) green tokens have been accumulated in the green token pool 76, or not enough red tokens remain to send the next packet, since almost all of the red tokens have already been used to send red packets.

Note that when the spacer token removal rate beta is equal to the input peak rate, queuing at the admission buffer 78 occurs only because of premarked green packets, or because the red tokens have been exhausted. If admission buffer 71 had a threshold K, as in FIG. 3, packets could also be waiting for this threshold K to be reached.

4. In order to limit the number of red packets sent into the network, an upper bound M(r) is imposed on the maximum number of data units that can be sent as red in any given time interval T. The number of red tokens available is refreshed to its maximum value Mr at the beginning of every period T.

With the above procedure of FIG. 6, at transient periods of long bursts of input packets, blocks of red packets will again be interleaved with blocks of green packets. The threshold Roff is made large enough to provide sufficient hysteresis to avoid alternating between green and red packets being launched into the packet network. The parameters M(r), T and beta are chosen so that there is sufficient time separation between the blocks of red packets and that the amount of red packets sent into the network in a short period of time does not significantly increase the loss probability of the red packets at intermediate network nodes.

It should also be clear to those skilled in the art that further embodiments of the present invention may be made by those skilled in the art without departing from the teachings of the present invention.

Claims

1. A system for a source of user data packets to control access to a packet communications network comprising
means for marking each packet launched on said network with a high priority marking when the data packets from said source stay within a predefined range of statistical parameters,
means for marking each packet launched on said network with a lower priority marking when the data packets from said source fall outside of said predefined range of statistical parameters, and
means for prolonging the operation of said means for marking with a lower priority to produce a serial train of packets with said lower priority marking.

2. The system to control access to a packet communications network according to claim 1 further comprising
means for limiting the total number of packets with said lower priority marking for each successive fixed time interval.

3. The system to control access to a packet communications network according to claim 1 further comprising
means for maintaining at least a minimum space between successive packets launched on said network regardless of their priority markings.

4. The system to control access to a packet communications network according to claim 1 further comprising
a network admission buffer having a low priority marking threshold therein for queuing said user data packets, and
means for enabling said low priority marking means when the contents of said admission buffer exceeds said threshold.

5. The system to control access to a packet communications network according to claim 1 further comprising
means for generating high and low priority tokens for enabling the marking of any one of said packets when sufficient numbers of one or the other of said priority tokens are available to accommodate the number of data units in said one packet,
means for storing said tokens for said high priority marking in a high priority token pool, said high pri-

FORTINET EX1002 Page 95

ority token storage means having a high priority resume threshold, and
means for terminating low priority marking of said packets when said high priority resume threshold is exceeded.

6. A method controlling the access to a packet communications network at each access point to said network, said method comprising the steps of
marking each packet launched on said network at each of said access points to said network with a high priority marking when the data packets at said each access point stay within a predefined range of statistical parameters,
marking each packet launched on said network with a lower priority marking when the data packets at said each access point fall outside of said predefined range of statistical parameters, and
prolonging the marking with a lower priority to produce a serial train of packets with said lower priority marking.

7. The method according to claim 6 further comprising the step of
limiting the total number of packets with said lower priority marking for each successive fixed time interval.

8. The method according to claims 6 and 7 further comprising the step of
maintaining at least a minimum space between successive packets launched on said network regardless of their priority markings.

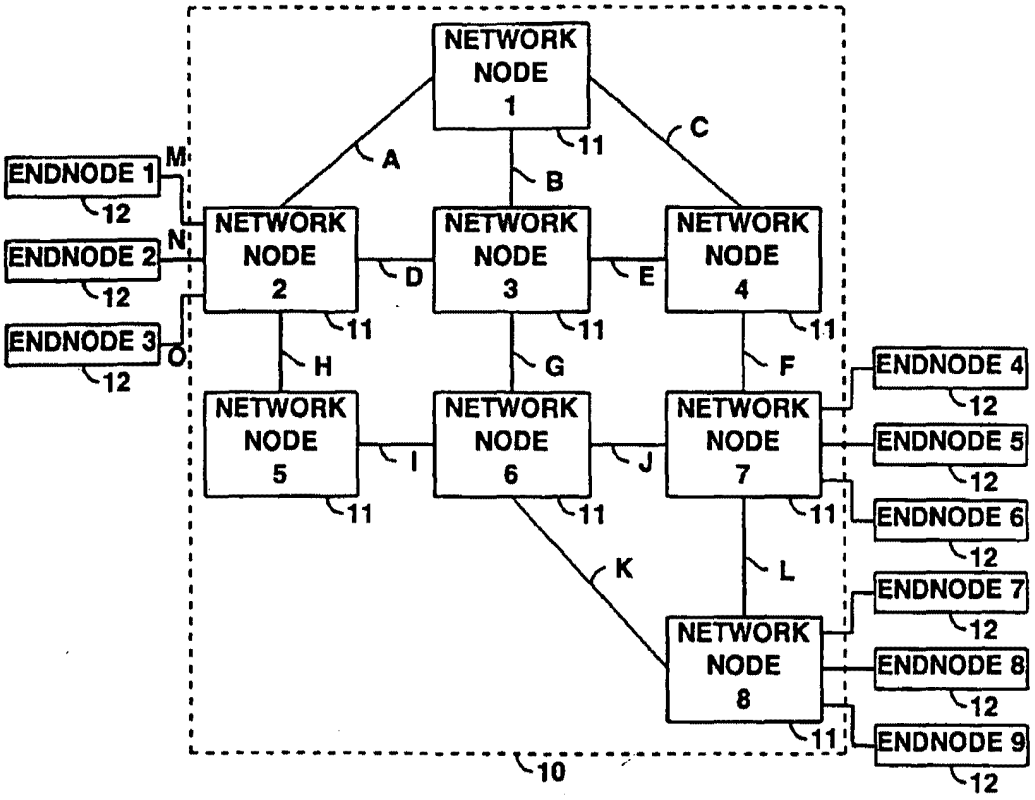
9. The method according to claims 6 to 8 further comprising the steps of
queuing said user data packets in a network admission buffer having a low priority marking threshold therein, and
enabling said low priority marking means when the contents of said admission buffer exceeds said threshold.

10. The method according to claims 6 to 9 further comprising the steps of
generating high and low priority tokens for enabling the marking of any one of said packets when sufficient numbers of one or the other of said priority tokens are available to accommodate the number of data units in said any one packet,
storing said tokens for said high priority marking in a high priority token pool, said high priority token pool having a high priority resume threshold, and
terminating low priority marking of said packets when said high priority resume threshold is exceeded.

FORTINET EX1002 Page 96

FIG. 1

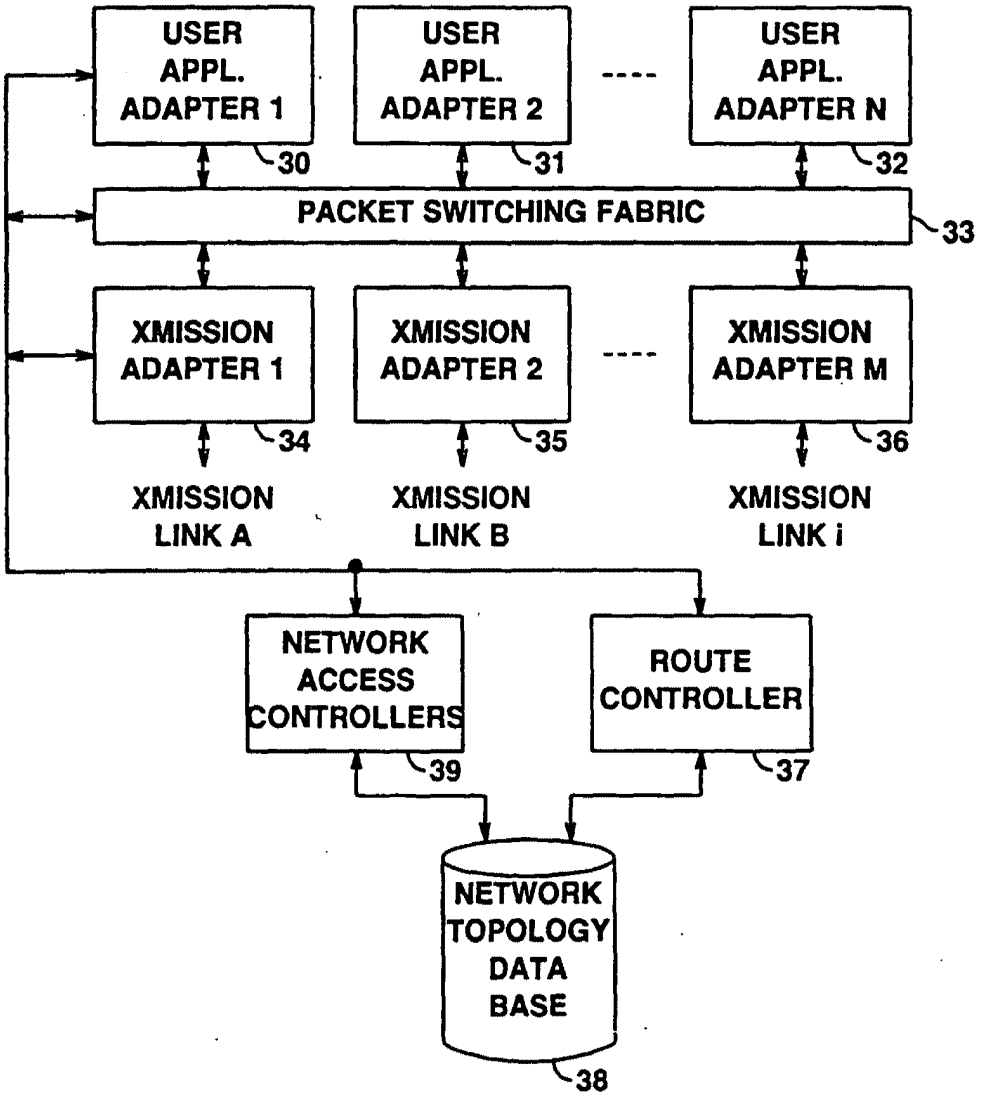
COMMUNICATIONS NETWORK



FORTINET EX1002 Page 97

FIG. 2

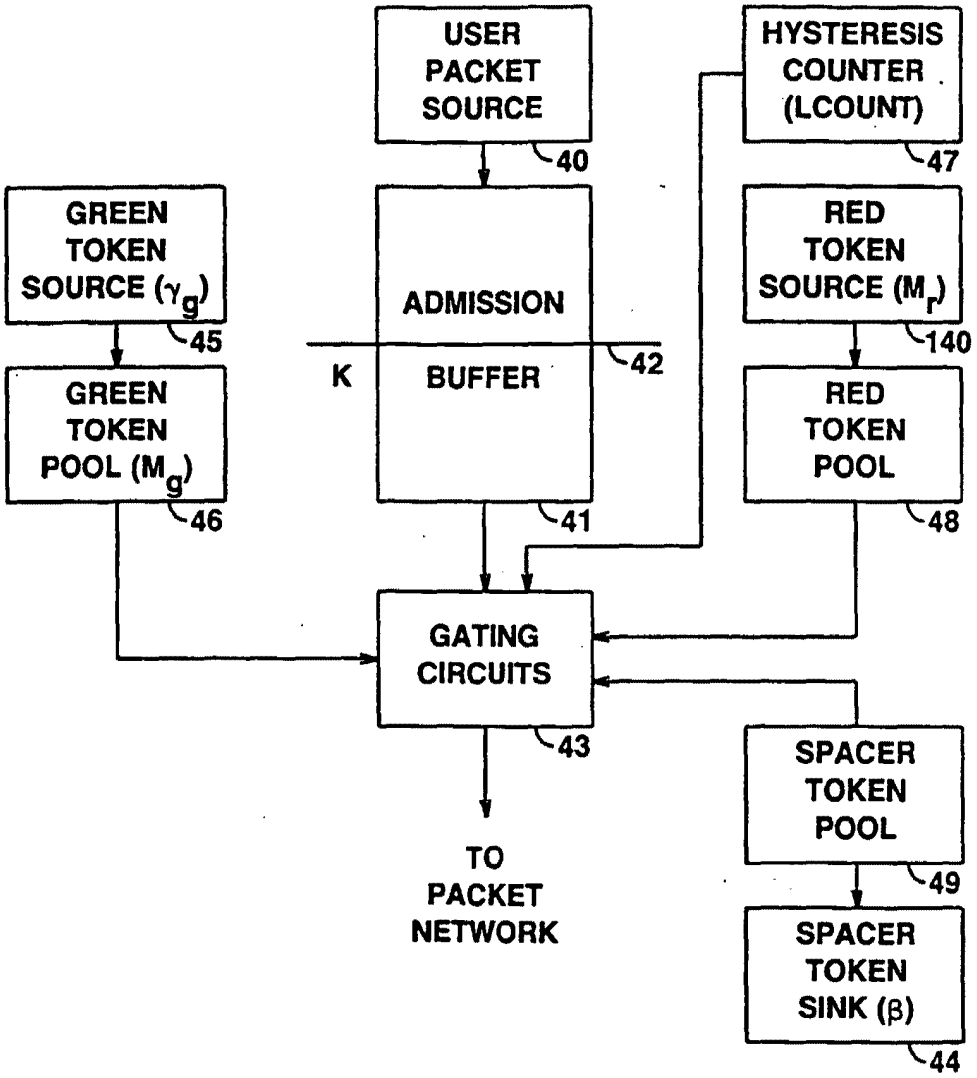
TYPICAL PACKET DECISON POINT



FORTINET EX1002 Page 98

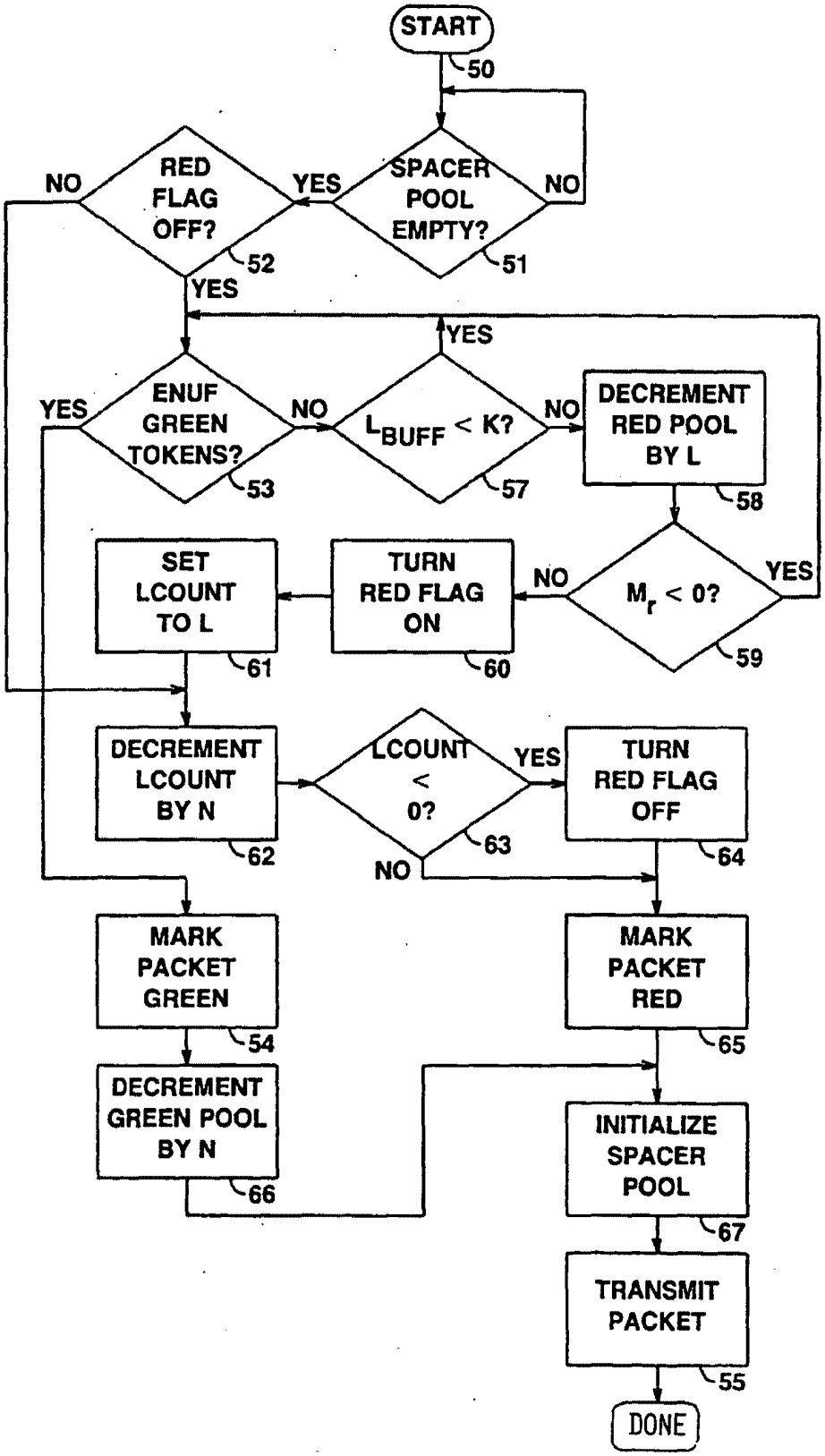
FIG. 3

LEAKY BUCKET ACCESS CONTROL
WITH STATIC HYSTERESIS



FORTINET EX1002 Page 99

FIG. 4



FORTINET EX1002 Page 100

FIG. 5

LEAKY BUCKET ACCESS CONTROL
WITH DYNAMIC HYSTERESIS

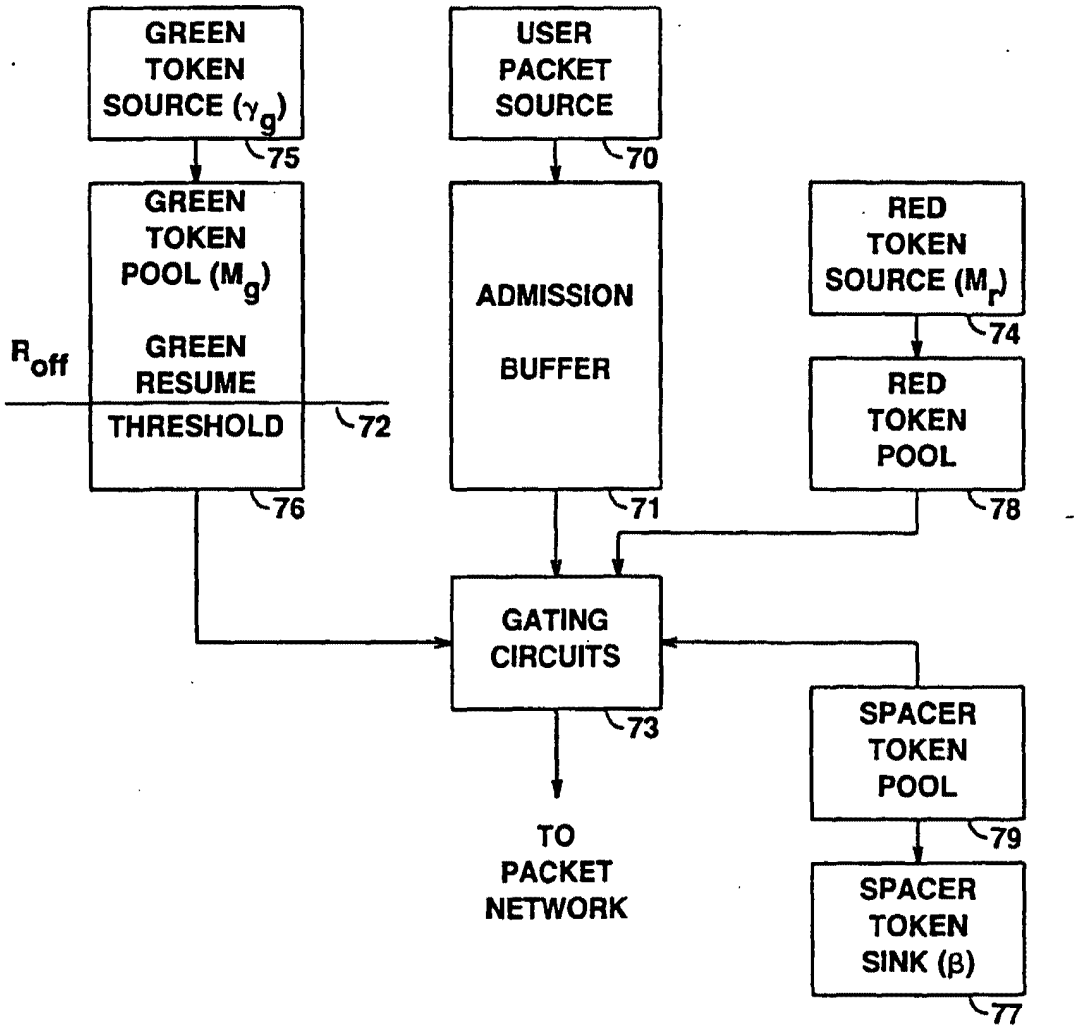
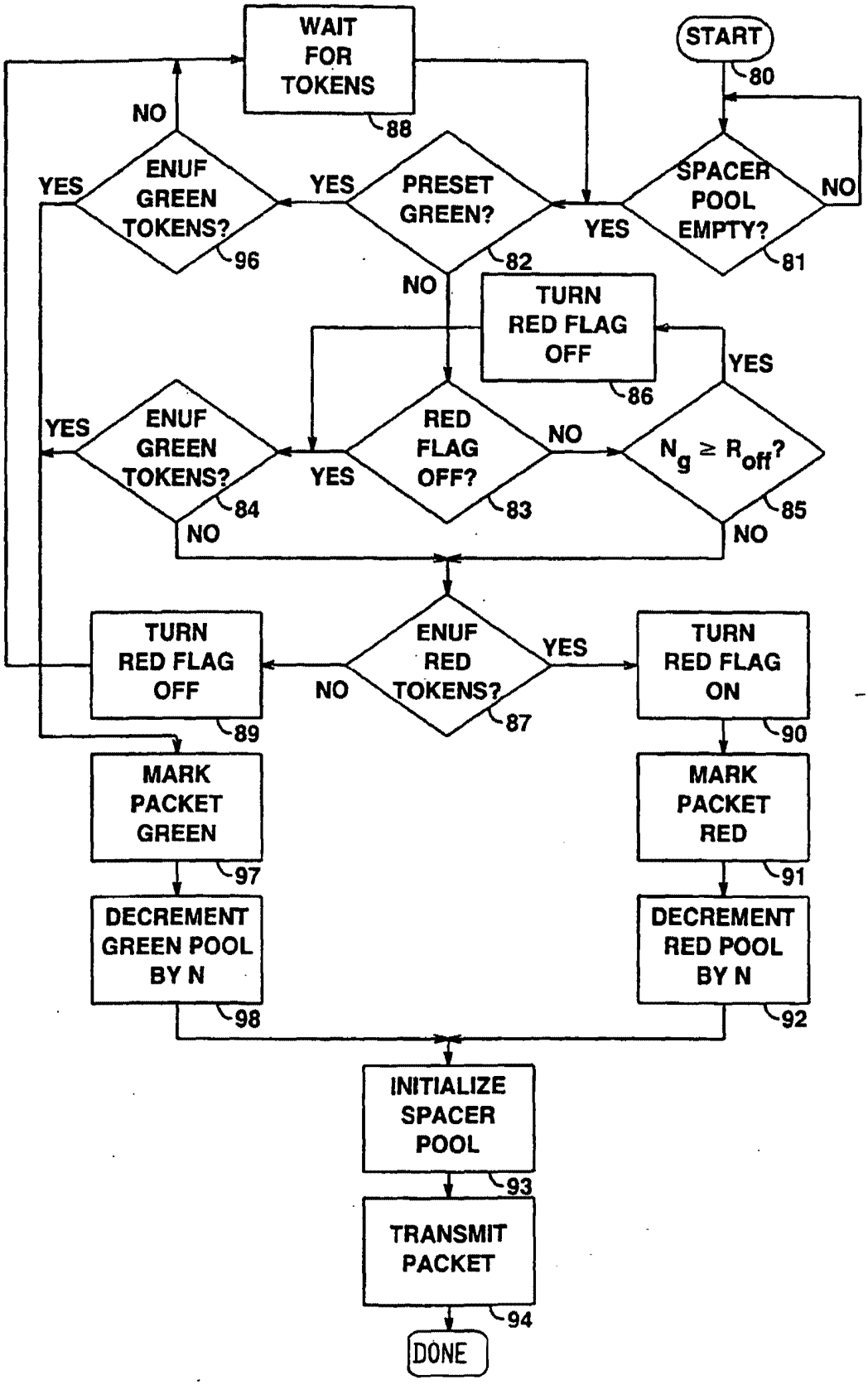


FIG. 6


START
80
WAIT FOR TOKENS
88
SPACER POOL EMPTY?
81
NO
YES
PRESET GREEN?
82
YES
ENUF GREEN TOKENS?
96
YES
NO
TURN RED FLAG OFF
86
YES
$N_g \geq R_{off}$?
85
NO
RED FLAG OFF?
83
YES
NO
ENUF GREEN TOKENS?
84
YES
NO
ENUF RED TOKENS?
87
YES
NO
TURN RED FLAG ON
90
TURN RED FLAG OFF
89
MARK PACKET RED
91
MARK PACKET GREEN
97
DECREMENT RED POOL BY N
92
DECREMENT GREEN POOL BY N
98
INITIALIZE SPACER POOL
93
TRANSMIT PACKET
94
DONE

B2

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/077787 A3

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US01/40405

(22) International Filing Date: 30 March 2001 (30.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/540,299 31 March 2000 (31.03.2000) US

(71) Applicant: SIEBEL SYSTEMS, INC. [US/US]; 2207 Bridgepointe Parkway, San Mateo, CA 94404 (US).

(72) Inventors: BRODERSEN, Karen; 17 Spinnaker Place, Redwood City, CA 94065 (US). ROTHWEIN, Thomas, M.; 314 Ballymore Circle, San Jose, CA 95136 (US). MALDEN, Matthew, S.; 1945 Pacific Ave. #3B, San Francisco, CA 94109 (US). CHEN, Ming, J.; 35829 Carnation Way, Fremont, CA 94536 (US). ANNADATA, Anil; 815 Cameron Circle, Milpitas, CA 95035 (US).

(74) Agents: GRABAREK, Robert, L., Jr. et al.; Cooley Godward, LLP, Patent Group, One Freedom Square, 11951 Freedom Drive, Reston, VA 20191-5601 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

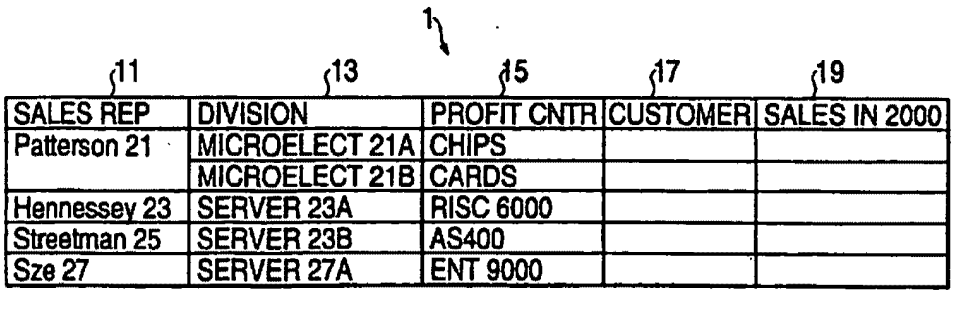
(88) Date of publication of the international search report:
21 February 2002

(48) Date of publication of this corrected version:
10 October 2002

(15) Information about Correction:
see PCT Gazette No. 41/2002 of 10 October 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DATABASE ACCESS METHOD AND SYSTEM FOR USER ROLE DEFINED ACCESS



(57) Abstract: Method and system for determination and granting of access to data and files (11) by the file or database creator (13), owner or manager or by group or user access profiles (19). The database is partitionable among data owners (31), and access is awarded based upon the requestor's organizational attributes (33).

WO 01/077787 A3

DATABASE ACCESS METHOD AND SYSTEM FOR USER ROLE DEFINED ACCESS

FIELD OF THE INVENTION

The invention relates to determination and granting of access to data and files by the file or database creator, owner or manager or by group or user access profiles.

BACKGROUND

Current database management applications and especially the access subsystems thereof support what could be called a "Single Organization Model". This means that all users of a system, even though they may work in various divisions of a company or various channels of a marketing organization, or even different entities leasing portions of the same database through a common vendor or service organization, are deemed to ultimately work for the same organization, and that organization is at the root of the organizational hierarchy.

Present access control mechanisms, built on the "Single Organization Model," are cumbersome when applied to multi-divisional or multi-channel organizations or to multi-tenant databases. This is because present access authorization systems are adapted to: (1) partition data to show users only those records that they or their position have been granted visibility to, and (2) show users all "global" data in a particular dataset. However, absent cumbersome "work arounds" present access authorization subsystems do not have the ability to partition data at the organizational or channel level. This makes it impossible, for instance, for companies using the "e-channel marketing" paradigm that do business in multiple countries in Europe to maintain separate price lists for each country and have only those price lists that are appropriate for a region or country be accessible. This cumbersome access control also makes it difficult for multiple small financial service organizations to outsource database and telephone support operations to a common vendor while preserving customer confidentiality.

FORTINET EX1002 Page 104

SUMMARY

The invention is a database management system and a method of using the system. The system has an access control subsystem, and is characterized by a plurality of user entries representing users seeking access to data items, where each of the user entries has at least one organizational access attribute. The data stored in the underlying database has a plurality of data items. Each of the data items may be a data file, a data field within a data file, or a view of a data items. Selected ones of the data items have at least one organizational access attribute. This organization attribute is used by the access control subsystem. The access control subsystem receives a database query from a user requesting access to one or more of the data items. The access control subsystem reads the user's organizational access attributes, and reads the data item's organizational access attributes. The access control subsystem then presents data items to the user to which the user has access authorization.

In one embodiment of the invention, particularly useful in channel marketing and in multi-divisional enterprises, the database files have a plurality of fields, and the users have personal, positional, and organizational attributes, and are divisible into multiple membership sets based upon organizational attributes. The database views are visible to users based upon the personal, positional, and organizational attributes of the users.

The data files and fields may extend across organizations, or they may be disjoint, extending to only one organization. Likewise, the users may be in overlapping organizations, or in only one organization.

According to this embodiment of the invention, the views visible to a user are determined by the user's organizational and positional attributes, and the view files are determined by a user's organizational and/or positional attributes. In a still further embodiment, the view files are determined by a user's organizational attributes, and view fields are determined by a user's positional attributes.

In an alternative embodiment of the invention a plurality of organizations exclusively own individual data files in the database management system. An individual data file has a single owner. The access control subsystem is configured to authorize a customer

of the owner organization to have access to their own data items and to grant access to their own data items to an additional user, for example, a telephone service representative, while the customer accesses the data items. The customer can authorize the additional user to access and update the data item.

In this embodiment, the database system may be regarded as a partitionable database with a plurality of separate virtual databases. Each of the separate virtual databases may have a unique database owner, and a user can only access files in a virtual database to which the user has access authorization from the database owner.

The separate virtual databases may be disjoint, for example with common ownership or separate and unique owners. Access may depend upon authorization from the database owner to access either the database or a file within the database, and where the user requesting access is not the owner of the file, access may require authorization from the owner of the file. This situation typically occurs in a multi-tenant database having a plurality of tenants, where each tenant is the owner of a separate virtual database, and at least two of the tenants utilize a common call center service, as is the case with a large financial institution servicing the customer accounts of other financial institutions.

THE FIGURES

The method and system of the invention are illustrated in the FIGURES.

FIGURE 1 represents a simplified, high level view of the schema of a database of the "multi-organization support" method and system of the invention.

FIGURE 2 represents a simplified, high level view of the schema of a database of the "multi-tenancy support" method and system of the invention.

OVERVIEW

This invention relates to database access and more particularly to methods and systems for controlling database access through an access authorization subsystem of the database management system. The access authorization subsystem utilizes user and data attributes that have utility beyond database access or visibility; the access

FORTINET EX1002 Page 106

authorization subsystem filtering, screening, and querying these attributes to determine access or visibility of a user to a data item. The ability to dynamically support database access based upon the instantaneous role of the user at the time of access, that is, in real time, requires a user role defined access authorization subsystem such as the "Multiple Organization Model," having a schema as shown at a very high level in FIGURE 1, or "Multi-Tenant Model," having a schema as shown at a very high level in FIGURE 2.

The concept of the "multiple organization model" or "multi-organizational" support is especially important to e-channel marketing. The driving force behind e-channel marketing is that multiple channel partners share a common database, including business objects and tools, with the main company. Each of the channel partners should only see data that is relevant to their own organization. This means that they would not see data for other channel partners or non-global data from the parent organization.

Similarly, the concept of the "Multi-Tenant Model" or "Multi-Tenant Support" is especially important to small financial service providers, retailers, and the like. This is because multi-tenant support enables these businesses to out source, for example, their credit card operations to a service agency or large financial services organization, with the telephone support staff member of the large financial services organization having gaining real time access to the individual account being serviced during the service call.

DETAILED DESCRIPTION

This invention relates to database access where a user's access rights to specific data items are defined dynamically, that is, in real time, based upon the user's status at the time of access request, and data and user attributes having independent utility and significance apart from access and visibility. Colloquially, the user has one set of access authorizations while wearing a red hat and another set of access authorizations while wearing a blue hat. The hats could represent roles as a telephone service representative for multiple credit card issuers sharing a multi-tenant, vendored, database, or roles as a marketing representative of a company in first and second regions.

FORTINET EX1002 Page 107

The database access system and method of the invention utilizes a division of the data "owners" either (1) hierarchically, that is vertically, with horizontal divisions in branches, or (2) horizontally, that is, separate virtual databases. The database itself is divided into files, the files are divided into records within the files, and individual records are divided into fields. In either mode of division, the (schema and metadata data needed and would be sophisticated), and user access is based upon user's relationship to one or more owners in the hierarchy. (for example, owners could be independent lessees of database capacity or divisions in a multi-divisional enterprise).

The method and system of the invention builds upon partitionability of the individual database files in the database based upon an attribute of ownership and/or control. For example, in the multi-tenancy model, the database might be partitionable into separate and distinct individual virtual databases, as in the case of financial services organizations, for example competing financial services organizations, vendoring database capacity, database management services, and telephone support services for a service provider. By way of contrast, in the multi-organization support model, the database's parent organizational owner is hierarchically and organizationally divisible, for example into divisions, departments, and offices, where each branch point may be a hierarchical level and each branch may be a functional owner of a portion of the enterprise database.

In both embodiments user access is triggered by a "need to know" or "convenient to know." In the multi-tenancy embodiment, the access is typically triggered by an incoming call to a vendored call center, and the view is the customer's computer telephony integration (CTI)-identified account number. Similarly, in the multi-organization support embodiment, the access is triggered end user action, and the specific view is triggered by the end-user's logon, that is, which division or channel or reporting chain is used for this task.

Multi Organization Support

In a large organization where the same products and/or services are rendered through different employees and/or rendered to different customers, or where some goods,

FORTINET EX1002 Page 108

services, or customer sets are prohibited to some employees or organizations and permitted to others (for example, sale of encryption equipment or code to the PRC, or the sale with English only labeling/instructions in Quebec), and the product set is too large and/or unwieldy to maintain separate databases, there is a definite productivity advantage to organizationally limiting access so that the marketing representative is not inundated with "useless" information. This is accomplished by assigning access authorization organizationally, including regionally. This way, when a sales or service rep or a channel partner enters a "MYLIST" command, he or she is only presented with a virtual database of the products and/or services that he or she can actually render. This is the "single database – multiple independent users" embodiment, also referred to as the "multi-organization support" method and system.

FIGURE 1 is a very high level view of the database schema of a "multi-organization support" model. The schema, 1, has, for purposes of illustration, five fields in each record. These fields are the Sales Rep, 11, the Division, 13, the Profit Center (within the Division, 13), 15, the customer 17, and the sales to that customer in the year 2000, 19. Sales Representative Patterson, 21, is in the Microelectronics Division 21A, 21B, and sells in two profit centers of the division, cards, and chips. Hennessey, 23 is in only one Division, the Server Division, 23A, and sells the goods of only one profit center, RISC 6000. Also in the Server Division, 25B, is Streetman, 25, who only sells the product of one profit center, the AS400 profit center. Sales Representative Sze, 27, is also in the Server Division, here 27A, and only sells the products of one profit center, the ENT 9000 profit center.

The multi-organization support utilizes new types of visibility attributes called "organization" and "organization team" visibility. In the multi-organization support method and system of the invention, the records that a user sees with "organization" and "organization team" visibility are restricted based upon the organization(s) that the user has been given visibility into, while the ones the end user sees with "position" and "position team" visibility are restricted based upon the user's current position. While there may be some overlap between "organization" attributes and "position" attributes, they may confer different rights. For example, "organization" attributes may only confer "read" authorization, while "position" attributes may confer "read," "write", and

FORTINET EX1002 Page 109

"delete" authorization. The "organization" and "organization team" visibility is used in a series of "My Organization's" views that show all of the data that the user's organization has been granted visibility to. In this way, multiple organizations can share the same database but see a partitioned set of data that is pertinent to them. It is also to be understood, that there may be inheritance of access up and down and across a hierarchy.

One access attribute specifies the visibility attributes of the higher level organization, for example a division. This means that the number of distinct organizational partitions will be relatively small compared to the overall number of divisions in the hierarchy. Also, organizational partitions should be relatively high in the hierarchy. Therefore, most of the lower level entities in a large enterprise, for example a domestic marketing division of a large international enterprise may reference the US division as their visibility organization. This would enable all people who work for any of those lower level product or marketing organizations to see the same partition of data.

The relationship between divisions and positions is normally a 1-to-many relationship, although the system and method of our invention can support a many-to-many relationship. That is, a position belongs to exactly one division. If a user needs to have access to data in multiple organizations, then the user would be required to have positions in the appropriate organizations, or, in an alternative embodiment of our invention, to have personal or positional access to the data separate and apart from but in addition to his or her organizational access to the data. This could be done by having positions specifically for granting visibility to users outside of the organization.

Single organization ownership is added to an entity by adding a foreign key to the owning organization and configuring the business component appropriately. Organization teams are added to an entity by adding an intersection table between that entity and organization and a foreign key to the primary owning organization, and configuring the business component appropriately.

During login, while the system is collecting information about the positions a user is associated with, the system looks at the user's division or divisions and collects the set

of organizations those divisions have visibility into. If a user has n positions, that is, n positional attributes, the user will have between 1 and n organizations for visibility.

The organization and organization team visibility's are used for "My Organization's" views to show the user all of the records for the entity where the user's "current" organization is either the owner, or on the organization team. The user's "current" organization will be the visibility organization assigned to the division of the user's current position. When a user changes current position, the current organization will be changed automatically.

Channel Partners may be administered by creating a division node or hierarchy as the visibility organization in the appropriate table. All sub-organizations for that channel partner should specify the root channel partner division node as the visibility organization. Similarly, the Pick Lists and association lists for entities that are "multi-org'd" will show the appropriate organization specific data.

Channel partners may either assign access authorization to their own users or request the database owner to assign access authorization.

Multi Tenancy Support

An alternative embodiment of our invention is the "multiple tenancy" model described with respect to CTI applications. This embodiment solves problems associated with the situation of a plurality of merchants and/or financial services organization vendoring out their telephone service and data processing operations to a common vendor. The common vendor stores the merchants' and institutions' customer accounts in an access controlled database while also providing customer telephone support service for the customer accounts. That is, the CTI (computer-telephony integration) automatically switches the agent to the correct slice (that is, customer files) of the database. Access to a customer account is authorized in real time during the individual telephone support session with the customer. During the individual customer support session, the telephone support representative has access to the individual merchant's or financial institution's business objects, queries, and views, as well as those of the database service provider.

FORTINET EX1002 Page 111

FIGURE 2 shows a very high level view of the "multi-Tenant" database schema, 1. This schema shows three banks in the Bank column 31, CITI 43, MBNA, 45, and BankOne, 45. In the customer column, 33, each bank is shown with only two customers, McCabe 43A and Smith 43B for CITI, 43, Van Ness 45A and Bird, 45B for MBNA, 45, and Stewart, 47A, and Lightfoot, 47B, for BankOne 47. Each customer has an account number, shown in column 35, and space for the last three transactions, shown in columns 37, 39, and 41. In operation, if VanNess were to call the Vendor's support center on the appropriate access number, and properly enter the account number shown for VanNess in column 35, line 45, VanNess's account would come up on the CTI operator's screen, and both VanNess and the CTI operator would have access to account information.

To be noted is that when a caller calls in to an outsourcing call center or multi-tenancy call center, the gets switched to the slice of the database for that tenant (for example, the slice of the database assigned to their financial service provider) not just the particular file for that particular caller or customer. This is important because in this way the customer can access information about Products, Price Lists, Service Requests and Sevices of the tenant that is being provided by the tenant, either directly or through outsourcing.

While the invention has been described with respect to certain preferred embodiments and exemplifications, it is not intended to limit the scope of the invention thereby, but solely by the claims appended hereto.

We claim:

1. A database management system having an access control subsystem, said database management system comprising:

a) a plurality of user entries representing users seeking access to data items, each of said user entries having at least one organizational access attribute; and

b) a plurality of data items, each of said data items being a data file, a data field within a data file, or a view of data items, and selected ones of said data items have at least one organizational access attribute;

said access control subsystem being configured to:

a) receive a database query from a user requesting one or more data items;

b) read the user's organizational access attributes;

c) read the data item's organizational access attributes; and

d) present data items to the user to which the user, based on the user's access attributes, has access.

2. The database management system of claim 1 in which access is granted to the user by determining whether the user's organizational access attributes and the data item's organizational attributes include a match.

3. The database management system of claim 1 wherein a plurality of organizations exclusively own individual data files in the database management system, whereby an individual data file has a single owner.

4. The database management system of claim 3 wherein said access control subsystem is configured to authorize a customer of an owner organization having access to a data item to grant access to the data item to an additional user while the customer accesses the data item.

FORTINET EX1002 Page 113

5. The database management system of claim 4 wherein said access control subsystem is configured to authorize the customer of the owner organization to access the data item and to thereafter authorize the additional user to access and update the data item.

6. The database management system of claim 1 wherein said organizational access attributes are configured hierarchically, such that each organizational access attribute has a hierarchical level and a hierarchical branch, and each user access attribute has a hierarchical level and a hierarchical branch, and said access control subsystem is configured to grant access based on one or both of (a) the hierarchical levels of the user and data item, or (b) the hierarchical branch of the user and data item.

7. The database management system of claim 6 wherein said hierarchical levels correspond to ranges of organizations, and to data items identified thereto.

8. The database management system of claim 7 wherein the data items are chosen from the group consisting of data fields, data files, and views.

9. The database management system of claim 6 wherein said hierarchical branches correspond to virtual or real organizations and data items identified thereto.

10. The database management system of claim 9 wherein said data items are chosen from the group consisting of data files and views.

11. The database management system of claim 6 wherein hierarchical levels correspond to access to data fields and data views, and hierarchical branches correspond to access to data files and data views.

12. A method of managing a database having:

a) a plurality of user entries representing users seeking access to data items, each of said user entries having at least one organizational access attribute; and

b) a plurality of data items, each of said data items being a data file, a data field within a data file, or a view of data items, and selected ones of said data items have at least one organizational access attribute;

FORTINET EX1002 Page 114

said method comprising:

a) receiving a database query from a user requesting one or more data items;

b) reading the user's organizational access attributes;

c) reading the data item's organizational access attributes; and

d) presenting data items to the user to which the user based on the user's access attributes has access.

13. The method of claim 12 comprising determining whether the user's organizational access attributes and the data item's organizational access attributes include a match, and if so, granting access.

14. The method of claim 12wherein a plurality of organizations exclusively own individual data files in the database management system, and an individual data file has a single owner.

15. The method of claim 14 comprising a customer of an owner organization having access to a data item granting access to the data item to an additional user while the customer is accessing the data item.

16. The method of claim 15 comprising the customer of the owner organization accessing the data item and to thereafter authorize the additional user to access and update the data item.

17. The method of claim 12 wherein said organizational access attributes are configured hierarchically, such that each organizational access attribute has a hierarchical level and a hierarchical branch, and each user access attribute has a hierarchical level and a hierarchical branch, said method comprising granting access based on one or both of (a) the hierarchical levels of the user and data item, or (b) the hierarchical branch of the user and data item.

FORTINET EX1002 Page 115

18. The method of claim 17 wherein said hierarchical levels correspond to ranges of organizations, and to data items identified thereto.

19. The method of claim 18 wherein the data items are chosen from the group consisting of data fields, data files, and views.

20. The method of claim 17 wherein said hierarchical branches correspond to virtual or real organizations and data items identified thereto.

21. The method of claim 20 wherein said data items are chosen from the group consisting of data files and views.

22. The method of claim 17 wherein hierarchical levels correspond to access to data fields and data views, and hierarchical branches correspond to access to data files and data views.

23. A method of managing a database system having a plurality of files, said files having a plurality of fields, said database being divisible into multiple sets of file and field entries having views visible to users having personal, positional, or organizational attributes associated with the said views, said users being divisible into multiple membership sets based upon organizational attributes, which method comprises:

(a) determining the personal, positional, and organizational attributes of users; and

(b) when a users queries the database:

(i) accessing files and fields within the database to which the user has access based upon the user's attributes; and

(ii) presenting a view to which the user has access based upon the user's attributes.

24. The method of claim 23 comprising determining access to files based upon one attribute and determining access to fields based upon another attribute.

25. The method of claim 23 comprising determining access to files based upon a first organizational attribute and determining access to fields within the files based upon one of a personal attribute or a second organizational attribute.

26. The method of claim 23 comprising determining access to a file based upon an attribute and to at least one field in the file based upon the same attribute.

27. The method of claim 26 comprising determining access to a file based upon an organizational attribute and to at least one field in the file based upon the same organizational attribute.

28. The method of claim 25 wherein one of said users is an internal user having access to first portions of a view, and wherein another one of said users is an external user having access to second portions of the view.

29. The method of claim 28 wherein said first and second portions of the view are partially overlapping and partially non-overlapping.

30. A database system comprising a database having a plurality of files, said files having a plurality of fields, said users having personal, positional, and organizational attributes, and being divisible into multiple membership sets based upon organizational attributes, said database having views visible to said users based upon the personal, positional, and organizational attributes thereof.

31. The database system of claim 30 wherein the multiple sets of files and fields are overlapping across organizations.

32. The database system of claim 30 wherein the multiple sets of files and fields are disjoint across organizations.

33. The database system of claim 30 wherein the multiple sets of users are in overlapping organizations.

34. The database system of claim 30 wherein the multiple sets of users are in disjoint organizations.

FORTINET EX1002 Page 117

35. The database system of claim 30 wherein views visible to a user are determined by the user's organizational and positional attributes.

36. The database system of claim 35 wherein view files are determined by a user's organizational attributes.

37. The database system of claim 35 wherein view fields are determined by a user's positional attributes.

38. The database system of claim 35 wherein view files are determined by a user's organizational attributes, and view fields are determined by a user's positional attributes.

39. A database system comprising a partitionable database of a plurality of separate virtual databases, each of said separate virtual databases having a unique database owner, and wherein a user can only access files in a virtual database to which the said user has access authorization from the database owner.

40. The database system of claim 39 wherein said separate virtual databases are disjoint.

41. The database system of claim 40 wherein said separate, disjoint virtual databases have unique owners.

42. The database system of claim 41 wherein a user requires authorization from a database owner to access the owner's separate, virtual database.

43. The database system of claim 42 wherein a user requires authorization from the owner of a file within the separate, virtual database to access the file owner's file.

44. The database system of claim 43 wherein a user's access authorization to a particular file in the virtual database is granted by the file owner's initiation of a database call through an associated computer telephony integration (CTI) system.

FORTINET EX1002 Page 118

45. The database system of claim 44 wherein the database is a multi-tenant database having a plurality of tenants, each tenant being the owner of a separate virtual database, at least two of the tenants utilizing a common call center service.

46. A method of managing a database system having a partitionable database of a plurality of separate virtual databases, each of said separate virtual databases having a unique database owner, said method comprising the owner of a separate virtual database granting access authorization to a user, and the user thereafter accessing a file in the virtual database to which the said user has been granted access authorization from the database owner.

47. The database management method of claim 46 wherein said separate virtual databases are disjoint.

48. The database management method of claim 47 wherein said separate, disjoint virtual databases have unique owners.

49. The database management method of claim 46 wherein a user requires authorization from the owner of a file within the separate, virtual database to access the file owner's file.

50. The database management method of claim 49 wherein the file owner grants access authorization to the file owner's file in the virtual database to a user.

51. The database management method of claim 50 wherein the file owner's initiation of a database call through an associated computer telephony integration (CTI) system grants access authorization to the file owner's file to a user.

52. The database management method of claim 51 wherein the database is a multi-tenant database having a plurality of tenants, each tenant being the owner of a separate virtual database, at least two of the tenants utilizing a common call center service.

FORTINET EX1002 Page 119

FIG. 1

1

11 SALES REP	13 DIVISION	15 PROFIT CNTR	17 CUSTOMER	19 SALES IN 2000
Patterson 21	MICROELECT 21A	CHIPS		
	MICROELECT 21B	CARDS		
Hennessey 23	SERVER 23A	RISC 6000		
Streetman 25	SERVER 23B	AS400		
Sze 27	SERVER 27A	ENT 9000		

FIG. 2

1

31 BANK	33 CUSTOMER	35 ACCOUNT #	37 TRANSACTION 1	39 TRANSACTION 2	41 TRANSACTION 3
CITI 43	McCabe 43A	4567-1234-5678	-------	-------	-------
	Smith 43B	4567-1234-6587	-------	-------	-------
MBNA 45	VanNess 45A	4210-5678-9111	-------	-------	-------
	Bird 45B	4210-6294-6611	-------	-------	-------
BANKONE 47	Stewart 47A	4816-1776-1812	-------	-------	-------
	Lightfoot 47B	4816-2558-1149	-------	-------	-------

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/40405

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G6F 17/30
US CL : 707/9; 707/2
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/9

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 6,085,191 A (FISHER et al.) 04 JULY 2000, col. 25, lines 51-col. 26, lines 60, col. 28, lines 58-64, col. 18, lines 39-67, col. 21, lines 59-66, col. 29, lines 42-52, col. 29, lines 42-52, col. 5, lines 15-24, col. 23, lines 37-45, col. 9, lines 40-55, col. 9, lines 56-col. 10, lines 54, and col. 23, lines 22-27.	1-52
Y	US 5,778,357 A (KOLTON et al.) 07 JULY 1998, col. 4, lines 18-34, and col. 5, lines 51-col. 6, lines 16.	1-52

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September 2001 (17.09.2001)	01 NOV 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Kim Yen Vu Telephone No. 703-305-4700

Form PCT/ISA/210 (second sheet) (July 1998)

B3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/09458 A2

(51) International Patent Classification[7]: H04Q 7/00

(21) International Application Number: PCT/US01/23145

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,385 24 July 2000 (24.07.2000) US

(71) Applicant: **BLUESOCKET, INC.** [US/US]; 7 New England Executive Park, Burlington, MA 01803 (US).

(72) Inventor: **CROSBIE, David, B.**; 47 Bay State Avenue, Somerville, MA 02144 (US).

(74) Agents: **WAKIMURA, Mary, Lou** et al.; Hamilton, Brook, Smith & Reynolds, P.C., 530 Virginia Road, P.O. Box 9133, Concord MA 01742-9133 (US).

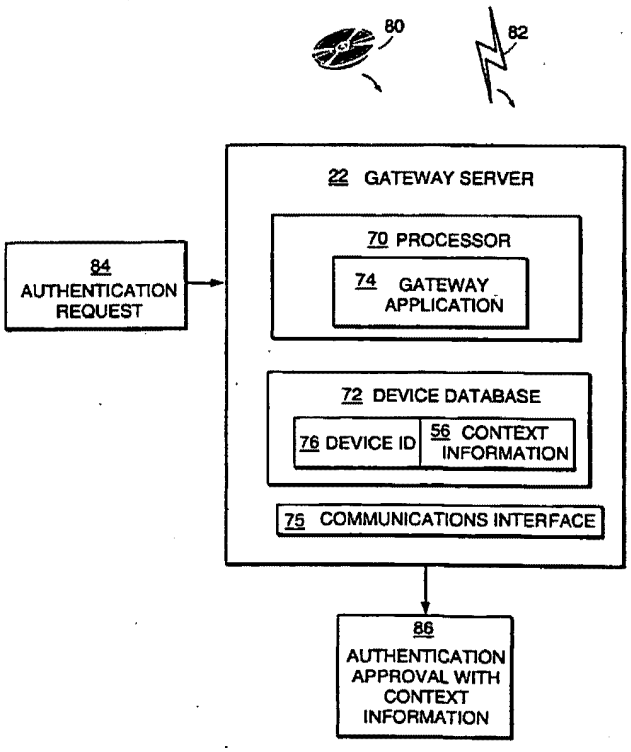
(81) Designated States *(national)*: CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR ENABLING SEAMLESS ROAMING IN A WIRELESS NETWORK



(57) Abstract: A gateway server manages connections in a wireless local area network (WLAN). The gateway server provides context information, such as an IP address, that is stored after being previously allocated to a mobile device in a previous connection to the WLAN. The gateway server reassigns the IP address to the mobile device after it reconnects to the WLAN after a disconnection, thus providing seamless roaming for the mobile device from WLAN to WLAN (or subnets within one WLAN) without requiring the user of the device to re-register. The gateway server also provides cluster information (e.g., as part of the context information) for a mobile device making a new connection to the WLAN, such as access privileges associated with the cluster of users of the mobile devices. The gateway server also provides load balancing among two or more WLAN's by directing a newly connection mobile device to another WLAN (or subnet), if less congestion results.

WO 02/09458 A2

METHOD AND SYSTEM FOR ENABLING SEAMLESS ROAMING IN A WIRELESS NETWORK

BACKGROUND OF THE INVENTION

Networked desktop computing is typical in both the office and home. Networking of mobile devices, such as mobile telephones, laptop computers, headsets, and PDA's (Personal Digital Assistants), is more difficult. One problem has been that there has not been a commonly accepted standard approach for attaching such devices, such as the mobile equivalent of a LAN (Local Area Network) card or a modem, to a WLAN (wireless LAN).

Bluetooth (BT) is a low cost wireless connection technology. The Bluetooth technology is described in the Bluetooth specification version 1.1, available from Bluetooth SIG, Inc. (see also the www.bluetooth.com web site.) This technology provides for a common attachment approach for different devices, and so enables mobile phones, laptops, headsets, and PDA's to be easily networked in the office and eventually in public locations. Other standards such as the IEEE 802.11 (Institute of Electrical & Electronics Engineers) and ETSI (European Telecommunications Standards Institute) HIPERLAN/2 provide a generally similar connection function as Bluetooth and may be used to support WLAN (see the IEEE 802.11 "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications" and ETSI specifications for HIPERLAN/2 such as ETSI document number TR 101 683, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview").

Wireless LAN (WLAN) access points (LAP's) such as those used by 802.11 and Bluetooth are part of an IP subnet; that is, a range of IP addresses that are normally used by all the devices connected to a section of the network delineated by a router (which may also be known as a gateway), direct packets to and from devices that are outside the subnet.

In one conventional approach, devices (e.g., a router, gateway, or mobile devices) inside the subnet are primarily identified by their MAC address. This is a fixed address tied to the Ethernet card. IP addresses are associated with MAC

addresses. There can be multiple IP addresses associated with a single MAC address. Each router or gateway device on the subnet maintains a cache which maps IP addresses within the sub-net to the associated MAC addresses. Data packets are sent to the MAC address associated with the IP address by the cache. (For destinations outside the sub-net the data is sent to the router which then forwards them.)

In order for a device (e.g., router or gateway) to find the MAC address associated with a particular IP address, an ARP (address resolution protocol) is used. The device (e.g., router or gateway) follows the ARP and sends out a broadcast message asking for the device associated with the included IP address to respond with its MAC address. Once received it is added to the cache.

For a situation where there are mobile devices attached to an access point then the mobiles MAC address is associated with an IP address from within the subnet IP address space. If the mobile device moves to another access point that is in the same subnet then all that is required is for the new access point to realize that it must respond to the MAC address of the mobile device that has just associated itself, and the previous access point to cease to response to that MAC address. The MAC to IP address cache does not need to be changed.

If, however, the mobile device moves to an access point connected to another subnet then the local MAC to IP cache does not apply. The mobile device would typically be required to obtain a new IP address and so break the previous connection. The user of the mobile device is typically re-required to re-establish a stateful end to end connection such as IPSec (IP Security Protocol, an encryption protocol from the Internet Engineering Task Force (IETF), an organized activity of the Internet Society), and so the user may be required to re-register with the WLAN. For example, the user may be required to re-enter a PIN (personal identification number) when connecting to a new subnet.

SUMMARY OF THE INVENTION

To be truly effective, mobile users must be able to move their mobile devices freely from location to location. For example, users must be able to move their

mobile devices from the office to their own conference room to the airport lounge to their client's conference room, while maintaining access to the same set of resources without manually registering anew in each location. They should also be able to send and receive messages and voice calls, wherever they are located. Connection servers, such as routers, WLAN gateways, and security servers, should be able to handle a mobile device that moves its connection to the network from access point to access point, and from public to private networks.

Mobile devices also need to be allocated the appropriate amount of bandwidth to their class of service, and able to find and access the resources they need.

In the case of a BT based network or other wireless local area networks (WLAN), there are likely to be many small coverage areas and many network operators, and users are likely to roam much more frequently from one small coverage area to another. So there is a need for an automatic registration system that registers users as they move from one WLAN coverage area serviced by one wireless base station LAP (LAN access point) to another coverage area serviced by another wireless base station LAP, as well as between coverage areas supported by different security servers and network operators. The solution must be cost effective, but also scalable enough for it to be extendable to many thousands of service providers and millions of users. It is also important to implement the solution only in the network side, to avoid changes to the mobile device such as adding new software or hardware.

In general, the techniques of the invention manage WLAN connectors and maintain context information for connections to enable a user to move a mobile device so that its connection to the network moves from access point to access point, and from public to private networks without requiring re-registration by the user ("seamless roaming"). The solution provided by the invention described herein is an approach that is used by the network operator to enable roaming from subnet to subnet inside that WLAN supported by the network operator. This approach of the invention provided herein describes how to integrate separate WLAN coverage areas so that users of mobile wireless devices may seamlessly roam from location to

location. In particular, it describes how to enable users with Bluetooth devices (or other wireless technologies) to move from wireless access node to another coverage area without requiring the user to re-register. It goes on to describe how independent networks can be linked so as to enable users to move easily between coverage areas managed by different servers and different operators.

With an existing conventional WLAN installation where there are multiple overlapping WLAN's, it is up to the mobile device to decide which WLAN to join, and the mobile device makes this decision irrespective of the loading level of the WLAN or its service level. This conventional approach can lead to a problem of having all the mobiles connected to the nearest access point and none attached to an access point that is further away. The approach of the invention allows directing mobile devices away from busy or highly loaded WLAN's to a WLAN connection that provides better service for the mobile device and less overall congestion.

Thus, the present invention provides a method and system for managing access by a user to a resource over a WLAN by a gateway server. In particular, the method of the system (e.g., gateway server) includes setting access privileges to the resource for a cluster of users of the WLAN and receiving a request from a device controlled by the user to access the resource over the WLAN. The user has a membership in the cluster, and the request includes a user identifier for the user and a device identifier for the device making the request. The membership in a cluster typically reflects the user's role in an organization, such as a student who takes history classes at a university and is thus a member of the history cluster and is allowed access to a database of historical information. In another example, an accountant in a company is a member of a financial cluster and is allowed access to financial records. The method further includes locating access privileges based on the device identifier, the user identifier, and the cluster and authorizing a current session between the device and the resource based on the access privileges. Thus a gateway server can determine the access privileges for a mobile device seeking access to a WLAN based on the cluster the user belongs to.

In another aspect, the present invention provides a method and system (e.g., gateway server) for managing context information for a wireless local area network.

The method includes receiving a request to access the resource over the WLAN, in which the request includes a device identifier for a device making the request and locates context information associated with the device identifier. The context information is associated with a previous session between the device and the resource. The method further includes providing the context information for use in a current session between the device and the resource. Thus the gateway server can reassign context information (e.g., IP address) from a previous session or connection to the mobile device, based on the device identifier without requiring re-registration by the user of the mobile device.

In a further aspect, the present invention provides a method and system (e.g., gateway server) for balancing the load among wireless local area networks. The method includes receiving an indication that a device has established a first connection with a first wireless local area network, the device having a device identifier and determining a user service level associated with the device based on the device identifier and based on a load level for the first wireless local area network in comparison to the load levels associated with each of the other wireless local area networks available for connection by the device. The method further includes directing the device to establish a second connection with a second wireless local area network based on the user service level and the load level of the first wireless local area network, if the second connection provides a preferable balancing of loads among the wireless local area networks. Thus, if the first WLAN that the mobile device connects to is congested, the gateway server can direct the mobile device to another WLAN that should provide a better level of service for the mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The

drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

Fig. 1 illustrates a networked system that enables sharing of cluster access privileges in a WLAN provided by a gateway server configured according to the invention.

Fig. 2 illustrates a networked system that enables roaming of a wireless device between locations supported by a gateway server configured according to the invention.

Fig. 3 illustrates a voice enabled networked system that enables sharing of context information provided by a gateway server configured according to the invention.

Fig. 4 illustrates an example of a gateway server suitable for use in the networked systems of Fig. 1, 2, and 3.

Fig. 5 illustrates an example of a device database suitable for use with the gateway server of Fig. 4.

Fig. 6 illustrates a procedure for authorizing access based on cluster access privileges.

Fig. 7 illustrates a procedure for managing context information in a WLAN.

Fig. 8 illustrates a networked system in a WLAN environment with multiple subnets or channels.

Fig. 9 illustrates a networked system in a WLAN environment with a gateway server and a home server.

DETAILED DESCRIPTION OF THE INVENTION

A description of preferred embodiments of the invention follows.

Fig. 1 illustrates a networked system 20 that enables sharing of cluster access privileges 46 in a WLAN provided by a gateway server 22 configured according to the invention. The networked system 20 includes one or more base stations or LAP's (LAN access points) 24 that provide access to a WLAN, mobile devices 28 (e.g., 28-1, 28-2, and 28-3), home database 32, firewall 34, corporate network 36, Internet 38, and various resources 44. In general, the invention may be used with

any suitable wireless LAN, such as a WLAN based on Bluetooth, IEEE 802.11, ETSI HIPERLAN/2 or similar protocols. The mobile devices 28 are any suitable portable communications device that supports the Bluetooth (or other suitable WLAN protocol such as IEEE 802.11 or ETSI HIPERLAN/2) communications protocol. In a preferred embodiment, the mobile device 28 uses a radio communication frequency greater than 2000 megahertz (e.g., frequencies suitable for Bluetooth , IEEE 802.11, or ETSI HIPERLAN/2). The mobile devices 28 include, for example, a laptop computer 28-1, a PDA (personal digital assistant) 28-2, and a mobile telephone 28-3. The connections 40 (e.g., 40-1, 40-2, and 40-3) are Bluetooth wireless connections established between each mobile device 28-1, 28-2, and 28-3 and the LAP base station 24. The cluster access privileges 46 are access privileges providing access to a resource 44 (e.g., 44-1 or 44-2) from a mobile device 28 over a connection 40 and through the networked system 20. The resource 44-1 may be a server computer, database, or other electronic or computing resource available through the corporate network 36. The resource 44-2 may be a server computer, database, or other electronic or computing resource available through a global network, such as the Internet 38. A resource 44 is not required to be a computer system, but may be a component of a computer system, such as a database or application available on a server computer. The cluster access privileges 46 provide access to a resource 44 or specify the nature of the access, that is, the amount of bandwidth made available to a device 28 by the base station LAP 24 for a user that is a member of the respective cluster, as will be discussed in more detail later. The firewall 34 is a server or other computing device that controls access to the corporate network 36. The home database 32 is a centralized or home database (or computer server with database) that stores security certificates, such as those used to authenticate a user of a mobile device 28.

In a general summary of the operation of the networked system 20, the Bluetooth base station 24 uses a Bluetooth inquiry mode to discover devices 28 within radio communication range (based on frequencies supported by the Bluetooth protocol) of the base station 24, and/or a device 28 uses the inquiry mode to discover if the device 28 is within radio communication range of one or more base

station LAN access points 24 (LAP's) that have advertised their presence within range of the device 28. The mobile device 28 then requests the establishment of a connection 40 to an appropriate LAP 24. A link is established using point to point connections (PPP) 40 over RFCOMM (a serial emulation protocol based on ETSI TS 07.10) and L2CAP (logical link controller adaptation protocol) according to techniques typical for Bluetooth WLAN. For other WLAN protocols such as 802.11b the link is made at protocol level 2 as opposed to protocol level 3 (PPP), so the link establishment is made using the TCP/IP protocol.

For devices 28 requesting Internet only access, then Bluetooth PIN (personal identification number) authentication can be used. The gateway server 22 allocates to the device 28 an IP address that the corporate firewall 34 blocks so as to deny access to the corporate network 36 by the device 28. In one embodiment, the gateway server 22 is a RADIUS (remote authentication dial-in service) server that is typically used to authenticate dial-in access to corporate networks 36 and Internet Service Provides (ISP's) and also provide Bluetooth gateway functionality and SDP (service discovery protocol) functionality.

For devices 28 requiring corporate LAN access, then strong authentication is used based on EAP (Extensible Authentication Protocol) based on a strong system based on SPEKE (Simple Password Authenticated Exponential Key Exchange), Smartcards, or Security Dynamics (e.g., Secure ID token card).

In a preferred embodiment, the gateway server 22 database is extended to map Bluetooth device numbers to "personal clusters" and hence to a person. Logging on one device 28 in a personal cluster can automatically enable all other devices 28 on the same LAP 24 to log on (that are in the same personal cluster) as determined by the users of the devices 28, as will be described in more detail later.

As described above, Fig. 1 illustrates one networked system 20 suitable for use with the gateway server 22 of the invention. Fig. 2 illustrates another networked system 50 suitable for use with the gateway server 22. Fig. 3 illustrates a voice enabled networked system 60 suitable for use with the gateway server 22. Fig. 4 illustrates the gateway server 22 shown in Figs. 1, 2, and 3 in more detail.

Fig. 2 illustrates the networked system 50, which enables roaming of a wireless mobile device 28 (e.g., shown in Fig 2 as PDA mobile device 28-2) between locations supported by the same gateway server 22. In addition to what is illustrated in Fig. 1, Fig. 2 illustrates a conference room base station LAP 24-1, an office base station LAP 24-2, and context information 56 provided from the gateway server 22 to the mobile device 28-2. In a preferred embodiment, the conference room LAP 24-1 is a Bluetooth base station that provides WLAN connections (e.g., connection 40-4) for a conference room (e.g., a conference room in a corporate office or other organizational setting). In a preferred embodiment, the office LAP 24-2 is a Bluetooth base station that provides WLAN connections 40 (e.g., connection 40-5) for one or more offices in a corporate or other organizational setting. The context information 56 is information (e.g., an IP address) associated with a particular mobile device 28-2, such as information indicating the context of an earlier or initial session of the mobile device 28-2 retained (or pointed to) by the gateway server 22, as will be discussed in more detail later.

In reference to Fig 2, roaming occurs as a user moves a mobile device 28-2 from one location to another, for example, from the conference room into an office. For example, first the device 28-2 is authenticated and connected via a PPP connection 40-4 to conference room LAP 24-1. The user moves out of range and so the packet error rate on the connection 40-4 increases rapidly. The PPP controller in the conference room LAP 24-1 clears down the connection 40-4. The user then moves the device 28-2 into range of the office LAP 24-2 and uses inquiry mode to discover the LAP 24-2. The device 28-2 connects to the LAP 24-2 and re-authenticates. The gateway server 22 recognizes the unique device identifier and re-assigns the IP address and configuration from the previous connection 40-4 to the device 28-2 to be used with the new connection 40-5. It also upgrades the user location.

This approach described immediately above will take at least 10 seconds. For more rapid hand-over it is necessary for the conference room LAP 24-1 to signal to the gateway server 22 that it is terminating the connection 40-4, and then for the gateway server 22 to instruct all the local LAP's 24 to page the device 28-2 by name.

Fig. 3 illustrates a networked system 60 that enables communication of a voice enabled device 28 (e.g., shown in Fig. 3 as mobile telephone 28-3) over a WLAN. In addition to what is shown in Fig. 1, Fig. 3 illustrates a Bluetooth voice gateway 52, an H.323 gateway 54, a PSTN 58 (public switched telephone network), a voice enabled Internet resource 44-3, and a PSTN resource 44-4. The Bluetooth voice gateway 52 is adapted to handle voice communications, such as from the mobile telephone 28-3. The voice gateway 52 is one example of a base station LAP 24. The voice gateway 52 is one example of a Bluetooth base station LAP 24. The H.323 gateway 54 is a server that handles voice-based communications between the gateway server 22 and a PSTN 58 or the Internet 38 (based on the ITU-T H.323 standard for video and/or audio transmission over packet switched networks). The gateway server 22 provides context information 56, such as an IP address, that was previously allocated to the mobile telephone in a previous connection (in a manner similar to the use of context information 56 as described for Fig. 2).

In a general summary of the operation of the networked system 60, the voice enabled mobile device 28 registers with a voice gateway LAP 52 connected to a gateway server 22 when in range. The voice gateway LAP 52 authenticates with gateway server 22 and informs an H.323 gateway 54 (connected to a PSTN 58, the Internet 38, or voice-enabled network) of the new user. The H.323 gateway 54 maps the device 28 to a phone number so that the user may receive calls that are made to the user's home H.323 from the PSTN 58 or the Internet 38. Typically, the voice gateway LAP 52 is a separate device from a data only LAP 24 so that voice and data would not normally be on the same subnet (e.g., Bluetooth scatternet).

If the user roams away from voice gateway LAP 52, then a telephone call for the user is received by a centralized home H.323 server which then forwards the call to the relevant H.323 gateway 54 by looking up the current user location in the gateway server 22 (or a centralized security database or server that maintains information or user locations as indicated by local gateway servers 22 or local security servers).

Fig. 4 illustrates an example of a gateway server 22 suitable for use in the networked systems of Fig. 1, 2, and 3. The gateway server 22 includes a digital

processor 70 (e.g., microprocessor), a device database 72 (e.g., stored in a memory or on a hard disk drive) and a communications interface 75. The digital processor 70 hosts and executes a preferred embodiment of a gateway application 74 that manages context information 56 (e.g., IP address 88 allocated to the mobile device 28) for the mobile device 28 and generally manages the connection between the mobile device 28 and the resource 44 (e.g., routes packets between the mobile device 28 and the resource 44) In general, when the gateway server 22 is referred to herein as performing some function, this means that the digital processor 70 of the gateway server 22 is performing that function based on the instructions of the gateway application 74 that is hosted and executing on the digital processor 70. The device database 72 stores device identifiers 76 for mobile devices 28 and, in a preferred embodiment, context information 56 for each device identifier 76. The communications interface 75 includes communications hardware and software that provides communications over network or other connections (wireless or cable) to other entities such as the base station LAP 24 or a server over the Internet. An authentication request 84 is a Bluetooth (or other WLAN) request originating from a mobile device 28 to authenticate the device 28 and establish a connection 40 between the device 28 and a base station LAP 24. The authentication approval with context information 56 is an approval of the authentication request 84 that includes the context information 56 (e.g., IP address previously assigned to the device identifier 76 in an earlier session of the device 24 previously authenticated by the gateway server 22). The cluster access privileges 46 illustrated in Fig. 1 is one example of context information 56.

In one embodiment, a computer program product 80, including a computer readable or usable medium (e.g., one or more CDROM's, diskettes, tapes, etc.), provides software instructions for the gateway application 74 (see Fig. 4). The computer program product 80 may be installed by any suitable software installation procedure, as is well known in the art. In another embodiment, the software instructions may also be downloaded over a wireless connection. A computer program propagated signal product 82 embodied on a propagated signal on a propagation medium (e.g., a radio wave, an infrared wave, a laser wave, a sound

wave, or an electrical wave propagated over the Internet or other network) provides software instructions for the gateway application 74 or any of its components (see Fig. 4). In alternate embodiments, the propagated signal is an analog carrier wave or digital signal carried on the propagated medium. For example, the propagated signal may be a digitized signal propagated over the Internet or other network. In one embodiment, the propagated signal is a signal that is transmitted over the propagation medium over a period of time, such as the instructions for a software application sent in packets over a network over a period of milliseconds, seconds, minutes, or longer. In another embodiment, the computer readable medium of the computer program product 80 is a propagation medium that the computer may receive and read, such as by receiving the propagation medium and identifying a propagated signal embodied in the propagation medium, as described above for the computer program propagated signal product 82.

Fig. 5 illustrates an example of a device database 72 suitable for use with the gateway server 22 of Fig. 4. The device database 72 includes device identifiers 76-1, 76-2, and 76-3. The device identifier 76 is a unique identifier or address for the mobile device 28, such as unique unit identifier for a particular device, a MAC (Media Access Control) address, other network address, or other identification information that uniquely identifies a particular mobile device 28 from any other mobile device 28. The context information 56 includes IP addresses 88 (e.g., 88-1, 88-2, and 88-3) and pointers to cluster information 90 (e.g., 90-1, 90-2, and 90-3). Each IP address 88 (e.g., 88-1, 88-2, and 88-3) and pointer to cluster information 90 (e.g., 90-1, 90-2, and 90-3) are associated with a device identifier 76 (e.g., 76-1, 76-2, and 76-3). The term "pointer to cluster information" uses the term "pointer" in a general sense to indicate a pointer, reference, address, or other indication of where the cluster information 96 is located. Generally, the cluster information 96 may be obtained on a cluster information database 94 associated with the gateway server 22, or in a cluster information database 94 associated with another server, computer, or data server, as will be discussed in more detail later.

The device database 72 also stores user identification information 92 (e.g., 92-1, 92-2, and 92-3) associated with each device ID 76 (e.g., 76-1, 76-2, and 76-3),

as shown in Fig. 5. The user identification information 92 includes information identifying or related to a user of a mobile device 28, such as a unique user identifier or a user PIN (Personal Identity Number). The user identification information 92 may also include other user information, such as the user service level (e.g., allocated WLAN bandwidth) if such information is not determined by the cluster access privileges 46. In one embodiment, the user identification information 92 is used by the gateway server 22 but not necessarily stored or retained in the device database 72 after it is used.

Fig. 6 illustrates a procedure for authorizing access based on cluster access privileges 46. In step 200, the security server identifies users that belong to a cluster (e.g., perform similar roles in an organization). Typically, membership in a cluster reflects a role in an organization such as an accountant in a business or a student in a university. For example, students majoring or taking courses in history at a university are members of a history cluster, and students majoring or taking courses in engineering are members of an engineering cluster. In one embodiment, cluster information 96 (that indicates the members of a cluster and the corresponding cluster access privileges 46 for all members of the cluster) are stored on the gateway server 22. In another embodiment, the cluster information 96 and cluster access privileges 46 are stored in a cluster information server separate from the gateway server 22. For example, the information for the history cluster may be stored in a history server (i.e., server computer providing database and other support to the history department). The pointer to the cluster information 90 (as shown in Fig. 5) thus points to a database on the history server having the cluster information 96 and access privileges 46 for the cluster of history students.

In step 202, the gateway server 22 sets access privileges 46 to a resource for a cluster of users in a WLAN. In one embodiment, the gateway server 22 sets the access privileges 46 based on input from an operator. For example, an operator in a history department sets the access privileges 46 for the history cluster of students by entering data at a keyboard at the history server. In such a case, the access privileges 46 may include access to databases of course materials and reference materials in the history server (but not to allow access to course materials and reference materials on

databases on servers of other department's computers). The history server is one example of a resource 44. Furthermore, access privileges 46 may specify a bandwidth allocation on the WLAN for each mobile device 28 used by a member of the history cluster that may be different for the bandwidth allocation on the WLAN for mobiles devices of students in other clusters, such as the engineering cluster.

In step 204, the gateway server 22 receives a request from a mobile device 28 controlled by a user who is a member of a cluster to access the resource 44-2. The request includes a user identifier 92 and a device identifier 76. Typically, the request originates from a mobile device 28 to the LAP base station 24, which then passes on the request (as an authentication request) to the gateway server 22.

In step 206, the gateway server 22 locates access privileges 46 based on the device identifier 76, user identifier 92, and the cluster information 96. As described earlier, the cluster information 96 may be stored in a cluster information database 94 associated with the gateway server 22 or another server.

In step 208, the gateway server 22 authorizes a current session over the WLAN between the mobile device 28 and the resource 44 based on the access privileges 46. For example, the gateway server 22 authorizes access to databases on a particular server, such as the history department server, and/or authorizes a certain level of WLAN bandwidth to be allocated to the mobile device 28 that originated the request.

Fig. 7 illustrates a procedure for managing context information 56 in a WLAN. In step 300, the gateway server 22 authorizes an initial session from a user's mobile device 28 over a WLAN to a resource 44. Typically, the mobile device 28 is then able to communicate with the resource through a networked system, such as the networked system 50 shown in Fig. 2.

In step 302, the gateway server 22 provides a context for the session (e.g., allocates an IP address 88 for use by the device 28). For example, the gateway server 22 dynamically allocates an IP address 88 for use by the mobile device 28 or requests such an allocation from a DHCP (Dynamic Host Configuration Protocol) server. The gateway server 22 may also allocate or specify other information, such as configuration information for the session or the connection 40.

In step 304, the gateway server 22 saves the context information 56 for the session (e.g., IP address 88 and other information) based on the device identifier 76, after a disconnection that interrupts the session between the mobile device 28 and the resource 44. For example, the user moves the mobile device 28 from one location to another, as from a conference room to an office, as shown in Fig. 2. The gateway server 22 stores the IP address 88 in a device database 72 and associates the IP address 88 with the device identifier 76 of the mobile device 28.

In step 306, the gateway server 22 receives a request (including device identifier 76) to access the resource 44 from the mobile device 28 over the WLAN. For example, the user moves the mobile device 28-2 from a conference room to an office out of range of the conference room LAP 24-1 (as shown in Fig. 2), where the mobile device 28-2 comes within range of an office LAP 24-2. Through Bluetooth (or other WLAN protocol) inquiry mode, the mobile device 28-2 seeks to establish a connection with the office LAP 24-2 and obtain renewed access to the resource 44. The office LAP 24-2 communicates with the gateway server 22, providing the request for the mobile device 28-2 to access the resource 44.

In step 308, the gateway server 22 locates the context information 56 (e.g., IP address 88) associated with the device identifier 76 for the initial session between the mobile device 28 and the resource 44. For example, the gateway server 22 looks up the context information 56 in the device database 72 associated with the gateway server 22 and locates the IP address 88-2 associated with a specific mobile device 28-2, as well as other information such as the pointer to the cluster information 90-2 if needed.

In step 310, the gateway server 22 provides the context information 56 (e.g., IP address 88) for use in the current session between the mobile device 28 and the resource 44. For example, the gateway server 22 retrieves the IP address 88-2 associated with the mobile device 28-2 from the device database 72 and reassigns the IP address 88-2 to the mobile device 28-2.

The gateway server 22 may also serve as a centralized security server or clearinghouse (or provide a connection) to such a central server. Such a central security server provides context information 56 (e.g., IP address 88) to different

providers of WLAN services. The providers use the context information 56 directly or provides it to local security servers 22 so that users of mobile device may roam to WLAN's provided by different service providers while retaining context information 56 such as an IP address 88 allocated to the mobile device during initial session or connection 40 to a WLAN.

In a preferred embodiment, in which the device identifier 76 is based on a MAC address for the mobile device, the gateway server 22 is a conventional RADIUS server that is extended so that it contains a version of the MAC to IP address cache (e.g., device database 72) that is used by the gateway application 74 to map MAC addresses to IP addresses. In the preferred embodiment, the gateway server 22 recognizes the unique device identifier 76 (in this case the MAC address) and re-assigns the same IP address 88 and configuration. It upgrades the user location, as described in more detail below.

When a mobile device 28 moves to a new subnet, the newly associated LAP 24 starts to answer for the MAC address of the mobile device 28, and also to send out packets to the gateway server 22 with the MAC address of the mobile device. In this case the gateway server 22 is actually a combined router and RADIUS server, as shown in Fig. 4 (perhaps with a centralized database).

In another preferred embodiment, the RADIUS functionality is implemented as a separate RADIUS server that includes the device database 72 (with device identifiers 76 based on the MAC address and corresponding IP addresses 88), and the gateway server 22 hosts and executes the gateway application 74. In this embodiment, the gateway server 22 detects that the packet comes from a mobile device 28 whose MAC address is not part of its subnet cache, and so looks it up in the RADIUS server MAC to IP table (e.g., device database 72). Once found it enters it in its local cache, and updates the RADIUS server with the new location. It also informs the previous gateway server 22 that manages the subnet for the previous connection of the mobile device 28 that the mobile device 28 has moved. The previous gateway server 22 then alerts its routing table so that packets addressed to that IP address 88 are forwarded to the new gateway server 22 for delivery to the mobile device 28.

Fig. 8 illustrates a networked system 100 in a WLAN environment with multiple channels. Fig. 8 illustrates a gateway server 22 with a connection to the Internet 38, and connections to two base station LAP's 24-3 and 24-4, which have connections 40-7 and 40-8 to user mobile devices 28-4 and 28-5. Mobile device 28-4 is part of scatternet 102-1 and mobile device 28-5 is part of scatternet 102-2. The scatternet 102 is a WLAN channel, such as a Bluetooth scatternet. A scatternet 102 is made up of piconets connected together by a data relay that transfers data packets between piconets so as to transfer the data packets between the mobile device 28 and the LAP 24. Scatternets 102 enable one shared channel of a Bluetooth network to cover a larger physical area. In the IEEE 802.11 protocol the same concept applies, but the term channel is applied in place of piconet, and scatternets 102 can be built by linking IEEE 802.11 channels together using a relay device. The invention is described in terms of scatternets 102 but also works in a piconet because a piconet is the most simple implementation of a scatternet 102. Each scatternet 102-1 and 102-2 may have a larger number of users than is shown is Fig. 8, which shows only one representative mobile device 28-4 or 28-5 per scatternet 102 -1 or 102-2.

In a crowded environment such as a conference room there may well be multiple devices 28 desiring high speed WLAN access. Maximum asymmetric capacity per scatternet 102 (e.g., Bluetooth scatternet) is 721 kbps up (or down) and 56kbps up (or down) but this is split between the seven active users (for a scatternet 102 that is limited to this number of users). In Bluetooth, a scatternet 102 is two or more channels (Bluetooth piconets) co-located in the same area. Symmetric mode gives 460 kbps in each direction. Operating 10 scatternets 102 in the same location only reduces throughput per scatternet 102 to around 650 kbps, so for best performance users should be spread between scatternets 102. Users should also be assigned to symmetric or asymmetric scatternets 102 according to their traffic pattern. They can also obtain faster speeds (1.4 Mbps) by being assigned multiple parallel channels using multi-channel (as used for ISDN).

Users can choose which scatternet 102 to join by signaling busy scatternets 102 via the loading variable in the SDP (service discovery protocol). Users can be directed to join a particular scatternet 102 by signaling "busy" scatternet 102 via the

loading variable in the radio protocol header. Not all users may pay attention, and it may be desirable to introduce different levels of service for different users.

In operation, the mobile device 28 requests service from a LAP 24 by sending a request along with its device address (e.g., device identifier 76). The LAP 24 (which is a scatternet master) would normally simply respond by paging the device 28 and starting the synchronization. Instead, in the present invention, the LAP 24 passes the request along with the device address (i.e., device identifier 76) back to the gateway server 22 which looks up the user's service level 104 and the loading on each of the relevant scatternets 102 in accordance with the procedure illustrated in Fig. 6. The user's service level 104 is an example of a cluster access privilege 46 or context information 56. The gateway server 22 then signals to the appropriate LAP 24 to page the device 28 (this may not be the LAP 24 that received the request).

When a mobile device 28 has mobile radio interfaces (that is, both a Bluetooth interface and a 802.11b interface) or can participate in one of a number of overlapping channels (which is the general case of a scatternet 102), then when the mobile device 28 moves to a new channel and starts to send packets, the gateway server 22 looks up the device 28 in the device database 72, and according to the user service level and scatternet loading (e.g., traffic or congestion on the subnet that the mobile device is connected to) might decide that the mobile device 28 should be communicating via another channel that is covering that mobile device 28. The mobile device 28 may be directed to a different channel (e.g., Bluetooth piconet) within a scatternet 102, or to a different scatternet 102. In that case the mobile device 28 is forced to transfer its connection 40. For example, mobile device 28-4 is seeking to make a new connection to one of the scatternets 102-1 or 102-2 in Fig. 8. First the mobile device 28-4 seeks to make a connection to congested scatternet 102-2. The gateway server 22 thus directs the mobile device 28-4 to join a less congested scatternet 102-1, with the result shown by connection 40-7 in Fig. 8. Subsequently, mobile device 28-4 access to resources 44 is provided without requiring re-registration with the gateway server 22, following the procedure of Fig. 7.

Fig. 9 illustrates a networked system 110 in a WLAN environment with a gateway server 22 and a home server 112. The home server 112 is a network (e.g.,

Internet) server computer that provides authentication services, such as RADIUS authentication services, for a user with a mobile device 28 seeking access to a resource 44-2 available on the networked system 110. The home server 112 functions as a home or base server for the user of the mobile device 28, and may provide cluster information 46 or context information 56 (as described previously).

In an example of using a home server 112, the user of a mobile device 28 first initiates a log on to a remote network, and indicates a desire to use restricted or "for charge" resources 44-2. The mobile device 28 starts an authentication session with the local gateway server 22. The mobile device 28 supplies the name of the home server 112 as part of the user identification during the authentication process (e.g., user@radius5.employer.com). The local gateway server 22 authenticates the user with the user's home server 112, passing back to the home server 112 the location (base station LAP 24 and network), IP address, and billing information.

This completes the registration of the mobile device 28 with the home server 112, which stores the mobile device 28 IP address and location of the mobile device 28. The user (i.e., device owner) may also set up a list of preferences indicating who is allowed to know the location of the mobile device 28 and which messages are allowed to be forwarded to the mobile device 28.

In one embodiment, the home server 112 (or other central authentication server) can act as a central roaming clearing house for companies and Bluetooth (or other wireless protocol) ISP's that provide WLAN services. The WLAN operator then needs only have one authentication and billing agreement with the central server (e.g., home server 112). Users are billed by their home network provider (e.g., ISP or corporation). Users that do not have a "home" who wish to use a free service (e.g., Internet access) can register with the central or home server 112 so that they can be authenticated but not charged.

While this invention has been particularly shown and described with references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.

CLAIMS

What is claimed is:

1. A method for authorizing access by a user to a resource over a wireless local area network, comprising the steps of:

setting access privileges to the resource for a cluster of users of the wireless local area network;

receiving a request from a device controlled by the user to access the resource over the wireless local area network, the user having a membership in the cluster, and the request including a user identifier for the user and a device identifier for the device making the request;

locating access privileges based on the device identifier, the user identifier, and the cluster; and

authorizing a current session between the device and the resource based on the located access privileges.

2. A system comprising a digital processor for authorizing access by a user to a resource over a wireless local area network, the system comprising:

a gateway application executing on the digital processor for setting access privileges to the resource for a cluster of users of the wireless local area network; and

a communications interface coupled with the digital processor for receiving a request from a device controlled by the user to access the resource over the wireless local area network, the user having a membership in the cluster, and the request including a user identifier for the user and a device identifier for the device making the request,

the gateway application being responsive to the received request and locating access privileges based on the device identifier, the user identifier, and the cluster and the gateway application authorizing a current session between the device and the resource based on the located access privileges.

3. A computer program product that includes a computer usable medium having computer program instructions stored thereon for authorizing access by a user to a resource over a wireless local area network, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

set access privileges to the resource for a cluster of users of the wireless local area network;

receive a request from a device controlled by the user to access the resource over the wireless local area network, the user having a membership in the cluster, and the request including a user identifier for the user and a device identifier for the device making the request;

locate access privileges based on the device identifier, the user identifier, and the cluster; and

authorize a current session between the device and the resource based on the located access privileges.

4. A method for managing context information for a wireless local area network, comprising the steps of:

receiving a request to access the resource over the wireless local area network, the request including a device identifier for a device making the request;

locating context information associated with the device identifier, the context information associated with a previous session between the device and the resource; and

providing the context information for use in a current session between the device and the resource.

5. The method of Claim 4, wherein the wireless local area network is based on a radio frequency suitable for use in local wireless communications.

6. The method of Claim 4, wherein communications over the wireless local area network are based on a spread-spectrum technique based on a carrier frequency greater than about 2,000 megahertz.

7. The method of Claim 4, wherein the device identifier is a unique identification number.

8. The method of Claim 4, wherein the context information includes an internet protocol address assigned to the device in the previous secure session.

9. The method of Claim 4, wherein the context information includes cluster information associated with a user of the device for the current session, the user having a membership in the cluster, and the cluster information providing access privileges associated with a member of the cluster who set the access privileges for the cluster in a previous request to access the resource.

10. The method of Claim 4, wherein the device is a voice-enabled communications device, and the gateway server is adapted for voice-enabled network communications.

11. A system comprising a digital processor for managing context information for a wireless local area network, the system comprising:

a communications interface coupled with the digital processor for receiving a request to access the resource over the wireless local area network, the request including a device identifier for a device making the request; and

a gateway application executing on the digital processor, in response to the received request, the gateway application locating context information associated with the device identifier, the context information associated with a previous session between the device and the resource, and providing the context information for use in a current session between the device and the resource.

12. The system of Claim 11, wherein the wireless local area network is based on a radio frequency suitable for use in local wireless communications.

13. The system of Claim 11, wherein communications over the wireless local area

network are based on a spread-spectrum technique based on a carrier frequency greater than about 2,000 megahertz.

14. The system of Claim 11, wherein the device identifier is a unique identification number.

15. The system of Claim 11, wherein the context information includes an internet protocol address assigned to the device in the previous secure session.

16. The system of Claim 11, wherein the context information includes cluster information associated with a user of the device for the current session, the user having a membership in the cluster, and the cluster information providing access privileges associated with a member of the cluster who set the access privileges for the cluster in a previous request to access the resource.

17. The system of Claim 11, wherein the device is a voice-enabled communications device, and the gateway server is adapted for voice-enabled network communications.

18. A computer program product that includes a computer usable medium having computer program instructions stored thereon for managing context information for a wireless local area network, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

receive a request to access the resource over the wireless local area network, the request including a device identifier for a device making the request;

locate context information associated with the device identifier, the context information associated with a previous session between the device and the resource; and

provide the context information for use in a current session between the device and the resource.

19. A method for balancing a load among a plurality of wireless subnetworks, comprising the steps of:

receiving an indication that a device has established a first connection with a first wireless subnetwork, the device having a device identifier;

determining a user service level associated with the device based on the device identifier and based on a load level for the first wireless subnetwork in comparison to load levels associated with each of the other wireless subnetworks available for connection by the device; and

if a second connection provides a preferable balancing of load levels among the wireless subnetworks, then directing the device to establish the second connection with a second wireless subnetwork based on the determined user service level and the load level of the first wireless subnetwork,

20. A system comprising a digital processor for balancing a load among a plurality of wireless subnetworks, the system comprising:

a communications interface coupled with the digital processor for receiving an indication that a device has established a first connection with a first wireless subnetwork, the device having a device identifier; and

a gateway application executing on the digital processor for determining a user service level associated with the device based on the device identifier and based on a load level for the first wireless subnetwork in comparison to load levels associated with each of the other wireless subnetworks available for connection by the device, and in response to a second connection providing a preferable balancing of the load levels among the wireless subnetworks, the gateway application directing the device to establish a second connection with a second wireless subnetwork based on the user service level and the load level of the first wireless subnetwork.

21. A computer program product that includes a computer usable medium having computer program instructions stored thereon for balancing load among a plurality of wireless subnetworks, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

receive an indication that a device has established a first connection with a first wireless subnetwork, the device having a device identifier;

determine a user service level associated with the device based on the device identifier and based on a load level for the first wireless subnetwork in comparison to load levels associated with each of the other wireless subnetworks available for connection by the device; and

direct the device to establish a second connection with a second wireless subnetwork based on the user service level and the load level of the first wireless subnetwork, if the second connection provides a preferable balancing of load levels among the wireless subnetworks.

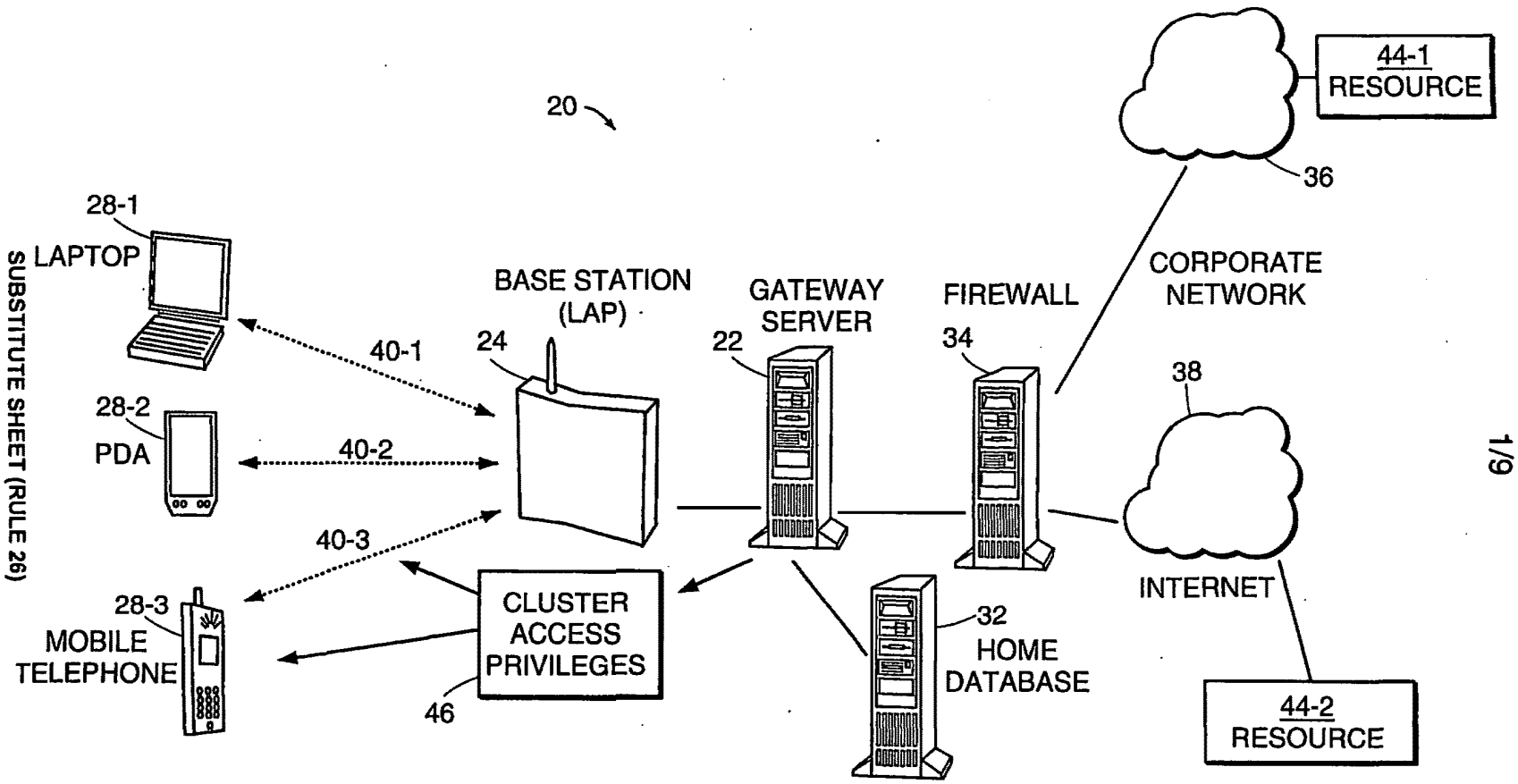


FIG. 1

SUBSTITUTE SHEET (RULE 26)

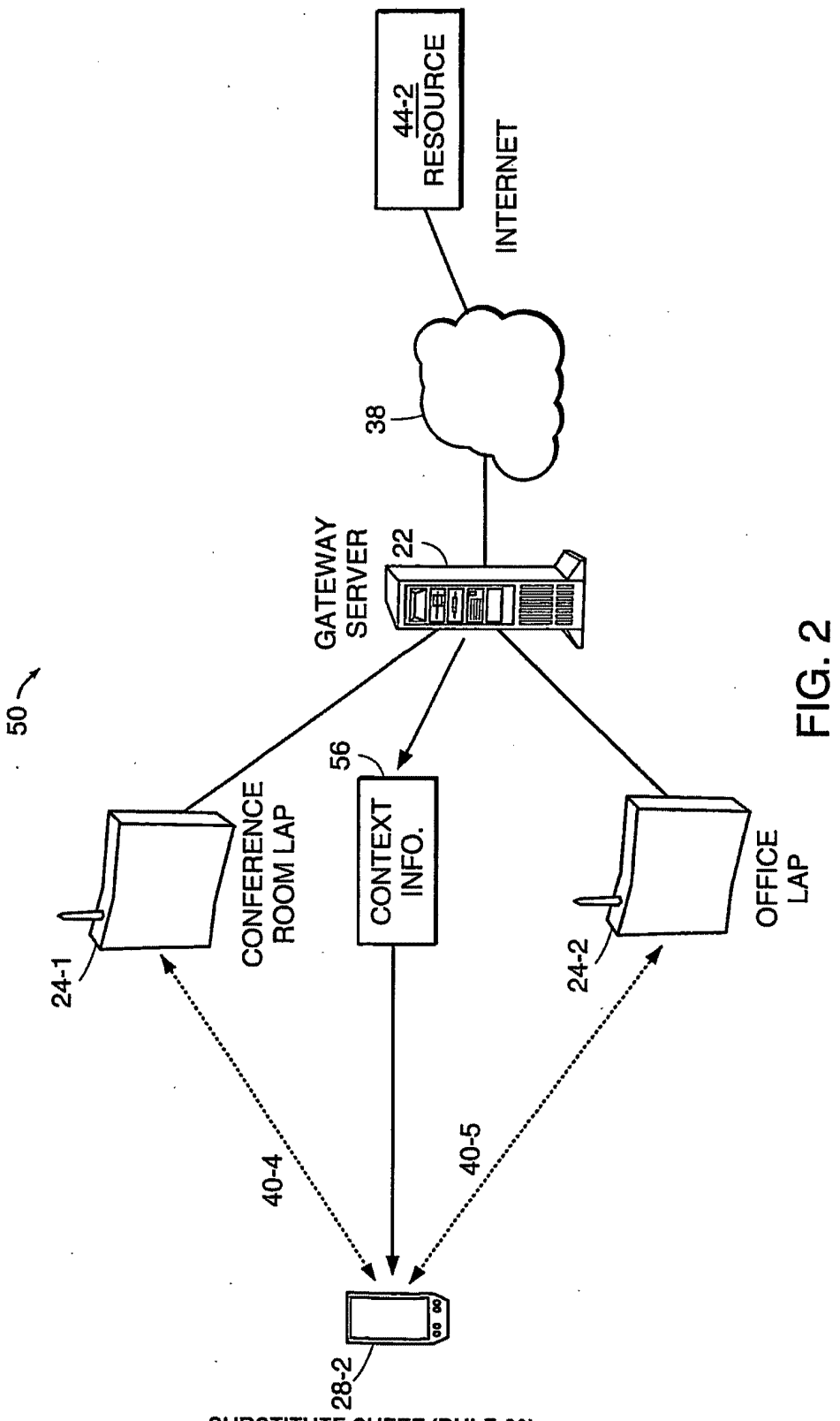

44-2
RESOURCE
INTERNET
38
GATEWAY
SERVER
22
50
56
CONTEXT
INFO.
CONFERENCE
ROOM LAP
OFFICE
LAP
24-1
24-2
40-4
40-5
28-2

FIG. 2

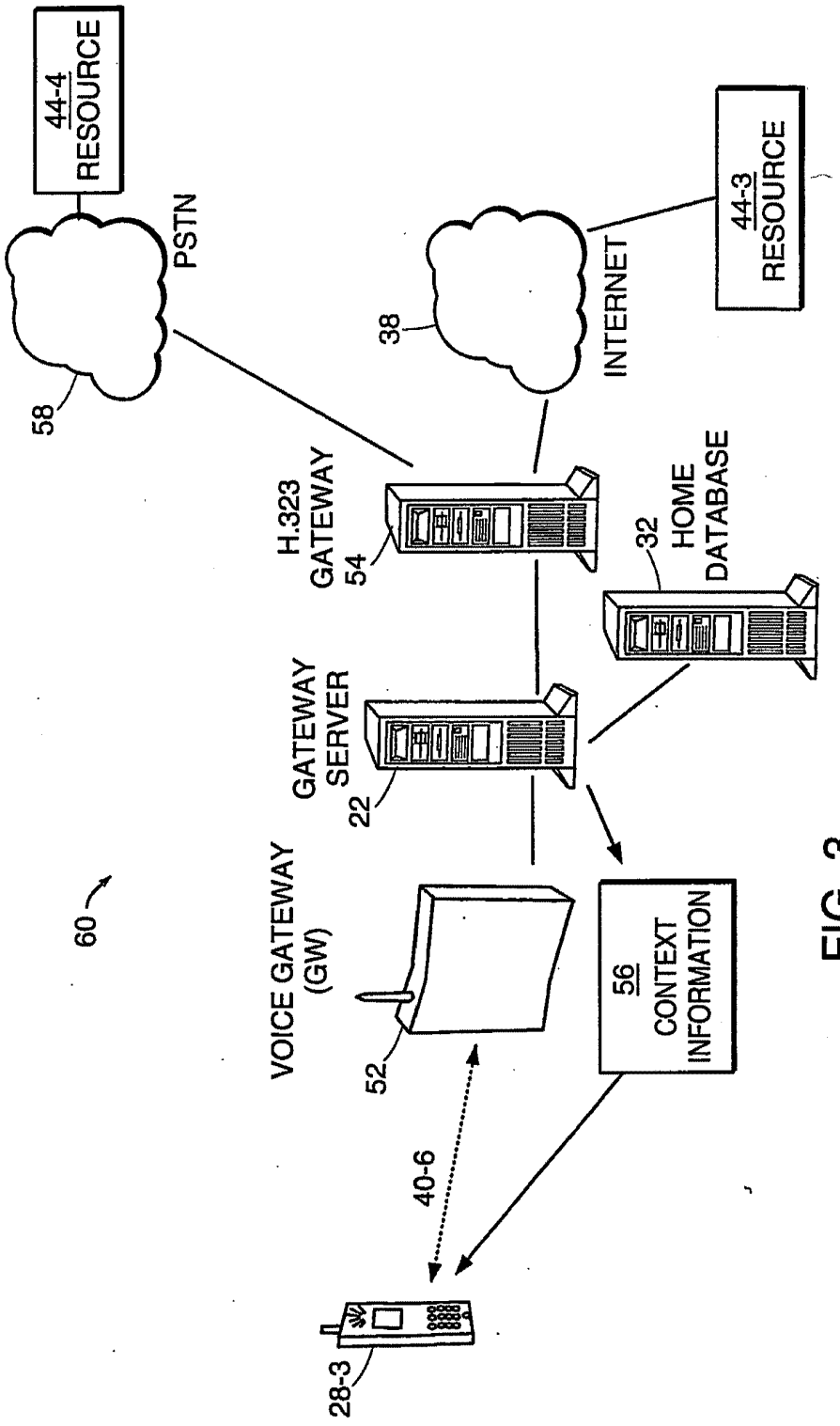


FIG. 3

FORTINET EX1002 Page 150

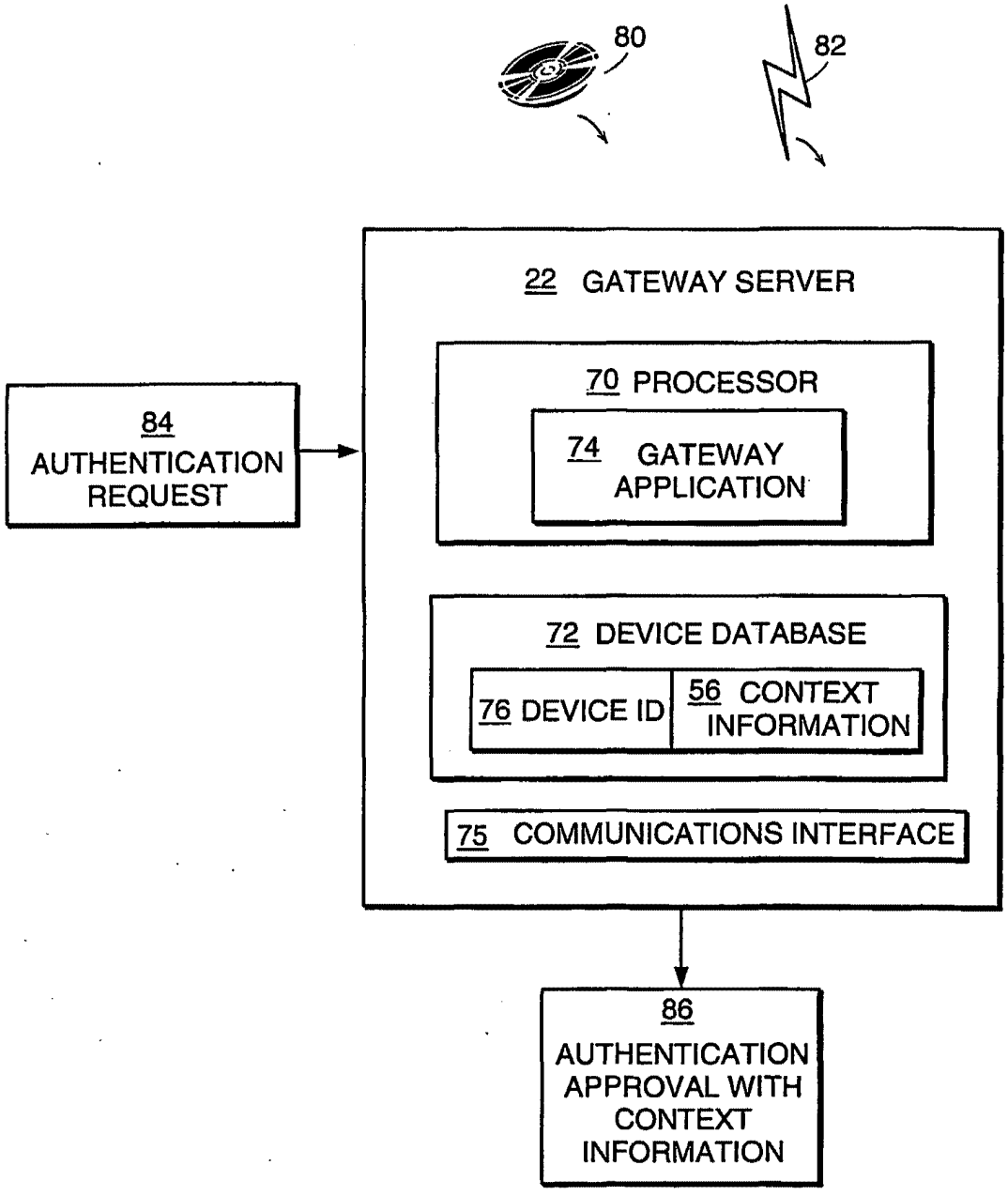

80
82
22 GATEWAY SERVER
70 PROCESSOR
74 GATEWAY APPLICATION
84 AUTHENTICATION REQUEST
72 DEVICE DATABASE
76 DEVICE ID
56 CONTEXT INFORMATION
75 COMMUNICATIONS INTERFACE
86 AUTHENTICATION APPROVAL WITH CONTEXT INFORMATION

FIG. 4

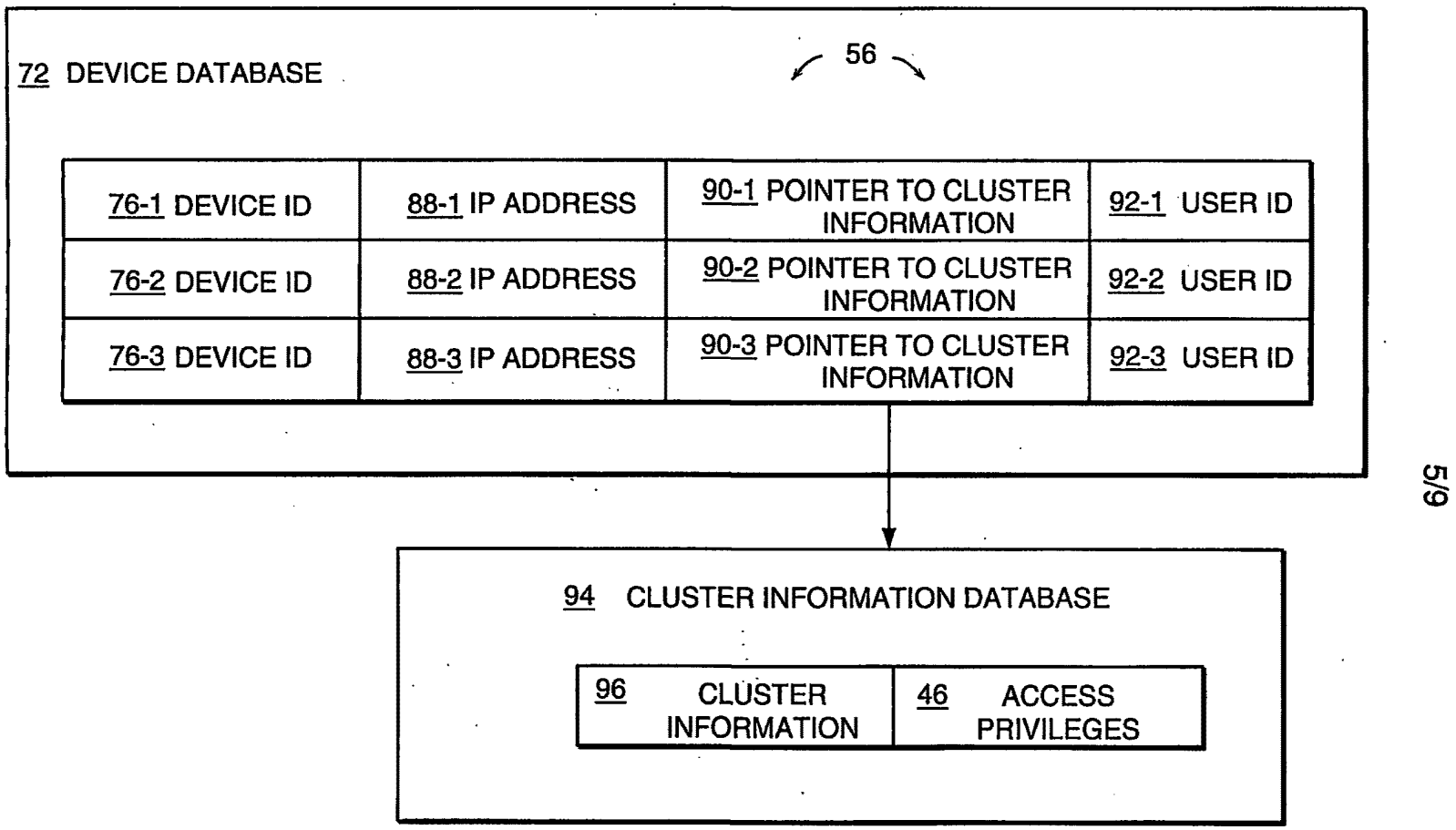


FIG. 5

SUBSTITUTE SHEET (RULE 26)

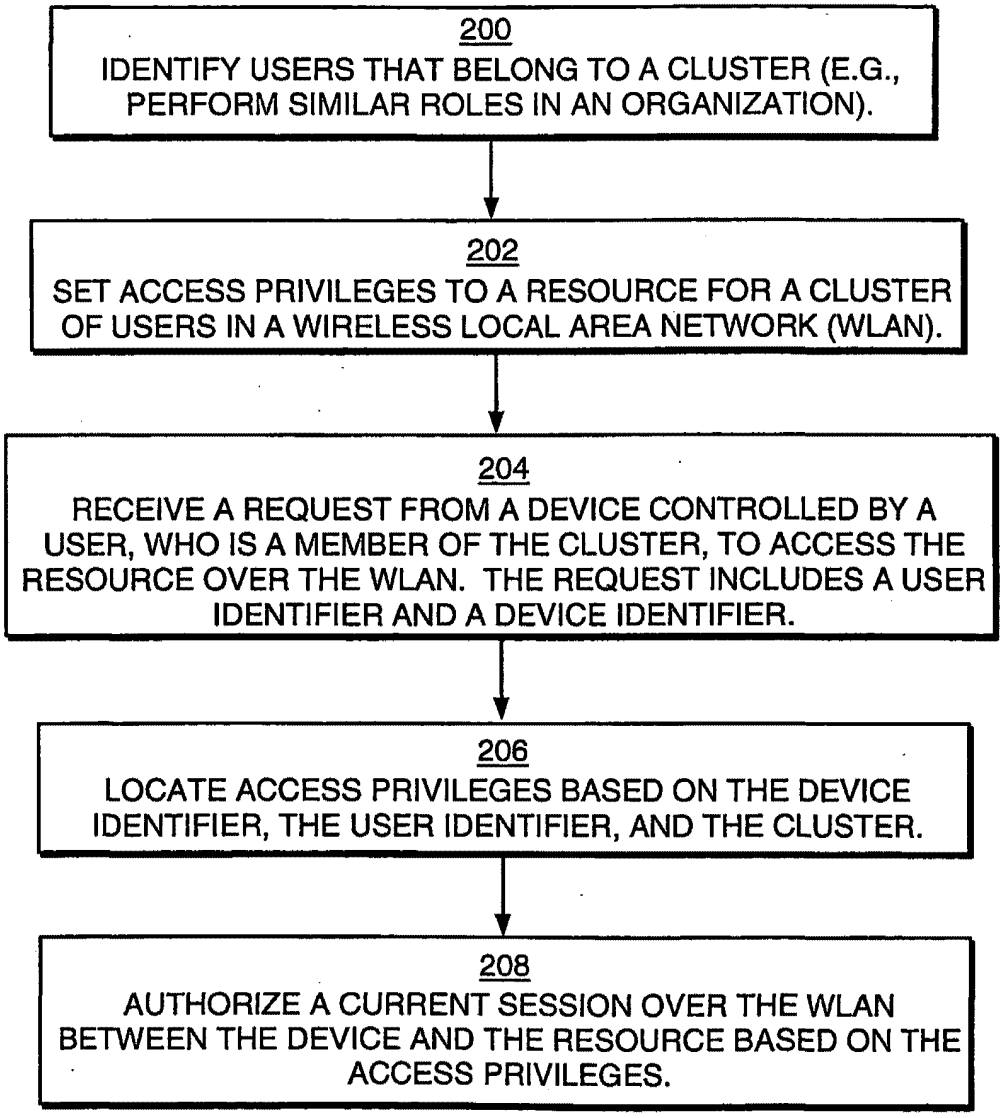

200
IDENTIFY USERS THAT BELONG TO A CLUSTER (E.G., PERFORM SIMILAR ROLES IN AN ORGANIZATION).
202
SET ACCESS PRIVILEGES TO A RESOURCE FOR A CLUSTER OF USERS IN A WIRELESS LOCAL AREA NETWORK (WLAN).
204
RECEIVE A REQUEST FROM A DEVICE CONTROLLED BY A USER, WHO IS A MEMBER OF THE CLUSTER, TO ACCESS THE RESOURCE OVER THE WLAN. THE REQUEST INCLUDES A USER IDENTIFIER AND A DEVICE IDENTIFIER.
206
LOCATE ACCESS PRIVILEGES BASED ON THE DEVICE IDENTIFIER, THE USER IDENTIFIER, AND THE CLUSTER.
208
AUTHORIZE A CURRENT SESSION OVER THE WLAN BETWEEN THE DEVICE AND THE RESOURCE BASED ON THE ACCESS PRIVILEGES.

FIG. 6

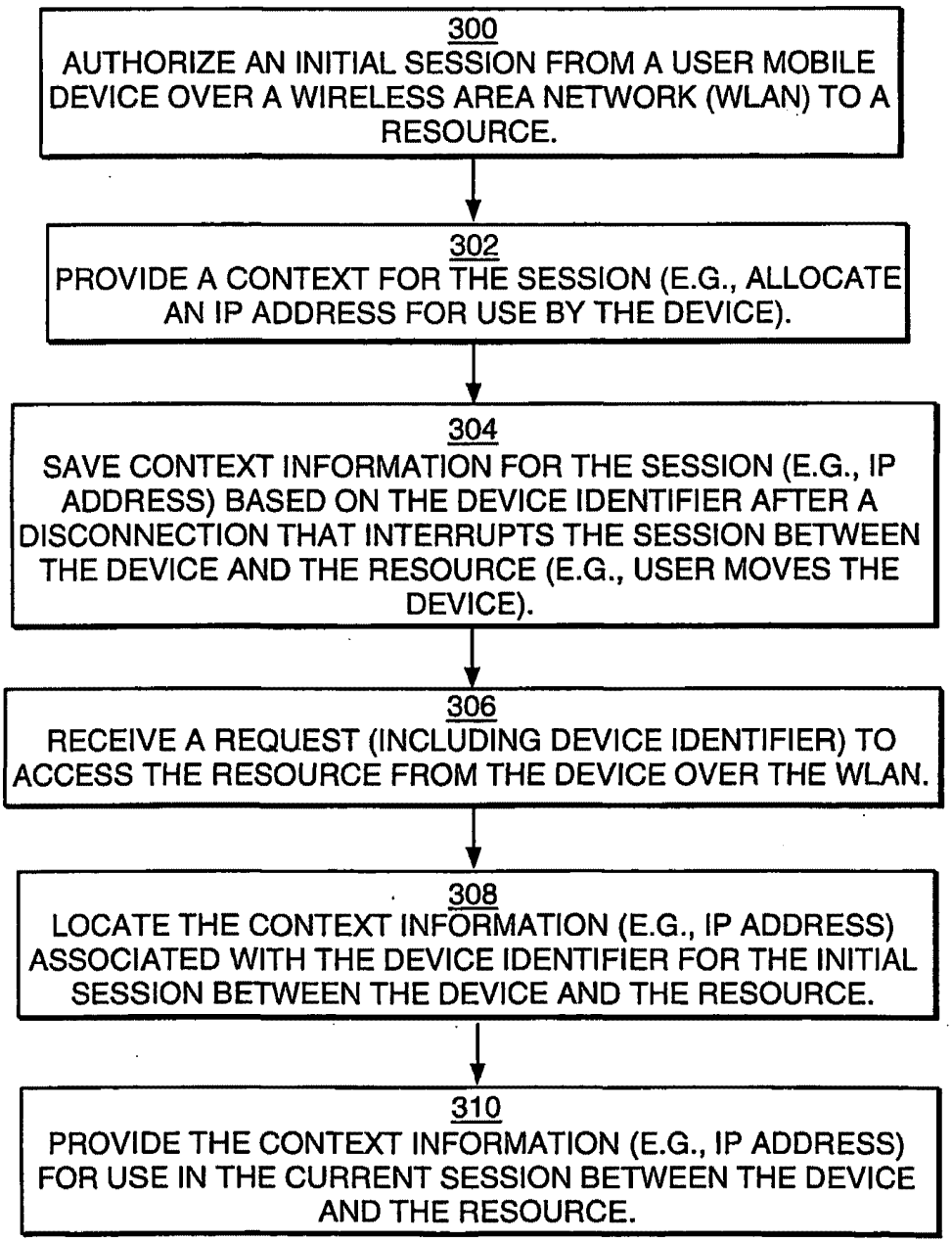

300
AUTHORIZE AN INITIAL SESSION FROM A USER MOBILE DEVICE OVER A WIRELESS AREA NETWORK (WLAN) TO A RESOURCE.
302
PROVIDE A CONTEXT FOR THE SESSION (E.G., ALLOCATE AN IP ADDRESS FOR USE BY THE DEVICE).
304
SAVE CONTEXT INFORMATION FOR THE SESSION (E.G., IP ADDRESS) BASED ON THE DEVICE IDENTIFIER AFTER A DISCONNECTION THAT INTERRUPTS THE SESSION BETWEEN THE DEVICE AND THE RESOURCE (E.G., USER MOVES THE DEVICE).
306
RECEIVE A REQUEST (INCLUDING DEVICE IDENTIFIER) TO ACCESS THE RESOURCE FROM THE DEVICE OVER THE WLAN.
308
LOCATE THE CONTEXT INFORMATION (E.G., IP ADDRESS) ASSOCIATED WITH THE DEVICE IDENTIFIER FOR THE INITIAL SESSION BETWEEN THE DEVICE AND THE RESOURCE.
310
PROVIDE THE CONTEXT INFORMATION (E.G., IP ADDRESS) FOR USE IN THE CURRENT SESSION BETWEEN THE DEVICE AND THE RESOURCE.

FIG. 7

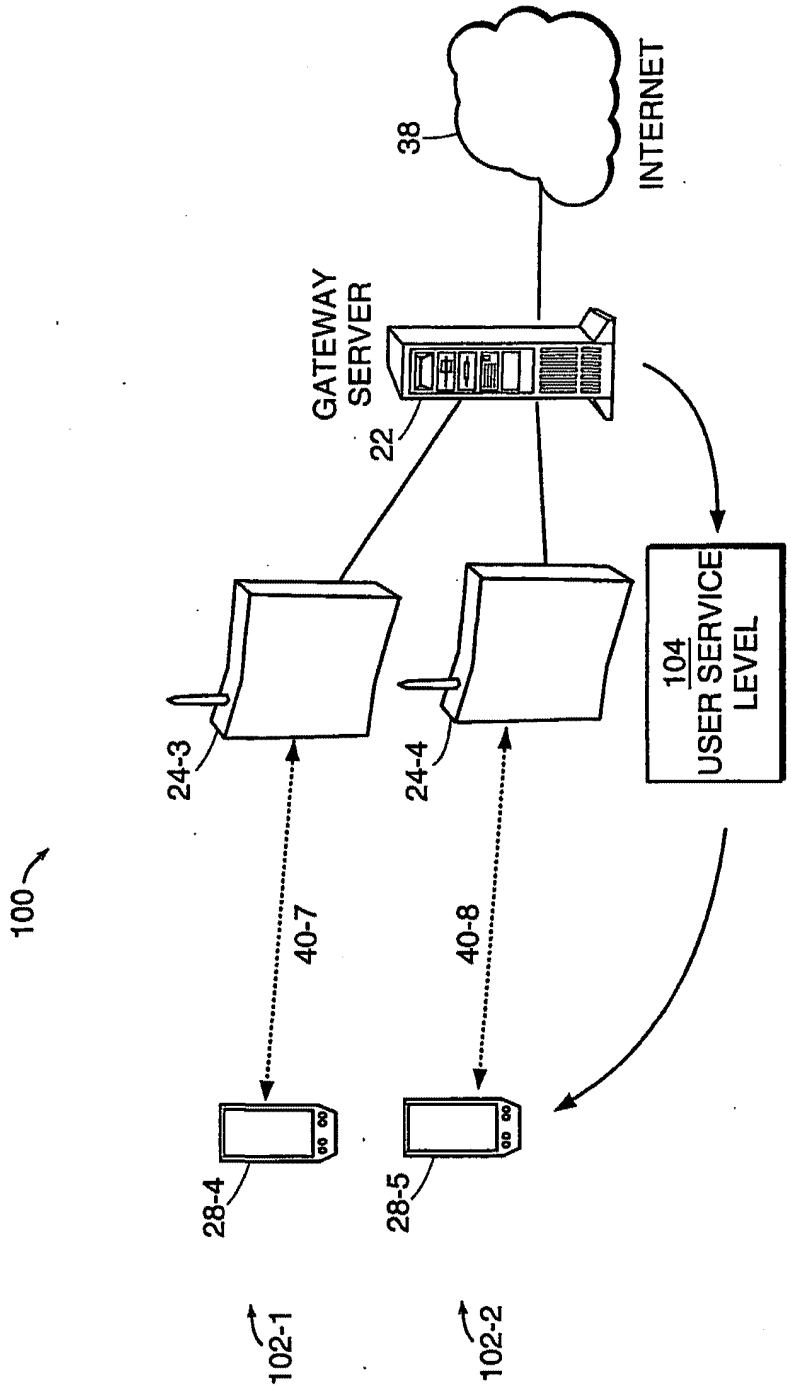

INTERNET
38
GATEWAY SERVER
22
104
USER SERVICE LEVEL
24-3
24-4
40-7
40-8
28-4
28-5
102-1
102-2
100

FIG. 8

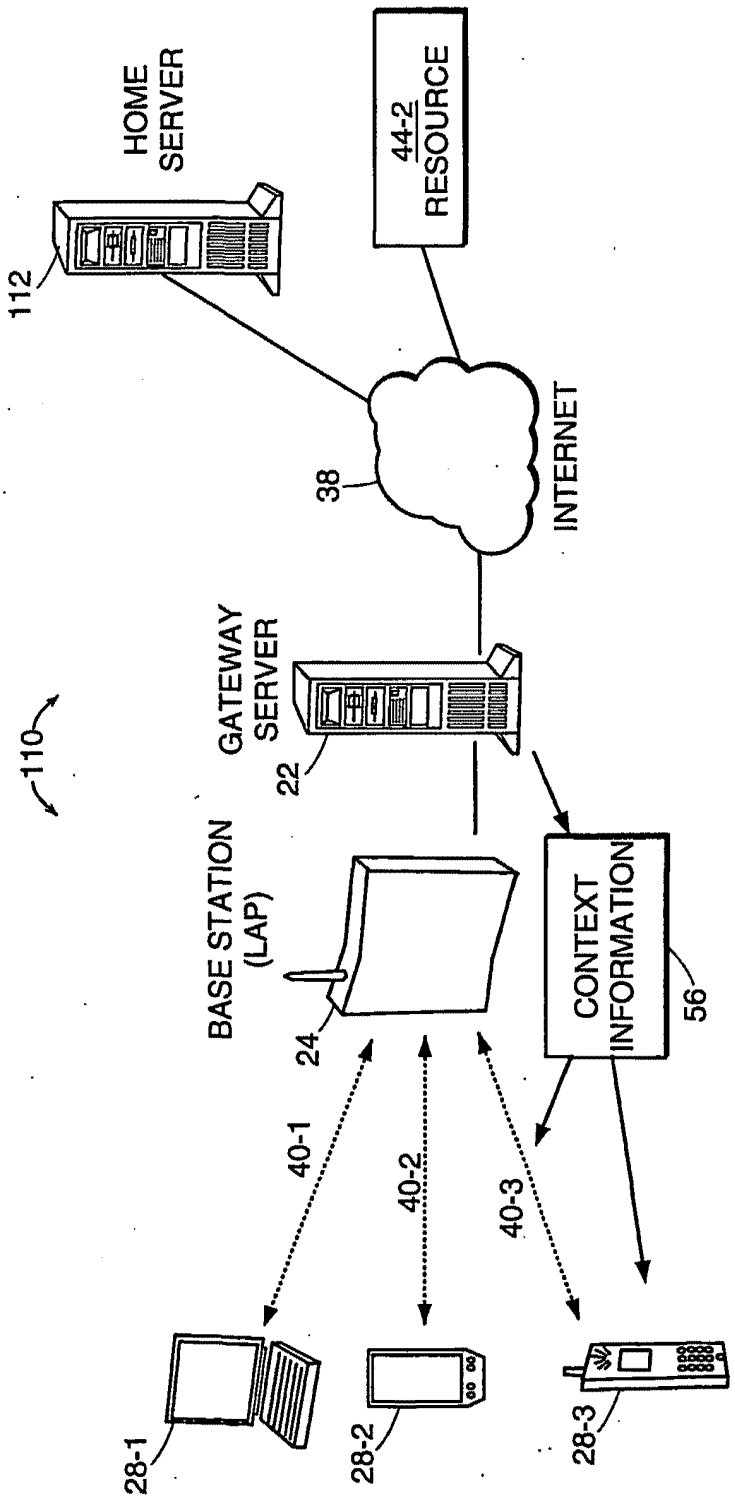

HOME SERVER
112
44-2 RESOURCE
38
INTERNET
GATEWAY SERVER
22
110
BASE STATION (LAP)
24
CONTEXT INFORMATION
56
40-1
40-2
40-3
28-1
28-2
28-3

FIG. 9

B4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23825 A1

(51) International Patent Classification[7]: H04L 12/28, 12/66, H04J 3/16

(21) International Application Number: PCT/US01/28424

(22) International Filing Date:
12 September 2001 (12.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/660,709 13 September 2000 (13.09.2000) US

(71) Applicant: WP MEDIA INC [US/US]; 209 W. Will Street, Kingstree, SC 29556 (US).

(74) Agent: ALEXANDER, Tony, D.; Technology Legal Counsel LLC, P.O. Box 1728, Evans, GA 30809-1728 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU (petty patent), AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

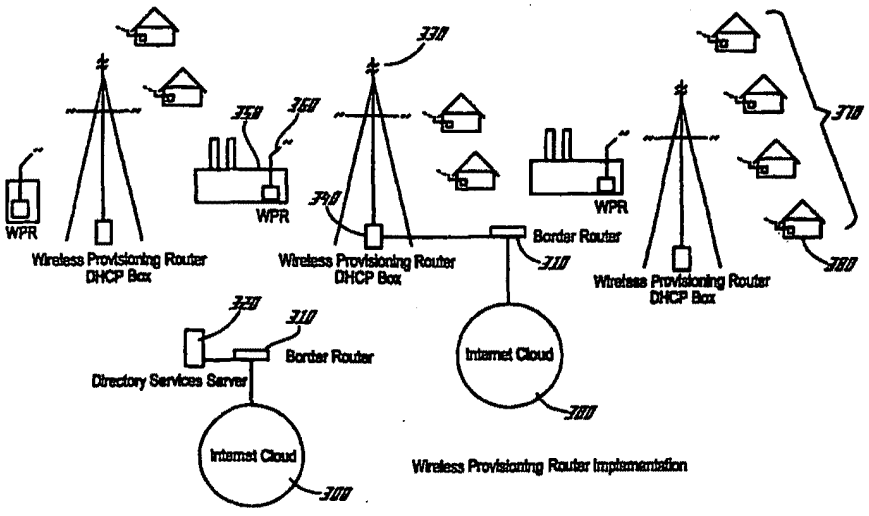
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,*

[Continued on next page]

(54) Title: WIRELESS PROVISIONING DEVICE



(57) Abstract: A wireless provisioning device (WPD) is a computer data traffic management system capable of routing TCP/IP traffic using 2.4 Ghz equipment. This WPD is to be strategically placed in logical segment regions within a wireless network to facilitate data traffic management. This device acts to provide connectivity between wireless backbone access points. The device may also be located within customer local area network (LAN) while providing connectivity to a wide area network (WAN). The wireless device has seven total wireless segments. The wireless device is capable of filtering IP addresses (330), controlling firewall (320) and/or router (340) and/or bridge. The wireless provisioning device increases effective throughput of TCP/IP traffic over the WAN or LAN while providing for secure management and greater connectivity.

WO 02/23825 A1

KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WIRELESS PROVISIONING DEVICE

FIELD OF THE INVENTION

The present invention relates to telecommunications gear, and more specifically, in the preferred form, to wireless provisioning devices capable of routing TCP/IP traffic using 2.4 Ghz equipment.

BACKGROUND OF THE INVENTION

Until recently, Internet connectivity was restricted to hard-wired connections to the Internet cloud. With the advent of stronger 2.4 Ghz antennae it became more practical to administer wireless connections to computers that would eventually connect back to the Internet cloud. As the speed of the wireless equipment increased, it became more cost effective to provide wireless connections to the user than cabling. As a result, attempts were made to replace wired Wide-area networks (WANs) with high-speed wireless connections.

Presently, wireless equipment only offers bridging solutions. These wireless bridges contain either one or two wireless cards, depending on manufacturer, and one wired connection. In some cases there are two wireless cards and one wired connection. However, in this rapidly expanding telecommunications landscape, it may prove necessary to have 3 or 4 wireless connections and 3 or 4 wired connections. Although a bridge is a good way to connect two or three Local-area networks (LANs) together, the overhead of

bridging will not function for an extensive WAN because current routing logic has a theoretical breakdown at 3 to 5 bridges. As a result, present day 2.4 Ghz wireless connection points provide bridging solutions that greatly restrict the ability of the user to place wireless equipment in a wide area network. 2.4 Ghz wireless equipment is designed to create hubbed LANs and to bridge together two or more small LANs. It was not designed to work in a public domain WAN environment.

Additionally, current wireless connections were designed for indoor use and security is only associated with the network name. Alternatively, the system may be held closed through the use of Media access control (MAC) addressing. Despite the wireless function, such LAN solutions assumed that the connections back to the wireless access point were relatively few in number and that the connections were somewhat stationary. As a result, the MAC filtering is housed resident on the access connection point. The connection point typically requires rebooting before the new access list may take effect. In addition, there are a finite number of MAC addresses that may be placed on the connection point. This effectively limits the number of roaming customers that may be added to the system. Each time a new member is added, every connection point in the network must be updated and rebooted.

In order to manage a wireless connection point, Simple Network Management Protocol (SNMP) became the standard method for data transfer. To modify the MAC filter, the administrative password for the access connection point is passed along the network. This password is passed in clear text. Without secure shell connections this clear text message becomes easy to intercept for anyone

connected to the WAN. Once the administrative password is breached the whole system becomes compromised. Earlier systems prevented this by providing only those within the organization the network name. Without the network name, wireless cards will not connect with the connection point. In a public domain environment the network name will be common to all those that use the service, which makes unauthorized access relatively simple.

There is a need for a piece of wireless equipment that can be used to effectively connect a large WAN. There is also an existing need for a wireless provisioning device that provides network routing at the source and security measures through the network. There is an additional need for 2.4 Ghz wireless connection points that provide bridging solutions that afford the user the ability to place wireless equipment in a wide area network. There is yet another existing need for wireless connections designed for outdoor use and flexible security. Additionally, there remains a need for a system that can accommodate multiple connections back to the wireless access point without requiring rebooting before the new roaming members can be added to the system.

SUMMARY OF THE INVENTION

The present invention provides a wireless provisioning device capable of routing TCP/IP traffic using 2.4 Ghz equipment. This device is to be strategically placed in logical segment regions within a wireless network to facilitate data traffic management. This device acts to provide connectivity between wireless backbone access points. The device may also be located within customer LANs

device has seven total wireless segments. The wireless device is capable of filtering IP addresses, controlling firewall and/or router and/or bridge needs and increases effective throughput of TCP/IP traffic over the WAN or LAN while providing for secure management and greater connectivity.

It is a primary objective of the present invention to provide a piece of wireless equipment that can be used to effectively connect a large WAN.

It is another objective of the present invention to provide a wireless provisioning device that provides network routing at the source and security measures through the network. The solution is to provide secure connections between wireless access points and to points that require administrative connections.

Yet another objective of the present invention is to provide 2.4 Ghz wireless connection points that provide bridging solutions that afford the user the ability to place wireless equipment in a WAN.

Still another objective of the present invention is to provide wireless connections designed for outdoor use and flexible security. The present invention achieves the above objective through each of several embodiments, particularly, by radius authentication. Radius authentication is a more universal, more flexible and more secure method of authentication. The authentication process is done with secure connections to a central server. If for some reason security is breached then the username and password can be changed on the server side through a database change as opposed to a hardware change. By incorporating a new operating system with the use of the present wireless cards, wireless devices can be configured for

logical management through secure connections. Furthermore, radius authentication can pass securely through the wireless device into the secure network.

An additional objective of the present invention is to provide a system that can accommodate multiple connections back to the wireless access point without requiring rebooting before the new roaming members can be added to the system.

In accomplishing these and other objectives, there has been provided, in accordance with one aspect of the present invention, a wireless provisioning device that can route at the node providing for lower network overhead and stabilizing the network into a durable redundant WAN.

Further objects, features and advantages of the invention will be apparent from the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of a wireless provisioning device in accordance with the present invention.

FIG. 2 is a schematic diagram of a two slot wireless device embodiment in accordance with the present invention.

FIG. 3 is a schematic diagram of a wireless provisioning system in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The Provisioning device system, in accordance with the present invention comprise a plurality of wireless access points; a wireless provisioning device for receiving, transmitting, and directing data over a plurality of networks and capable of sustaining connectivity between the wireless access points and the wireless provisioning device, the wireless provisioning device comprising a chassis, at lease one network card, at least one wireless card, at least one processor, and at least one operating system operable configured in the chassis and associated with at least one of the plurality of wireless access points for transmitting and receiving data between the wireless access point and a carrier structure and where the wireless provisioning device is capable of accommodating multiple connections back to the wireless access point without requiring rebooting before a new roaming member can be added to the system; a carrier structure communicably positioned between the wireless provisioning device and the plurality of wireless access points for transmitting and receiving data between the wireless provisioning device and the plurality of wireless access points by means of a secure connection; and a security authentication protocol capable of authenticating traffic as it passes through the carrier structure.

The following terms are used in this application:

Access Point: On a network, a device designed to allow computers that are not part of a network to connect to and communicate with the network. The primary function of an access point is to provide a point of access for those unconnected computers

Authentication: A system of measures for keeping information on a system safe from corruption or prying eyes. In networks, the procedure by which a computer verifies user identification. The most common form involves the comparison of a logon name and password to a stored file of approved user names and passwords. Any differences between the two will prohibit the user from accessing the information.

Bridge: Links networks so that data from one network can pass through another network on its way to still another network.

Datagram: A single unit of data, including its destination information, which is transmitted through a network.

Directory Service Member: A network management system, located on one enterprise capable computer. This computer maintains a database directory that stores all information from billing to authentication privileges for those on the network. Specifically this machine records MAC addresses and billing profiles for those in the system. This computer is a central repository that controls users access, system privileges and payment status.

Dynamic Host Configuration Protocol (DHCP): An Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stock configuration parameters, and provide other information such as the addresses for auxiliary servers.

Gateway: A complex internetworking device that converts information from one protocol to another. Gateways transfer information between networks that use

different communications protocols. The gateway actually tears down the information from one service and restructures it in the other network's protocol format. Gateways include all hardware and software used to link dissimilar network operating systems (NOS) or to link local-area networks (LANs) to mainframes or wide-area networks (WANs). Gateways also are used in electronic mail (E-mail) to convert messages between services using different E-mail protocols.

Graphical User Interface (GUI): A GUI uses graphical symbols, called icons, and menu to carry out commands.

Local-Area Network (LAN): A group of computers, usually in one building or office, physically connected in a manner that lets them communicate and interact with each other. For a network to operate, it needs a server, which is a computer that holds data used by the different computers on the network. Some of the benefits of a network connection include the ability to share document files and expensive equipment. Networks can be connected using different combinations of topologies, protocols, software and hardware. A network that uses radio transmissions instead of cables to connect computers may be called a local-area wireless network.

Media Access Control (MAC): The protocol that determines the transmission of information on a network.

Node: Any device that can communicate with other computers in a group of interconnected computers. Usually, a node refers specifically to a computer system (CS) or terminal that is part of a network.

Packet: A block of data transmitted from one computer to another on a network or on the Internet. A packet contains three parts: the data to be transmitted, the data needed to guide the packet to its destination, and the data that corrects errors that occur along the way. Several packets make up a typical transmission. The computer splits up the transmission at the transmission point and reassembles it at the destination point.

Protocol: A set of rules and procedures for exchanging data between computers on a network or through the Internet. Protocol usually includes information or error checking, data compression, and sending and receiving messages.

Router: The part of a communications network that receives transmissions and forwards them to their destinations using the shortest route available. Data may travel through multiple routers on the way to its destination.

Simple Network Management Protocol (SNMP): It exchanges network information through messages technically known as protocol date units (PDUs).

Telnet: Terminal emulation in which a user is connected to a remote host using an Internet account as if the user were directly connected to the host, such that a connectivity session continues as if the user was at a terminal connected to the host, though the user is actually connected to another site, using the Internet to connect to the host.

Topology: The physical configuration of a network that determines how the network's computers are connected.

Transmission Control Protocol/Internet Protocol (TCP/IP): A language governing communication among all computers on the Internet. TCP/IP is two

separate protocols, TCP and IP, that are used together. The Internet Protocol portion of the standard dictates how packets of information are sent out over networks. IP has a packet-addressing method that lets any computer on the Internet forward a packet to another computer that is a step or more closer to the packet's recipient. The Transmission Control Protocol ensures the reliability of data transmissions across Internet-connected networks. TCP checks packets for errors and submits requests for retransmission if errors are found; it also will return the multiple packets of a message into the proper, original sequence when the message reaches its destination.

Wide-Area Network (WAN): A collection of computers connected or networked to each other over a geographic area. WANs usually require special arrangements with telephone companies because data is transmitted among locations (called sites) across telephone lines.

A computer network is simply a collection of autonomous computers connected together to permit sharing of hardware and software resources, and to increase overall reliability. The qualifying term "local area" is usually applied to computer networks in which the computers are located in a single building or in nearby buildings, such as on a college campus or at a single corporate site. When the computers are further apart, the term "wide area network" is used, but the distinction is one of degree and the definitions sometime overlap.

A bridge is a device that is connected to at least two LANs and serves to pass message frames or packets between LANs, such that a source station on one LAN can transmit data to a destination station on another LAN, without concern for

the location of the destination. Bridges are useful network components, principally because the total number of stations on a single LAN is limited. Bridges can be implemented to operate at a selected layer of protocol of the network.

At the heart of any computer network is a communication protocol. A protocol is a set of conventions or rules that govern the transfer of data between computer devices. The simplest protocols define only a hardware configuration, while more complex protocols define timing, data formats, error detection and correction techniques and software structures.

Computer networks almost universally employ multiple layers of protocols. A low-level physical layer protocol assures the transmission and reception of a data stream between two devices. Data packets are constructed in a data link layer. Over the physical layer, a network and transport layer protocol governs transmission of data through the network, thereby ensuring reliable data delivery.

A model for network architectures has been proposed and widely accepted. It is known as the International Standards Organization (ISO) Open Systems Interconnection (OSI) reference model. The OSI reference model is not itself a network architecture. Rather it specifies a hierarchy of protocol layers and defines the function of each layer in the network. Each layer in one computer of the network carries on a conversation with the corresponding layer in another computer with which communication is taking place, in accordance with a protocol defining the rules of this communication. In reality, information is transferred down from layer to layer in one computer, then through the channel medium and back up the

successive layers of the other computer. However, for purposes of design of the various layers and understanding their functions, it is easier to consider each of the layers as communicating with its counterpart at the same level, in a "horizontal" direction.

The lowest layer defined by the OSI model is called the physical layer, and is concerned with transmitting raw data bits over the communication channel. Design of the physical layer involves issues of electrical, mechanical or optical engineering, depending on the medium used for the communication channel. The layer next to the physical layer is called the data link layer. The main task of the data link layer is to transform the physical layer, which interfaces directly with the channel medium, into a communication link that appears error-free to the next layer above, known as the network layer. The data link layer performs such functions as structuring data into packets and attaching control information to the packets.

Although the data link layer is primarily independent of the nature of the physical transmission medium, certain aspects of the data link layer function are more dependent on the transmission medium. For this reason, the data link layer in some network architectures is divided into two sublayers: a logical link control sublayer, which performs all medium-independent functions of the data link layer, and a MAC sublayer. This sublayer determines which station should get access to the communication channel when there are conflicting requests for access. The functions of the MAC layer are more likely to be dependent on the nature of the transmission medium.

The basic function of a bridge is to listen "promiscuously," i.e., to all message traffic on all LANs to which it is connected, and to forward each message it hears onto LANs other than the one from which the message was heard. Bridges also maintain a database of station locations, derived from the content of the messages being forwarded. Bridges are connected to LANs by paths known as "links." After a bridge has been in operation for some time, it can associate practically every station with a particular link connecting the bridge to a LAN, and can then forward messages in a more efficient manner, transmitting only over the appropriate link. The bridge can also recognize a message that does not need to be forwarded, because the source and destination stations are both reached through the same link. Except for its function of "learning" station locations, or at least station directions, the bridge operates basically as a message repeater.

As network topologies become more complex, with large numbers of LANs, and multiple bridges interconnecting them, operational difficulties can ensue if all possible LAN bridging connections are permitted. In particular, if several LANs are connected by bridges to form a closed loop, a message may be circulated back to the LAN from which it was originally transmitted, and multiple copies of the same message will be generated. In the worst case, messages will be duplicated to such a degree that the networks will be effectively clogged with these messages and unable to operate at all.

Internet is a collection of networks, including Arpanet, NSFnet, regional networks, local networks at a number of university and research institutions, and a number of military networks. The protocols generally referred to

as TCP/IP were originally developed for use only through Arpanet and have subsequently become widely used in the industry. The protocols provide a set of services that permit users to communicate with each other across the entire Internet. The specific services that these protocols include file transfer, remote log-in, remote execution, remote printing, computer mail, and access to network file systems.

The basic function of the Transmission Control Protocol (TCP) is to make sure that commands and messages from an application protocol, such as computer mail, are sent to their desired destinations. TCP keeps track of what is sent, and retransmits anything that does not get to its destination correctly. If any message is too long to be sent as one "datagram," TCP will split it into multiple datagrams and makes sure that they all arrive correctly and are reassembled for the application program at the receiving end. Since these functions are needed for many applications, they are collected into a separate protocol (TCP) rather than being part of each application. TCP is implemented in the transport layer of the OSI reference model.

The Internet Protocol (IP) is implemented in the network layer of the OSI reference model, and provides a basic service to TCP: delivering datagrams to their destinations. TCP simply hands IP a datagram with an intended destination; IP is unaware of any relationship between successive datagrams, and merely handles routing of each datagram to its destination. If the destination is a station connected to a different LAN, the IP makes use of routers to forward the message. TCP/IP frequently uses a slight deviation from the seven-layer OSI model in that it may have fewer layers. The seven layers are as follows:

Layer 7—The Application Layer. Identifies communications partners, user security, and authentication, as well as specific details about syntax of a transmission. Examples of Layer 7 protocols are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and telnet.

Layer 6—The Presentation Layer. Governs the translation of a transmission from data to text, depending on the software application in use. Control is generally vested in the operating system that deals with specific aspects of data through protocols such as Moving Pictures Experts Group (MPEG) and Joint Photographic Experts Group).

Layer 5—The Session Layer. Establishes communications between parties to both ends of a session, then terminates them when transmission is complete, via protocols such as AppleTalk and Session Control Protocol (SCP).

Layer 4—The Transport Layer. In this layer, Transmission Control Protocol (TCP) and Name Binding Protocol (NBP) add transport data to the packet and pass it to layer 3.

Layer 3—The Network/Internet Layer. When an action is initiated on a local host (or initiating host) that is to be performed or responded to on a remote host (or receiving host), this layer takes the package from layer 4 and adds IP information before passing it to layer 2. By way of protocols such as Border Gateway Protocol (BGP) or Routing Information Protocol (RIP), identifies a transmission's intended recipient based on specific network protocols and controls the route each packet of data, in the complete transmission, takes on its journey.

Layer 2--The Data Link/Network Interface Layer. This is the network device as the host, or local computer, sees it and it is through this medium that the data is passed to layer 1. Adds, via protocols such as Logical Link Control (LLC) or Media Access Control (MAC), the specific code necessary to take packets of data on their way using information from layer 3. For example, if a network standard requires that each data packet begin with a string of specific binary digits, they are added at layer 2.

Layer 1--The Physical Layer. This is literally the Ethernet or Serial Line Interface Protocol (SLIP) itself. Defines the physical interface necessary to get communication information from point A to point B, and it includes various LAN and WAN specifications.

At the receiving host the layers are stripped one at a time, and their information is passed to the next highest level until it again reaches the application level. If a gateway exists between the initiating and receiving hosts, the gateway takes the packet from the physical layer, passes it through a data link to the IP physical layer to continue. As a message is sent from the first host to the second, gateways pass the packet along by stripping off lower layers, readdressing the lower layer, and then passing the packet toward its final destination.

A router, like a bridge, is a device connected to two or more networks. Unlike a bridge, however, a router operates at the network layer level, instead of the data link layer level. Addressing at the network layer level makes use of a 32-bit address field for each host, and the address field includes a unique network identifier and a host identifier within the network. Routers make use of the

destination network identifier in a message to determine an optimum path from the source network to the destination network. Various routing algorithms may be used by routers to determine the optimum paths. Typically, routers exchange information about the identities of the networks to which they are connected.

When a message reaches its destination network, a data link layer address is needed to complete forwarding to the destination host. Data link layer addresses are 48 bits long and no two hosts, wherever located, have the same data link layer address. There is a protocol called ARP (address resolution protocol), which obtains a data link layer address from the corresponding network layer address (the address that IP uses). Typically, each router maintains a database table from which it can look up the data link layer address, but if a destination host is not in this ARP database, the router can transmit an ARP request. Only the addressed destination host responds, and the router is then able to insert the correct data link layer address into the message being forwarded, and to transmit the message to its final destination.

IP routing specifies that IP datagrams travel through internetworks one step at a time based on the destination address in the IP header. The entire route is not known at the outset of the journey. Instead, at each stop, the next destination is calculated by matching the destination address within the datagram's IP header with an entry in the current node's routing table.

Each node's involvement in the routing process consists only of forwarding packets based on internal information resident in the router, regardless of whether the packets get to their final destination. To extend this explanation a

MISSING AT THE TIME OF PUBLUCATION

task is left to another Internet protocol, the Internet Control Message Protocol (ICMP).

A router will perform protocol translation. One example is at layers 1 and 2. If the datagram arrives via an Ethernet interface and is destined to exit on a serial line, for example, the router will strip off the Ethernet header and trailer, and substitute the appropriate header and trailer for the specific network media, such as SMDS, by way of example.

A route policy may be used instead of routing table entries to derive the next step address. In the system and methodology of the present invention, the source address is tested to see in which ISP address range it falls. Once the ISP address range is determined the packet is then routed to the next step address associated with the specific ISP.

It must be noted, however, that routing wireless networks at connection nodes is the most efficient means of passing Internet data. One aspect of the present wireless provisioning device is to provide routing at each node connection point. This provides for a stronger network and provides flexibility in network design. This flexibility allows for better network traffic management and improves the overall bandwidth by reducing network latency through optimization of routes and data packet management. Although the wireless provisioning device is capable of bridging, it will be the determination of the network engineer to establish the wireless provisioning device as a bridge to the network or a router to the network. This feature gives the network engineer more flexibility to determine the network design. Furthermore, the flexible nature of the equipment allows the user

to change a leaf node that bridges into a major backbone node that routes through the use of code modification without the need to reboot.

Subsequently, as a node begins to grow, the network engineer can upgrade that node to fit the needs of the network without harming existing customers. By inserting the cards in the slots of a chassis that contains open-source code, preferably LINUX, as its operating system (OS), the wireless provisioning device can be configured as a router or a bridge. The routing module of LINUX is not a portion of the main operating kernel. Being a subcomponent of the OS, the routing module can be upgraded and modified without rebooting the system. A reboot of an advanced LINUX box may take up to 30 minutes to complete. The upgrade of a routing module in LINUX takes less than 2 seconds to reinitialize. This reinitialization is transparent to the customers attached to this box. The routing module is replaceable by a bridge module if routing is not necessary for the connection node. Routing at the connection point allows for the filtering of IP addresses for either all of the customers attached to that node or for an individual IP address attached to that node. Furthermore, the routing module contains routing logic capable of bandwidth shaping. This process only allows certain volumes of data to be transmitted to and/or from a certain customer IP address.

The present invention furthers the art with the addition of more access points. By providing a flexible configuration of preferably eight ports, the wireless provisioning device may contain up to seven wireless connections and one wired connection, or seven wired connections and one wireless connection, or any combination as seen fit for the network. This reduces overall cost and decreases

space requirements. By placing this system on a faster chip set, the equipment effectively processes more data from the same point. Furthermore, this feature allows the expansion of the system to develop from an outlying leaf node with little usage to a major backbone node with multiple redundancy without affecting existing customers. The user can also increase the number of potential customers to the connection point in the network by adding cards and antennas without the need for chassis changes. Because the physical configuration of the system resides in the chassis of a personal computer with preferably eight possible network slots, the wireless provisioning device can be configured with differing numbers of wireless cards and network cards. The chassis may contain up to two processors. Running the LINUX operating system the single or dual processor configuration allows for hefty data management. This processor configuration and extensive amounts of random access memory allows the operating system to handle extensively more information than the traditional wireless connection points.

The provisioning device, in accordance with the present invention, also addresses the security of wireless equipment. Using a secure shell telnet connection to the wireless provisioning device, message traffic and administrative information cannot be sniffed by other users on the network. Due to this feature, public domain wireless equipment can be made available. This feature uses a more universal management scheme of telnet. Thus the administrator may write interface Graphical User Interfaces (GUIs) or can control the node through the use of a plain text command line screen. Connection to these nodes can be limited to authorized IP addresses and domain names, reducing the chances of unauthorized network

entries. Presently, wireless equipment use Simple Network Management Protocol Version 1 (SNMPV-1) protocol for the management of the connection device. SNMPV-1 is limited to text message traffic. Any connection made to this connection point is on the same logical segment as those that are doing administrative work to the connection device. In every network solution logical segments contain all the information that is passed within that segment. Sniffing traffic on that logical segment has long been known to be a problem within networking circles. SNMPV-6 protocol is the typical solution to this problem while using SNMP protocol. However SNMPV-6 is a processor intense protocol providing for extensive network overhead. By using a secure telnet connection the network overhead is reduced while increasing the security of the system. A secure telnet connection only allows certain IPs to connect to certain dataports. This limited connection structure effectively creates different logical segments within the same physical network segment. The newly created logical segment prevents the sniffing of administrative traffic by the common user.

In a preferred embodiment of the present wireless provisioning device, limited static MAC addressing is replaced by or coupled with radius authentication. The radius authentication can be tied to the MAC addressing in conjunction with a user name and password. This method of authentication greatly reduces the chances of service theft and allows the user a mobile solution between cells. Furthermore this feature lends itself to a directory service method that will allow a more customized interface for the user. Using IP filtering, authorization levels and enterprise user management the wireless provision router with directory

service will control bandwidth consumption, and provide a more custom service to the user. Without radius authentication, users are connected to the network without any control from a central server. By providing radius authentication one server controls the ability of the user to enter certain parts of the network.

The present invention, in multiple embodiments, provides firewall and proxy service. The wireless provisioning device can provide both of these services at the user's termination point. These services will provide an added layer of protection to the user without the need for security management. Furthermore the proxy nature will provide for IP translation and allow users to maintain networks behind the entry point to the net.

Wireless provisioning devices, in accordance with the present invention, provide connections from both single personal computer cards and from other wireless provisioning devices. Therefore the same wireless WAN may contain single users and large LANs. In conventional wireless equipment configurations, the user must choose to provide service to either the personal computer containing the cards or to a wireless connection bridge. Commercial users would then select to use a wireless connection bridge while a residential user would choose to use a personal computer. Without the wireless provisioning device, two separate wireless infrastructures would have to be erected to satisfy all types of customers. The wireless provisioning device allows the user to connect to the wireless infrastructure using either an individual personal computer or another wireless provisioning device. As a result, one wireless infrastructure may be erected while satisfying all potential customer types.

It will be readily understood that the components of the present invention, as generally described and illustrated in the Figures herein, could be arranged and designed in a wide variety of different configurations. Thus, the following more detailed description of the embodiments of the system and method of the present invention, as represented in FIGS. 1 through 3, is not intended to limit the scope of the invention, as claimed, but it is merely representative of the presently preferred embodiments of the invention.

The presently preferred embodiments of the invention will be best understood by reference to the drawings of FIGS. 1-3, wherein like parts are designated by like numerals throughout.

In general terms, FIGS. 1-3 show a self-standing wireless system. Referring now to Fig. 3, connected to the wireless cloud 300 one readily notes a border router 310 at each connection point. In a preferred embodiment of the present invention, the border router 310 is a typical wired router. Connected to one layer of the cloud 300 is a directory services member 320. This device may be configured to control the objects to which all client side computers conduct authentication. The cloud 300 connected to the tower 330 passes through a wireless router 340. This router 340 serves as both a router and a Dynamic Host Configuration Protocol (DHCP) server. All further connections on the tower also use wireless routers to connect to the central wireless router.

Each time a wireless router 340 is located on a tower 330 that router acts as its own DHCP server. A predetermined set of IP addresses are assigned to that tower 330. All DHCP authentication returns to the Directory services member

320 to validate login. At large usage locations such as factories 350 a wireless router 340 is placed at the output connection point 360. This wireless router 340 serves as an internal router for all equipment within the facility and as a border router for the location. A wireless router 340 is only needed by those clients that have a large number of computers connected to the wireless network. Home users and small businesses 370 that have one or two PCs 380 that can connect directly back to the wireless router 340 on the tower 330. Furthermore, small computer users may bridge back to the tower 330 and then not get routed until they reach the border router 310 at the outlet to the Internet cloud 300.

Referring specifically to FIG. 1, an exemplary embodiment of a wireless provisioning device in accordance with the present invention may comprise a chassis 100 suitably configured with a UNIX based operating system 110 such as a LINUX operating system running on an Intel based CPU 120. The 2.4Ghz wireless cards 130 are constructed with typical PCM/CIA connectors 140. That connector is adapted to the PC bus structure 150 through a PCM/CIA to PCI adapter. The bus interface to the PC is all PCI. Information enters and exits the wireless cards through the PCI bus into the TCP stack (not shown) of the LINUX OS 110. The TCP stack on the LINUX OS is configured in a manner to either redirect or transmit the data through the appropriate interface. In many cases data will enter into the wireless provision device through the 10/100 Network Interface Card (NIC) 160 through standard wired IP methods 170. Once the information enters through the wired connection 170 the TCP stack configuration in the LINUX stack module will

direct the traffic out the appropriate connection. The LINUX TCP stack configuration optimizes the network data traffic flow.

Referring now, principally, to FIG. 2, a typical configuration for a 2.4Ghz bridge 200 is either 1 or 2 wireless cards 210 with PCM/CIA connectors 220. These cards 210 connect to the bridge bus through the PCM/CIA connections 230. The output from the wireless bridge 200 is either the 10/100 ethernet or the other wireless card 210. The wireless cards 210 have an adapter 240 for increased antenna gain. These connectors go to a lightning arrestor device 250 to prevent damage from lightning strikes. These lightning arrestors 250 connect to special low loss antenna cables 260. The low loss antenna cables 260 then connect to increased gain antennae of varying global patterns and strength. In some events these antennae require splitters 270 and amplifiers 280 to optimize globe patterns for the area.

An apparatus and system according to the invention works well in a wide variety of cases and does not inhibit or impact future enhancements to network protocols and operating systems. To assure that operations at the application and transport levels do become aware of changes of address promptly, the apparatus and system may eliminate the prospect of a single point of failure, eliminate or reduce sub-optimal routing for all applications, provide improved security to protect communication over wireless media, and allow users to switch network adapter cards while preserving all connections, such as software applications and network administration, transparently to the user.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative, and not restrictive. The scope of the invention is, therefore, indicated by the appended claims, rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

CLAIMS

What is claimed is:

1. A wireless provisioning device, comprising:

a chassis;

at least one network card;

at least one wireless card;

at least one processor;

an operating system, the operating system operably configured in the chassis to control the at least one network card, the at least one wireless card and the at least one processor;

a packet-switched interface capable of receiving a multiplicity of inbound framed packet-data to provide inbound packets and transmitting a multiplicity of outbound framed packet-data comprising outbound packets;

a channeling controller, coupled to the packet-switched interface that channels the inbound packets based on the inbound address information and that constructs the outbound packets and channels the outbound packets with the outbound address information, the channeling controller capable of being effectively connected to at least one network via the operating system.

2. The wireless provisioning device of claim 1, wherein the channeling controller routes the inbound packets.

3. The wireless provisioning device of claim 2, wherein the channeling controller routes the outbound packets.

4. The wireless provisioning device of claim 1, wherein the channeling controller bridges the inbound packets.

5. The wireless provisioning device of claim 4, wherein the channeling controller bridges the outbound packets.

6. The wireless provisioning device of claim 1, wherein the operating system of the wireless provisioning device is an open source UNIX based system.

7. The wireless provisioning device of claim 1, wherein the open source UNIX based system is LINUX.

8. The wireless provisioning device of claim 1, the wireless provisioning device further comprises a second processor.

9. The wireless provisioning device of claim 1, wherein the wireless provisioning device further comprises a memory device and a storage device.

10. A system, comprising:

a plurality of wireless access points;

at least one wireless provisioning device for receiving, transmitting, and directing data over a plurality of networks and capable of sustaining connectivity between the wireless access points and the wireless provisioning device, the wireless provisioning device comprising a chassis, at lease one network card, at least one wireless card, at least one processor, and at least one operating system operably configured in the chassis and associated with at least one of the plurality of wireless access points for transmitting and receiving data between the wireless access point and a carrier structure and where the wireless provisioning device is capable of accommodating multiple connections back to the wireless access point without requiring rebooting before a new roaming member can be added to the system;

a carrier structure communicably positioned between the wireless provisioning device and the plurality of wireless access points for transmitting and receiving data between the wireless provisioning device and the plurality of wireless access points by means of a secure connection; and

a security authentication protocol capable of authenticating traffic as it passes through the carrier structure.

11. The system of claim 10 wherein the wireless provisioning device further comprises a directory services member operatively connected to the operating system thereof, which is suitable for maintaining a database directory that stores MAC addresses and billing profiles for those in the system.

12. The system of claim 11, wherein the wireless provisioning device is capable of bridging.

13. The system of claim 12, wherein the wireless provisioning device is capable of routing.

14. The system of claim 13, wherein the wireless provisioning device is further capable of bridging.

15. The system of claim 11, wherein the carrier structure is a suitable antenna for providing bridging solutions that afford the user the ability to place wireless equipment in a wide area network.

16. The system of claim 10, wherein the security authentication protocol is a radius authentication protocol.

17. The system of claim 10, wherein the wireless provisioning device provides proxy service.

18. The system of claim 10, wherein the wireless provisioning device provides firewall service.

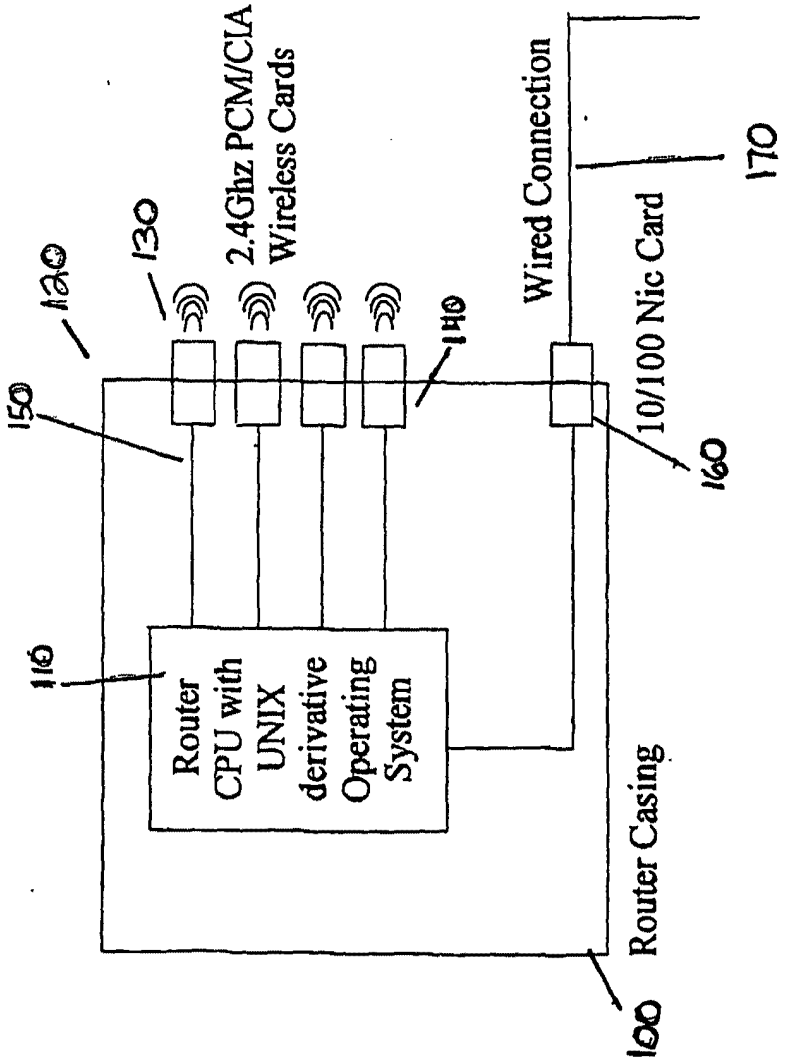
19. The system of claim 10, wherein the carrier structure secure connection is a secure shell telnet connection.

20. The system of claim 10, wherein the system further comprises at least one antenna.

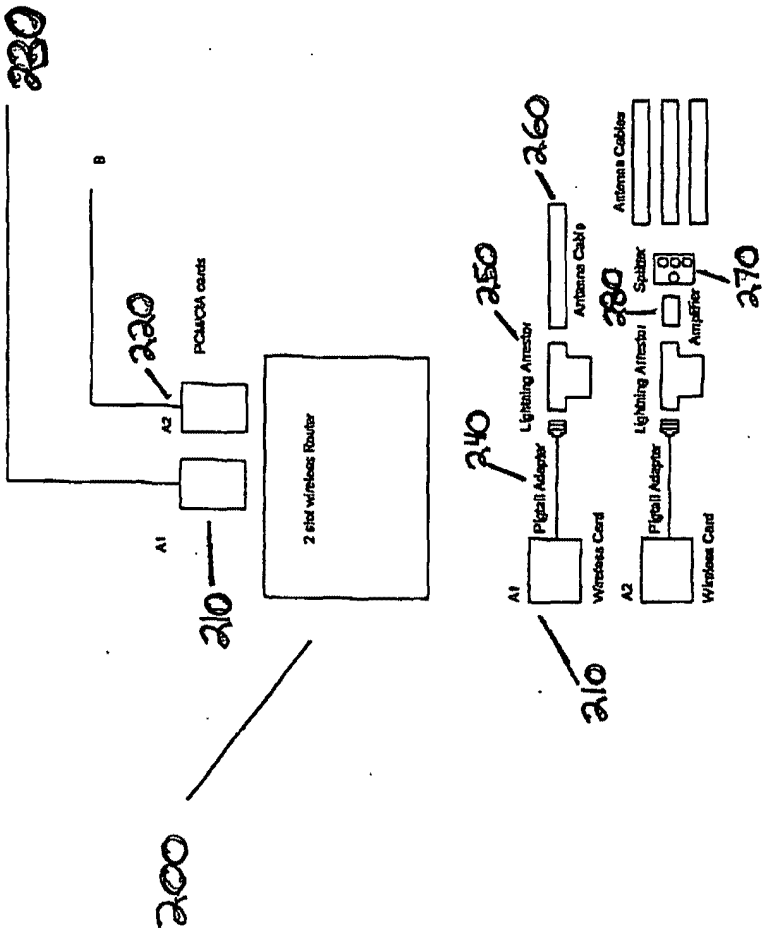
21. The system of claim 10, wherein the at least one antenna is a 2.4 Ghz antenna.

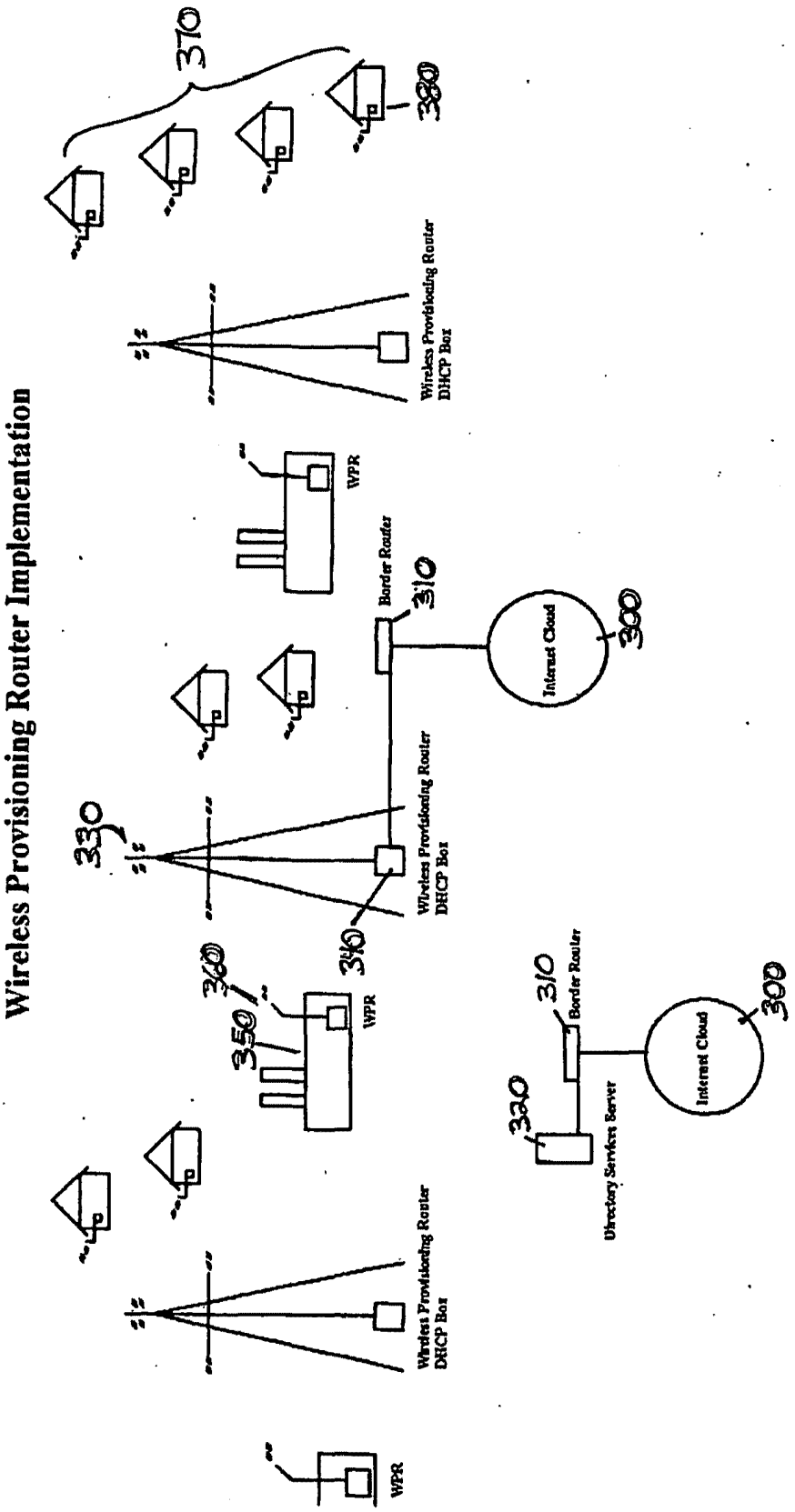
22. The system of claim 10, wherein the operating system of the wireless provisioning device is an open source UNIX based system.

23. The system of claim 10, wherein the open source UNIX based system is LINUX.



FORTINET EX1002 Page 189


220
B
320
PCMCIA cards
A2
A1
2 std wireless Router
310
300
240
Pigtail Adapter
Wireless Card
A1
250
Lightning Arrestor
260
Antenna Cable
Antenna Cables
280
Splitter
270
Amplifier
Lightning Arrestor
Pigtail Adapter
Wireless Card
A2
210


Wireless Provisioning Router Implementation
370
380
Wireless Provisioning Router DHCP Box
WPR
Border Router
310
Internet Cloud
300
330
Wireless Provisioning Router DHCP Box
340
360
350
WPR
Wireless Provisioning Router DHCP Box
WPR
310
Border Router
330
Directory Services Server
Internet Cloud
300

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/28424

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 12/28, 12/66; H04J 3/16
US CL :370/351, 352, 392, 396, 401, 404, 465
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/351, 352, 392, 396, 401, 404, 465

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST DATABASE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,745,884 A (CARNEGIE et al) 28 April 1998, see the entire document.	1-6, 8-16, 18-22
Y	US 5,960,074 A (CLARK) 28 September 1999, see the entire document.	1-23
A	US 5,572,528 A (SHUEN) 05 November 1996, see the entire document.	1-23

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
16 OCTOBER 2001

Date of mailing of the international search report
14 FEB 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
NGUYEN TOAN
Telephone No. (703) 305-0140

Form PCT/ISA/210 (second sheet) (July 1998)*

B5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 May 2002 (23.05.2002)

PCT

(10) International Publication Number
WO 02/41587 A2

(51) International Patent Classification[7]: H04L 12/28, 12/56, H04Q 7/38

(21) International Application Number: PCT/US01/51306

(22) International Filing Date: 22 October 2001 (22.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/241,975 23 October 2000 (23.10.2000) US
09/911,092 23 July 2001 (23.07.2001) US

(71) Applicant: BLUESOCKET, INC. [US/US]; 7 New England Executive Park, Burlington, MA 01803 (US).

(72) Inventor: CROSBIE, B., David; 47 Bay State Avenue, Somerville, MA 02144 (US).

(74) Agents: WAKIMURA, Mary, Lou et al.; Hamilton, Brook, Smith & Reynolds, P.C., 530 Virginia Road, P.O. Box 9133,, Concord, MA 01742-9133 (US).

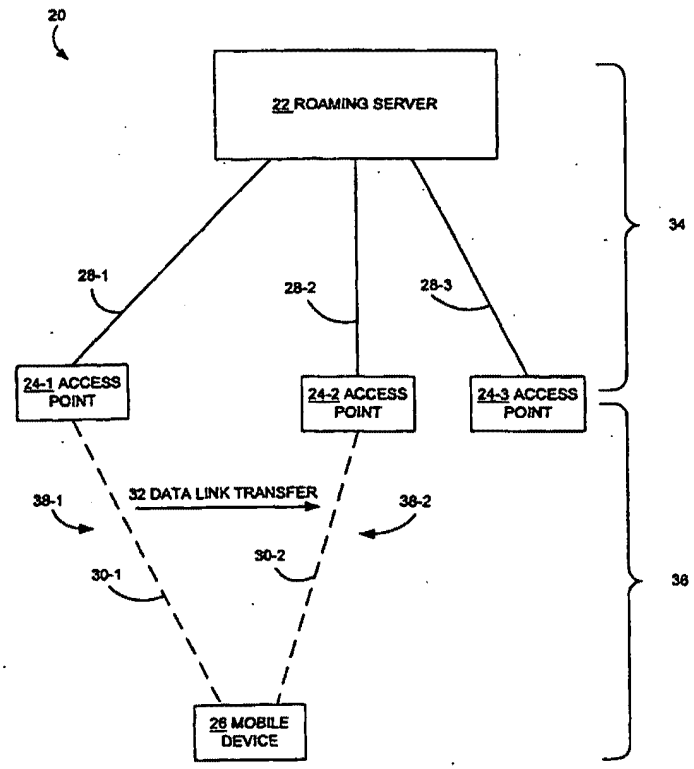
(81) Designated States *(national)*: AU, CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR ENABLING CENTRALIZED CONTROL OF WIRELESS LOCAL AREA NETWORKS



(57) Abstract: A wireless local area network (WLAN) includes mobile devices that are allowed to transfer wireless connections between WLAN subnets or channels having different access points. The access points connect to a central controller or roaming server that supports seamless hand-offs of mobile devices from one access point to another access point. The roaming server supports the reassignments of session data parameters from one access point to another (e.g., access point address spoofing) so that the mobile device can use the same parameters for comminicating to a new access point. The roaming server also supports the seamless handoff of a mobile device from one access point to another by using a master-slave switch technique across two piconets. The roaming server also facilitates the control of access points by establishing a host controller interface and wireless protocol stack in the roaming server then encapsulates host controller commands in a packet based network protocol used for communication between the roaming server and the access points.

WO 02/41587 A2

METHOD AND SYSTEM FOR ENABLING CENTRALIZED CONTROL OF WIRELESS LOCAL AREA NETWORKS

BACKGROUND OF THE INVENTION

Networked desktop computing is typical in both the office and home. Networking of mobile devices, such as mobile telephones, laptop computers, headsets, and PDA's (Personal Digital Assistants), is more difficult. New wireless standards, such as IEEE 802.11 and Bluetooth (BT) are designed to enable these devices to communicate with each other and a wired LAN (Local Area Network).

Bluetooth is a low cost wireless connection technology. Bluetooth is essentially a point-to-point (PPP) wireless communication technology that was developed as a replacement for using cable (i.e., hard wired) connections between devices. The Bluetooth technology is described in the Bluetooth specification, available from Bluetooth SIG, Inc. (see also the www.bluetooth.com web site), the entire teachings of which are herein incorporated by reference. This technology provides for a common attachment approach for different devices, and so enables mobile phones, laptops,

headsets, and PDA's to be easily networked in the office and eventually in public locations. Other standards, such as the IEEE 802.11 (Institute of Electrical & Electronics Engineers) and ETSI (European Telecommunications Standards Institute) HIPERLAN/2, provide a generally similar wireless connection function as Bluetooth and may be used to support WLAN (wireless LAN) communications. See the IEEE 802.11 "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," the entire teachings of which are herein incorporated by reference. See also the ETSI specifications for HIPERLAN/2, such as ETSI document number TR 101 683, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview," the entire teachings of which are herein incorporated by reference.

The Bluetooth technology provides for a piconet (or subnet), which is a group of up to eight devices, consisting of one master and a maximum of seven slaves that share a common hop sequence (based on a spread-spectrum frequency hopping technique, as is known in the art). Within the virtual channel created by a common hop sequence, the bandwidth is divided into seven time slots. One or more time slots are used for each master-slave communication. Amalgamating time slots increases capacity on that master-slave link.

As a user moves a mobile device connected to a WLAN from one location to another, the mobile device must establish a new connection with a new AP (access point, such as a local area network access point) when moving out of range of the previous AP. Typically, this transfer from the previous AP to the new AP requires the breaking down of the connection with the previous AP and the establishment of a new connection with the new AP.

SUMMARY OF THE INVENTION

One problem with both the IEEE 802.11 and Bluetooth standards has been a very limited or nonexistent ability for the mobile device to change its point of connection to the LAN (e.g., through an access point) in a seamless manner. This feature, known as "hand-offs" is required for many functions such as load balancing, improving radio link performance, and moving the mobile device inside a building without losing the network connection.

The Bluetooth standard version 1.1 does not support seamless hand-offs. The IEEE 802.11 standard does have the ability for the mobile device to change its point of LAN connection from one AP to another on the same IP sub-net (e.g., both AP's are directly connected via hubs or switches, not via a router), but the hand-off takes a number of seconds during which time there is no data flow. In addition the IEEE 802.11 standard has no method for the network to force the mobile device to transfer its LAN connection from one AP to another. This connection transfer is required for load balancing and improving the radio link quality of service.

A conventional approach, such as Bluetooth, may be modified to support hand-offs, but these hand-offs are typically controlled by the mobile device only, require changes to the software on the mobile device which stops backwards compatibility, and the hand-off itself is slow, which is a problem for some applications, such as voice communication.

The transfer of the mobile device from one AP to another occurs typically with a delay or interruption in the communications over the WLAN to the mobile device. Seamless hand-offs of the mobile device from one AP to another are required both for continuous coverage and for QoS (Quality of Service). In the latter case mobile devices are moved between co-located AP's so that users can be assigned, for example, their own dedicated channel (i.e., given a greater bandwidth).

The base version of Bluetooth has a 10 meter range and so if the Bluetooth technology is extended to enable Bluetooth to become a WLAN replacement, then an efficient, transparent and seamless approach to moving mobile devices from one piconet to another must be available. This approach must be transparent to layer 3 (i.e., network and route management layer) of the network interconnection layers (e.g., as specified in the Open System Interconnection Reference Model).

In the conventional Bluetooth approach, each member of the group (e.g., piconet or subnet) hops between seventy-nine different frequencies according to a sequence determined by the Bluetooth identifier (i.e., Bluetooth device address) of the master. All devices (e.g., mobile devices) have their own free running clock, but each uses a time offset to synchronize its hops with the master of a respective group. The master does not alter its clock. A device (e.g., mobile device) wanting to join a group

is initially in master mode. Such a device must detect the timing offset needed to join the group and then make the relevant offset at the same time as it switches into slave mode. This process is referred to a "joining a piconet" and is described in more detail in the Bluetooth specification.

Once the devices are synchronized then it is possible to set up a PPP session from a slave (e.g., mobile device) to the master (e.g., AP), and hence link the slave through the master to an Ethernet LAN connected to the master. The AP normally terminates the PPP session, and so the data is then sent and received as level 2 IP packets to any suitable device, connected locally or remotely across the Internet. If one of the slaves moves beyond the range of the master, then the connection breaks and the mobile device must then, if possible, establish a new radio link, and PPP link with the most appropriate AP. Establishing a PPP session is a long process; for example, tens of seconds of connectivity are lost.

One solution is to move the termination of the PPP session at a central controller (e.g., roaming server or gateway server) rather than at the AP. This means that when the radio connection from a mobile device to the AP is broken and re-established with another AP, then, as long as the switch-over between the two AP's is rapid, the PPP session between the mobile device and the central controller can be kept alive, hence avoiding the lengthy set-up process inherent in a PPP session. To implement this solution it is necessary for the mobile device to AP link to be seamlessly transferred from one AP to another. To achieve this all the AP'S are connected to a central controller (e.g., roaming server or gateway server) via an Ethernet LAN. Each master listens via a dedicated Bluetooth logical channel for all devices within range. When a master hears a new device, it relays this information back to the controller. In another case, one of the masters is maintaining a connection to a particular slave and signals to the controller that there is weakening reception for that slave as indicated by increased packet loss on the PPP link to that particular slave (this data is easily available from the PPP controller), and/or by another indication of weakening reception, such as RSSI (Received Signal Strength Indication). The controller can then look up another (or second) master with stronger reception of the mobile transmission and force a hand-off of the slave (i.e., transfer of the connection

for the mobile device from the previous AP to the new AP). This type of hand-off approach typically requires special client software (e.g., in the mobile device).

It is possible to solve this problem of seamlessly moving mobile devices at layer 3 (i.e., by using PPP). This PPP approach requires all the AP's to extend the PPP connection back to a master controller (e.g., roaming server) that terminates the PPP connections and switches them from one AP to another as the user moves. The problem with this PPP approach is scalability and speed of 'hand-off' which can be several seconds.

The techniques of the present invention provide two approaches that work at a lower network layer than layer 3, namely, layer 2 or the data link layer. One approach of the invention involves spoofing the identity of the AP. This approach involves assigning a separate Bluetooth identifier number to the master for each of the seven available time slots. The other approach of the invention involves an extension to the master-slave switch feature provided by the Bluetooth specification to separate a slave from one piconet cleanly and then attach it to another operating piconet. This master-slave switching is relatively simple if there is only one slave per piconet but the invention provides a solution that works with multiple slaves in a piconet, such as seven active slaves per piconet, and also when there are other parked slaves.

Further, the present invention achieves this seamless hand-off without requiring client software, which is typically required in prior art approaches. In the present invention, the second master inherits the characteristics of the first master. These characteristics include session data, such as the Bluetooth identifier (or other WLAN identifier) of the access point and encryption keys, as well as the PPP magic number. The session data may also include an identifier for the mobile device. Also, either the clocks of both masters are synchronized, or the slave is instructed to change its frequency offset to match the new master.

If there is more than one slave per master, however, this transfer of identity will either result in two identical masters or the first master changing its identifier and hence breaking its link to the other associated slaves.

Thus, the present invention provides solutions to the problems indicated above without requiring special software (or hardware) in the mobile device (that is, changes

from a conventional approach are only required in the AP's and the roaming server), as provided for in the embodiments described below. The techniques of the invention provide for use of spoofing AP's by transferring unique session data (access point device address, hop sequence, frequency offset, and encryption key) from one master AP to another so that the mobile device is unaware of the change in master. Higher level variables and link sessions such as IPSEC and PPP are held at the switch (e.g., controller, roaming server, or gateway server). The present invention also provides for the assignment of a series of unique Bluetooth Device (BD) addresses to the AP, one for each mobile device; so that each mobile device believes it is talking to a different master AP when in fact the AP is changing its BD address for each master-slave link. BD addresses are selected that do not synchronize the associated hop patterns but minimize the chance of a collision.

Thus, in one aspect, the present invention provides a method and system for performing a seamless handoff of a mobile device from an initial access point (e.g., initial AP) to a target access point (e.g., target AP). In particular, the method of the system (e.g., gateway application in a roaming server) includes (a) assigning session data to the initial access point to establish an initial connection from the mobile device through the initial access point to the roaming server, (b) detecting a triggering event that initiates a transfer of the mobile device from the initial access point to the target access point, and (c) transferring assignment of the session data from the initial access point to the target access point to establish a target connection from the mobile device through the target access point to the roaming server. This transfer of assignment is based on the session data and is in response to detecting that the triggering event has occurred, thus enabling the mobile device to use the session data to communicate with the target access point, such that the mobile device transfers seamlessly (without loss of connection and/or interruption of the current session with the user) from the initial access point to the target access point.

In another aspect, the present invention provides for the use of the master-slave switch to separate a slave from a piconet cleanly by forcing it to change into a master and then to associate it with another AP before switching it back to a slave in a piconet associated with the second AP. The present invention provides a method and system

(e.g., roaming server) in a wireless local area network for performing a seamless handoff of a mobile device from an initial piconet having an initial access point (e.g., initial AP) to a target piconet having a target access point (e.g., target AP). In particular, the method includes assigning the mobile device associated with the initial access point a master role for the initial piconet, assigning the target access point a slave role in the initial piconet while the target access point retains a master role in the target piconet, and establishing an association of the mobile device with the target piconet by switching roles of the mobile device and target access point. The mobile device establishes the association with the target piconet as a slave of the target piconet. The target access point terminates the slave role of the target access point with the initial piconet, while the target access point maintains the master role in the target piconet, such that the mobile device transfers seamlessly from the initial piconet to the target piconet.

In a further aspect, the present invention provides for splitting of the wireless protocol stack so that only the part required to deal with the radio frequency interface is located in the AP and the remainder of the stack is located in the central roaming server. The two parts communicate through a communications layer such as UDP packets sent over a LAN (e.g., Ethernet) that encapsulated host controller commands sent between the AP and the roaming server. This split is appropriate for all wireless protocols. The present invention provides a method and system (e.g., roaming server) for enabling seamless roaming of mobile devices among access points in a wireless local area network. In particular, the method includes (a) establishing a host controller interface in the roaming server, (b) encapsulating host controller commands in a packet-based network protocol for use in communication with access points in the wireless area network, the host controller commands directed to a connection session of the mobile device with the wireless local area network, and (c) exchanging the encapsulated host controller commands with access points in the wireless area network to enable a mobile device to receive the host controller commands and maintain the connection session while roaming among the access points.

In another aspect, the present invention provides an encapsulated packet for encapsulating and communicating commands based on a host controller interface using

a packet-based network protocol. The encapsulated packet includes a host controller command based on the host controller interface, device address of a host exchanging the encapsulated packet, a sequence number for use in a series of encapsulated packets, and an acknowledgment number for use in acknowledging a previously transmitted encapsulated packet.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

Fig. 1 is a block diagram of a wireless local area network, including a roaming server, access points, and mobile device according to the present invention.

Fig. 2 is a block diagram illustrating the components within the roaming server of Fig. 1.

Fig. 3 is a block diagram illustrating two access points having the same access point device address to provide a seamless transfer for a roaming mobile device according to the present invention.

Fig. 4 illustrates a procedure for a seamless transfer of a mobile device between two access points according to the present invention.

Fig. 5 is a representation of the master/slave relationships of an initial access point, a mobile device, and a target access point during a master-slave switch according to the present invention.

Fig. 6 is a flow chart of a procedure for a master/slave switch of the present invention.

Fig. 7 is a block diagram of the communications interface of Fig. 2 including a host controller interface and a packet encapsulation module.

Fig. 8 is a block diagram of a server wireless protocol stack and an associated access point wireless protocol stack according to the present invention.

Fig. 9 is a block diagram of the packet format of the present invention for an encapsulated packet for a host controller interface command based on a network based packet protocol.

DETAILED DESCRIPTION OF THE INVENTION

A description of preferred embodiments of the invention follows.

Fig. 1 is a block diagram of a network 20 including a roaming server 22, access points 24 (e.g., 24-1, 24-2, 24-3) to a WLAN (wireless local area network) 36, and mobile device 26. The network 34 is any suitable network for connecting access points 24 to a roaming server, such as a hard-wired Ethernet LAN or a wireless network using a wireless communications protocol. In one embodiment, the network 34 is hard-wired for part of the network 34 and wireless for one or more other parts of the network 34 (using one or more wireless communications protocols). The WLAN 36 is a network established in accordance with a wireless technology, which the present invention does not require to be the same as any wireless communication protocol or technology used in the network 34. In general, as used herein, the term "wireless technology" refers to a Bluetooth protocol technology, a IEEE 802.11 protocol technology, a ETSI HIPERLAN/2 protocol technology, or other wireless technology suitable for a WLAN 36 (e.g., typically providing coverage over 10 to 100 meters). The network 34 may use such a wireless technology for all or part of the network 34, or may use some other suitable wireless communications protocol. The network connection 28 (e.g., 28-1, 28-2, and 28-3) may be a hardwired connection, such as an Ethernet connection on a LAN 34, or may be a wireless connection based on a wireless technology or other suitable wireless communications protocol. The wireless connection 30 (e.g., 30-1 and 30-2) is a communication connection not requiring a hard-wired cable or link. For example, the wireless connection 30 is based on radio, optical, infrared, acoustic, or other non-hard-wired media.

The roaming server 22 is any suitable computing device or digital processing device that may serve as a server in the network 20. Such a roaming server 22 can be a

server, a router, a bridge, a switch, or other device that may serve the purpose of a central controller or a gateway server in the network 20. In one embodiment, the roaming server 22 is not a single physical entity, but the functionality of the roaming server 22 (such as shown in Fig. 2) is provided by a number of physical units (e.g., computers, servers, and/or network devices) that are networked together.

The access point 24 typically has a network connection 28 to the roaming server 22. The access point 24 also acts as a receiving point, or connecting point, to establish the wireless connection 30 with each mobile device 26. In that case, the access point 24 is equipped to recognize a wireless technology connection 30.

The mobile device 26 is any suitable type of device that will support a wireless technology. The mobile device 26 may be a computer with wireless connection adapter, a PDA (personal digital assistant), or a mobile telephone such as a cellular telephone. The WLAN subnet or channel 38 (e.g., 38-1 and 38-2) is an access point 24 and one or more mobile devices 26. In the case of the Bluetooth wireless technology, when there is more than one mobile device 26, then the WLAN subnet or channel 38 is termed a "piconet" and conventionally has up to seven mobile devices 26. When there is only one Bluetooth mobile device 26, then the channel 38 is known as a point to point link. For the present invention, even if there is more than one Bluetooth mobile device 26 connected to the access point 24, each Bluetooth mobile device 26 connected to the access point 24 views the channel 38 as a point to point link. The techniques of the present invention enable more than seven mobile devices 26 to connect to a single access point 24. The exact number depends on system performance. In the case of the IEEE 802.11 standard, a number of mobile devices 26 (potentially greater than seven, but limited by the address range within the subnet associated with that access point 24) are associated with a single access point 24.

To summarize briefly the operation of a transfer of the data link 32 from one access point 24-1 to another access point 24-2, the roaming server 22 determines that a mobile device 26 should change its LAN connection point from access point 24-1 to access point 24-2 based on a triggering or initiating event. Such an event can be the moving of the mobile device 26 (e.g., when the user moves the mobile device 26 from one location to another), or receiving a request from a mobile device 26 or access point

24 to move the mobile device 26. The triggering or initiating event can also be a load balancing event, such as receiving an indication that one access point 24 is congested and another access point 24 is less congested (e.g., so that the mobile device 26 can be moved to another access point 24 to obtain a higher level of service, such as more bandwidth). The triggering or initiating event can also be receiving an indication of the quality of service level assigned to the user of the mobile device 26 (e.g., moving the mobile device 26 to a new access point 24 to fulfill a predefined service level for the user of the mobile device 26). Furthermore, the triggering event can also be a indication of a poor or declining quality of the connection 30 (e.g., radio link) between the mobile device 26 and an access point 24 (e.g., resulting in a transfer of the mobile device 26 from one access point 24-1 to another access point 24-2 that provides an improved quality of service for the mobile device 26 over the radio link).

In general, the triggering event triggers a temporary or permanent handoff of the mobile device 26 from one access point 24-1 to another access point 24-2. The handoff may be due to a transient situation, such as due to temporary congestion of access point 24-1, or temporary decline in connection quality in the initial connection 30-1 (e.g., radio link quality). If the handoff is temporary, the initial access point 24-1 keeps knowledge of the mobile device 26 for a predefined period of time (e.g., short period of time) so that the mobile device 26 may transfer back to the initial access point 24-1 after the termination of the transient situation. The temporary handoff from one access point 24-1 to another access point 24-2 should occur quickly (i.e., without apparent or substantial interruption in the service to the mobile device 26), as is supported by the techniques of the present invention, as described herein. If the handoff is permanent, the initial access point 24-1 loses all knowledge of the mobile device 26. In general, if the handoff is temporary, but the transient situation persists, then the handoff may be made permanent.

After such a triggering or initiating event, the roaming server 22 instructs access points 24-1 and 24-2 to make a seamless handoff of the mobile device 26 from access point 24-1 to access point 24-2 at the data link level in a data link transfer 32 (that is, in the case of the Bluetooth technology, from point to point link 38-1 to point to point link 38-2, and, in the case of the IEEE 802.11 technology, from shared radio channel 38-1

to shared radio channel 38-2). In making this type of transfer at the data link transfer level 32, the transfer is transparent to the mobile device 26 and the connection 30-1 is transferred or reestablished as the wireless connection 30-2 without a requirement for a special technology or special software in the mobile device 26 (beyond the conventional wireless technology required to support communications over the WLAN 36).

In one example of determining that a mobile device 26 should change point to point links 38-1 to 38-2, the roaming server 22 first receives information (i.e., the triggering or initiating event) from access point 24-1 currently supporting the mobile device 26 as the mobile device 26 moves out of the range of access point 24-1. For example, this movement is indicated by a declining rate of packets (e.g., wireless connection packets based on the wireless technology) received at access point 24-1. The roaming server 22 then directs the access point 24-2 to establish a relationship or connection 30-2 with the subject mobile device 26. The roaming server 22 must have some indication from the access point 24-2 that the mobile device 26 is moving within range of that access point 24-2. In a preferred embodiment this indication may be provided by a query broadcast over the wireless medium (e.g., query over a radio frequency suitable for use with the WLAN 36 based on the wireless technology) from access point 24-2 to detect what mobile devices 26 are within range of the access point 24-2. When this is occurring, the roaming server 22 can instruct access points 24-1 and 24-2 to make the seamless handoff of the mobile device 26 as a data link transfer 32.

The roaming server 22 also determines base a triggering or initiating event based on congestion, quality of service level, or load balancing considerations. In this case, piconets 38-1 and 38-2 can be considered co-located (that is, provide wireless coverage to overlapping areas). For example, the mobile device 26 is within range of each access point 24-1 and 24-2 and may be connected, optionally, to either access point 24-1 or 24-2. In general, in a crowded environment such as a conference room there may well be multiple devices 26 desiring high speed WLAN 36 access.

Users may choose which access point 24 to join by signaling via the loading variable in the SDP (service discovery protocol) for the case of the Bluetooth technology, and the beacon for the case of IEEE 802.11 technology (based on proposed

modifications to the IEEE 802.11 standard). Alternatively, users may be directed to join a particular access point 24 by signaling via the loading variable in the radio protocol header or beacon. Generally, it may be desirable to introduce different levels of service for different users.

In operation, the mobile device 26 requests service from an access point 24 by sending a request along with the device address of the mobile device 26. The access point 24 would normally respond by paging the mobile device 26 and starting the synchronization between the access point 24 and the mobile device 26. Instead, in the present invention, the access point 24 passes the request along with the device address of the mobile device 26 back to the roaming server 22 which looks up the user's service level data 47 in the device database 42 (see Fig. 2) and the loading on each of the relevant access points 24 (e.g., traffic or congestion on the subnet that the mobile device 26 is connected to). In the case of the Bluetooth technology, the roaming server 22 then directs that the mobile device 26 connect to the appropriate access point 24 (this may not be the access point 24 that received the request). For example, the mobile device 26 requests service from access point 24-1, but, after determining the user's service level, the roaming server 22 signals access point 24-2 to page the mobile device 26 and establish a connection 30-2. In the case of the IEEE 802.11 technology, the roaming server 22 signals to all the relevant access points 24-1, 24-3 except the desired access point 24-2 to suppress their beacons.

When the mobile device 26 moves to a new connection 38 and starts to send packets, the roaming server 22 looks up the mobile device 26 in the device database 42, and according to the user service level data 47 and WLAN loading, the roaming server 22 might decide that the mobile device 26 should be communicating via another connection 38 that is covering that mobile device 26. That is, one access point 24 may offer a higher level of available bandwidth (i.e., lower level of congestion) for the mobile device 26 than another access point 24 that has less bandwidth available (i.e., higher level of congestion). For example, the preferable access point 24 may have fewer mobile devices 26 connected to it and thus more bandwidth available. The roaming server 22 may direct the mobile device 26 to a different access point 24. In either case the mobile device 26 is forced to transfer its connection 30. For example, a

user moves a mobile device 26 within range of both access points 24-1, 24-2. The mobile device 26 seeks to make a connection 30-1 to congested access point 24-1. The roaming server 22 thus directs the mobile device 26 to join a less congested access point 24-2, with the result shown by connection 30-2. Subsequently, the mobile device 26 moves to the less congested access point 24-2 in a seamless handoff, according to the techniques of the invention as described herein, without requiring re-registration with the roaming server 22.

The congestion at access point 24-1 may also be due to a transient situation or problem, such a temporary increase in traffic by one or more of the mobile devices 26 connected to access point 24-1. For example, after the mobile device 26 transfers to access point 24-2, the transient situation (e.g., congestion) at access point 24-1 terminates, and then the roaming server 22 directs the mobile device 26 to transfer back to access point 24-1.

As described earlier, a mobile device 26 may experience declining connection quality of the connection 30–1 (e.g., radio link) to the initial access point 24-1 (also termed the primary access point 24-1) due to some transient situation or problem. For example, path attenuation occurs if a human body is in the path of the radio link 30-1 between the mobile device 26 and the primary access point 24-1. That is, someone may be sitting down or standing in the path. The connection quality declines to a comparatively low level; for example, as measured by the signal strength of the connection 30-1 having a lower level (e.g., lesser amplitude) than the signal strength of the connection 30-2. The roaming server 22 directs the mobile device 26 to transfer from the primary access point 24-1 to a secondary access point 24-2 that has the better connection quality for the connection 30-2 (quality of the radio link) to the mobile device 26. This transfer may be temporary and the transient situation may terminate; for example, if the person obstructing the path moves out of the path. Then the roaming server 22 directs the mobile device 26 to transfer back from the secondary access point 24-2 to the primary access point 24-1.

Fig. 2 is a block diagram illustrating the components within the roaming server 22. These components include a digital processor 40, a device database 42, and a communications interface 44. The digital processor 40 hosts and executes a gateway

application 46 in the working memory of the roaming server 22. The gateway application 46 serves to provide for the management of the connections of the roaming server 22 to other devices, such as access points 24 and mobile devices 26 (typically through connections through access points 24). For example, the gateway application 46 may instruct an access point 24-1 to perform a transfer of wireless connections 30-1 so that the mobile device 26 can establish a new connection 30-2 with a different access point 24-2. In one embodiment, the gateway application 46 is implemented partially or totally in hardware, such as in an ASIC (application-specific integrated circuit).

The device database 42 in the roaming server 22 is a memory or disk or other storage device that provides database and storage services for the roaming server 22, such as providing service level data 47 that may be assigned to a mobile device 26, or a user of the mobile device 26. In another example, the device database 42 can provide information and store information on a wireless connection 30 such as wireless connection 30-1 so that the wireless connection 30-1 may be reestablished at a different access point 24 such as wireless connection 30-2 (i.e., using the same communication parameters as wireless connection 30-1 based on information that is stored in the device database 42 in the roaming server 22). The session data 48 is an example of such information, and can include the AP device address 52 (described for Fig. 3) and other information, such as encryption information. In one embodiment, the session data 48 also includes a mobile device address that the roaming server 22 assigns to the mobile device 26. For example, when the present invention is implemented for a Bluetooth wireless technology, the AP device address 52 is a BD_ADDR (Bluetooth device) address, and the mobile device address is an AM_ADDR (active member of a piconet) address. In another example, when the present invention is implemented for an IEEE 802.11 wireless technology, the AP device address 52 is a MAC (Medium Access Control) address, and the mobile device address is an AID (Association Identifier).

The device database 42 can be part of the roaming server 22, or may be accessed by the roaming server 22 over a communications connection or network connection (e.g., Internet connection).

A communications interface 44 of the roaming server 22 provides an interface to provide communications with other devices, such as a network interface to support network connections 28 over the LAN 34 to the access points 24. For example, the communications interface 44 is based on a NIC or Network Interface Card along with associated network communication software.

In one embodiment, a computer program product 80, including a computer readable or usable medium (e.g., one or more CDROM's, diskettes, tapes, etc.), provides software instructions for the gateway application 46. The computer program product 80 may be installed by any suitable software installation procedure, as is well known in the art. In another embodiment, the software instructions may also be downloaded over a wireless connection. A computer program propagated signal product 82 embodied on a propagated signal on a propagation medium (e.g., a radio wave, an infrared wave, a laser wave, a sound wave, or an electrical wave propagated over the Internet or other network) provides software instructions for the gateway application 46. In alternate embodiments, the propagated signal is an analog carrier wave or digital signal carried on the propagated medium. For example, the propagated signal may be a digitized signal propagated over the Internet or other network. In one embodiment, the propagated signal is a signal that is transmitted over the propagation medium over a period of time, such as the instructions for a software application sent in packets over a network over a period of milliseconds, seconds, minutes, or longer. In another embodiment, the computer readable medium of the computer program product 80 is a propagation medium that the computer may receive and read, such as by receiving the propagation medium and identifying a propagated signal embodied in the propagation medium, as described above for the computer program propagated signal product 82.

Fig. 3 is a block diagram of a WLAN 50 with two access points 24-4 and 24-5 that provide a seamless transfer for a roaming mobile device 26-2 using an access point device address transfer or spoofing approach according to the present invention. The AP device address 52 (e.g., 52-1, 52-2, 52-3, 52-4, and 52-5) is an identifier that provides an identification or address of an access point 24 in the WLAN 50. For example, for a Bluetooth implementation, the AP device address 52 is a Bluetooth

device address (BD_ADDR). In another example, for an IEEE 802.11 implementation, the AP device address 52 is a MAC (Media Access Control) address. The communication channel 54 (e.g., 54-1, 54-2, 54-3, 54-4, and 54-5) is a wireless communication link according to a wireless technology. In one embodiment, the communication channel 54 is an example of a wireless connection 30, as illustrated in Fig. 1. The point to point link 57 (e.g., 57-1 and 57-2) is a WLAN subnet, typically supported by a respective access point 24. In one embodiment, the WLAN 50 is one example of the WLAN 36 of Fig. 1, and the point to point links 57-1 and 57-2 are examples of the point to point link 38 of Fig. 1. Communication link transfer 56 indicates the transfer of the mobile device 26-2 from point to point link 57-1 to point to point link 57-2 using AP device address spoofing (i.e., the same AP device address 52-2 is used for access point 24-5 as for access point 24-4). Thus, communication channel 54-2A (between access point 24-4 and the mobile device 26-2) is based on AP device address 52-2, and communication channel 54-2B (between access point 24-5 and the mobile device 26-2) is also based on the same AP device address 52-2.

Fig. 4 illustrates a procedure 200 for a seamless transfer of a mobile device 26 between two access points 24 using the AP device address spoofing of Fig. 3. In step 202, a gateway application 46 in a roaming server 22 assigns session data 48 to the initial access point 24-4 to establish an initial connection 54-2 from the mobile device 26-2 through the initial access point 24-4 to the roaming server 22. The session data 48, for example, includes the AP device address 52-2, which is assigned to the initial access point 24-4 by the roaming server 22. In one embodiment, the roaming server 22 assigns a mobile device address to the mobile device 26 that is also included in the session data 48.

In step 204, a communications interface 44 of the roaming server 22 detects a triggering event that initiates a transfer of the mobile device 26-2 from the initial access point 24-4 to the target access point 24-5. This transfer is indicated by a communications link transfer 56' in Fig. 3. The triggering event, for example, can occur when the mobile device 26-2 is moved by the user from one location to another so that the mobile device 26-2 is moving out of range of the initial access point 24-4 and into range of the target access point 24-5. The triggering event can also be indicated by

congestion or the need for load balancing for the initial access point 24-4. For example, point to point link 57-1 may become congested in comparison to point to point link 57-2. Thus, the roaming server 22 initiates the transfer of the mobile device 26-2 from the initial access point 24-4 to the target access point 24-5. The triggering event can also be indicated by a decline in connection quality for connection 54-2A.

In step 206, the gateway application 46 transfers assignment of the session data 48 from the initial access point 24-4 to the target access point 24-5 to establish a target connection 54-2 from the mobile device 26-2 through the target access point 24-5 to the roaming server 22 based on the session data 48. For example, the session data 48 includes the AP device address 52-2, which the gateway application 46 is now assigning to the target access point 24-5 when it was previously assigned to the initial access point 24-4. The mobile device 26-2 can establish the same connection 54-2 using the AP device address 52-2 to the target access point 24-5. Thus, the mobile device 26-2 is using the same session data 48 when communicating with the target access point 24-5 that it was using when communicating with the initial access point 24-4.

For the example of an implementation based on IEEE 802.11 wireless technology, to accomplish the handoff using the techniques of the present invention, the target access point 24-5 (secondary access point) constructs a spoof frame (based on an 802.11 frame) that includes the AP device address 52 (MAC address) of the initial access point (primary access point), the mobile device address (Association ID) of the mobile device 26 that was assigned by the roaming server 22 to the mobile device 26, as well as any data to be transferred. For example, the roaming server 22 determines that the connection quality of a connection 30 (radio link connection) is declining, and thus sends the next data packet to the target or secondary access point (e.g., 24-5) and instructs it to create the spoof frame to be sent to the mobile device 26-2.

In another example of using the techniques of the present invention in an implementation based on IEEE 802.11 technology, the roaming server 22 instructs the target or secondary access point 24-5 to listen for a packet from the mobile device 26-2 even if the packet is addressed to another access point (e.g., 24-4) having a different MAC address , so that packets could be returned from either access point (e.g., 24-4 or

24-5). Generally, each access point 24 is aware of all the packets that arrive on a radio channel (e.g., assuming the channel can be accessed by both access points 24-4 and 24-5). To avoid interference between the access points 24-4 and 24-5 if on the same channel, frequency hopping between the main and spoofing channels could be used. In this case, both access points 24-4 and 24-5 normally operate on different main channels, but the controller or roaming server 22 forces secondary or target access point 24-5 to jump onto the same channel as the primary or initial access point 24-4 to send the spoofed packet.

In a conventional IEEE 802.11 approach, the access point 24 changes channels in response to SNMP (Simple Network Mangement Protocol) MIB-2 (Management Information Base) commands, which are kept in a queue to be processed on a best efforts basis. Typically, such a command is executed an indeterminate amount of time after the command is received. The present invention provides for a direct link between the access point 24 and the controller or roaming server 22 that can force an immediate channel change (as soon as the current packet is sent or received).

In a conventional IEEE 802.11 approach, the access point 24 uses a look up table to determine what to do with packets that arrive with a particular device address 52 (MAC address). When the mobile device 26 associates with an access point 24, then the device address 52 (MAC address) is added to this look-up table (and removed when the mobile device 26 disassociates from that access point 24).

In one embodiment for an IEEE 802.11 implementation, the present invention provides that the look-up table be expanded to include a new category called "watch out". For example, the watch out category includes device addresses 52 (MAC addresses) and spoofing channels that the access point 24 should look out for. When the access point 24 receives packets with one of these device addresses 52 (MAC addresses), at a receiver signal strength (RSSI) above a certain, predefined signal strength then the access point 24 sends a notification packet to the controller or roaming server 22.

In one embodiment for use with an IEEE 802.11 implementation, each mobile device 26 is synchronized with its access point 24-4, and typically changes synchronisation when associating with a different access point 24-5. If the access

points 24-4, 24-5 are on different channels, they are members of different ESS's (extended service sets). Then, the access points 24-4, 24-5 can be synchronized (because they are allowed to be synchronized because they are on different ESS's), thus avoiding any delay due to synchronization when the mobile device 26 is transferred form one access point 24-4 to the other access point 24-5.

For the example of an implementation of the present invention based on Bluetooth wireless technology, the techniques of the present invention support seamless hand-offs of a mobile device 26 between two access points 24 by assigning a unique BD_ADDR (Bluetooth device) address for the AP device address 52 to the access point 24 for each communication channel 54 that it is supporting. In a conventional piconet 57 (or subnet), the communication channel 54 is a master-slave link. The master (e.g., access point 24) can have up to seven slaves (e.g., mobile devices 26), each slave following a hop pattern (based on a spread spectrum frequency hopping) set by the master. Each master-slave communication channel 54 occupies one or more time slots.

In a Bluetooth device address spoofing point to point link 57, the access point 24 has a particular AP device address 52 associated with each master-slave link (i.e., communication channel 54). So in case of seven slaves there are seven communication channels 54 (e.g., master-slave links), and the access point 24 changes its AP device address 52 for each time slot. The access point 24 does not, however, need to change its timing offset as this is set by the clock of the access point 24, so all the slaves (e.g., mobile devices 26) are in synchronization with the master (e.g., access point 24). As each communications channel 54 is associated with a particular AP device address 52, the slaves hop between frequencies in synchronization with the access point 24 but they are no longer synchronized with each other.

This AP device address spoofing approach of the invention has several effects, as described in the following paragraphs.

It is easy to move mobile devices 26 between access points 24 by copying the session data 48, such as appropriate AP device address 52 and encryption codes, from one access point 24 to another access point 24. The session data 48 is the data for the current session between the mobile device 26 and the access point 24 based on a

connection 30. The session data 48 can include the AP device address 52 (e.g., Bluetooth address), mobile device address, hop sequence, frequency offset, and encryption data (e.g., encryption key or codes). The movement of session data 48, such as the AP device addresses 52 and encryption codes, is achieved by controlling all the access points 24 from a central roaming server 22. By having all the access points 24 in synchronization there is no clock offset to adjust, although this issue can be resolved using a clock offset command (e.g., Bluetooth clock offset command). The clock offset command may be required because Bluetooth devices, such as access points 24 and mobile devices 26, normally having free running clocks. Creating a piconet 57 requires each slave to temporarily apply an offset to their clock so as to synchronize clocks with the master.

The AP device address spoofing approach of the invention also permits a master (e.g., access point 24) to have an almost unlimited number of slaves (e.g., mobile devices 26) attached to it. This is possible because on each time slot there can be multiple slaves, each in synchronization with a different AP device address 52, and so hopping to a different sequence derived from the AP device address 52.

For example, a roaming server 22 that controls the access point 24-4 can decide, for each time slot, which AP device address 52-3 to give the access point 24-4. This AP device address 52-3 determines which mobile device 26-3 that the roaming server 22 communicates with through the access point 24-4. In this example, all the other mobile devices 26-1 and 26-2 connected to the access point 24-4 are probably on the wrong frequency when the roaming server 22 transmits the packet intended for mobile device 26-3. Thus, the other mobile devices 26-1 and 26-2, in effect, hear nothing from the roaming server 22 but they continue to stay in synchronization with the access point 24-4.

Occasionally two or more mobile devices 26 receive the same packet from the roaming server 22. All mobile devices 26, except the one intended to receive the packet, reject the packet because the encryption key does not work. In one embodiment, it is also possible to have a number of mobile devices 26 associated with the same AP device address 52 and use different encryption keys to designate the appropriate recipient. The techniques of the invention enable unlimited numbers of

mobile devices 26 (i.e., slaves) per piconet 57 and provide an alternative means of paging a mobile device 26, thus eliminating any constraint on the number of parked devices 26 (i.e., parked slaves).

If the transfer of the assignment of the session data 44 (step 202 in Fig. 4) is due to a transient situation, as described previously, the roaming server 22 may reassign the session data 44 to the initial access point 24-2 to re-establish the initial connection 54-2A after a termination of the transient situation. Thus the roaming server 22 reassigns the AP device address 52-2 to the initial access point 24-4 so that the mobile device 26-2 can communicate with the initial access point 24-4 using the same AP device address 52-2 that it used previously to communicate with the initial access point 24-4.

Fig. 5 is a representation of the master-slave relationships 302, 304, 306, 308, 310 of an initial access point 24-6, a mobile device 26-6, and a target access point 24-7 during a master/slave switch according to the present invention.

A master-slave switch (MSS) is a conventional, known operation in which the master (typically the creator of a piconet 38, such as an access point 24) and a slave (e.g., mobile device 26) switch roles so that the former master becomes a slave to the new master (former slave). The conventional switch involves a TDD (Time Division Duplex) switch so that the master and slave switch their TX (transmission) and RX (receiving) timing. The piconet 38 for the former master is based on piconet parameters derived from the AP device address 52 and clock of the former master. The conventional MSS switch leads to a newly defined piconet 38 based on piconet parameters derived from the AP device address 52 and clock of the new master.

The Bluetooth baseband specification version 1.0 B (available from Bluetooth SIG, Inc.), describes a conventional MSS in Section 10.9.3, "Master-slave switch." For this discussion, the slave in the original piconet 38 is unit "A" and the master in the original piconet 38 is unit "B" In summary, the conventional procedure for a MSS switch involves:

1. The two units (slave A and master B) agree to trade roles so that unit A will be master and B will be slave.
2. Slave A and master B perform a TDD switch between the slave A and

master B while retaining (temporarily) the hopping scheme of master B (i.e., spread-spectrum frequency hopping).

3. Master A sends a LMP (Link Manager protocol) timing packet to slave B to be used in synchronizing the timing of transmissions between master A and slave B.

4. Master A establishes new channel parameters for a new piconet 38 (including master A and slave B) based on new piconet parameters derived from the address 52 and clock of master A.

5. Master A communicates the new piconet parameters to each slave in the former piconet 38.

6. Master A verifies the switch of the slaves to the new piconet 38 based on the new piconet parameters.

Using the techniques of the present invention, it is possible to use this master-slave switch to facilitate a seamless handoff of a mobile device 26 between two access points 24 without requiring any additional software in the mobile device 26.

Referring to Fig. 5, access points 24-6 and 24-7 are controlled by a common roaming server 22. Initial access point 24-6 is the master of piconet A, and target access point 24-7 is the master of piconet B (see relationships 302 and 304 in Fig. 5). In one embodiment, piconet A and piconet B are examples of piconet 38 of Fig. 1. Fig. 6 is a flow chart illustrating a procedure 400 for a master-slave switch of the present invention. In step 402, the roaming server 22 detects a triggering event for mobile device 26-6, which is currently a slave to initial access point 24-6, indicating that the mobile device 26-6 should transfer from the initial access point 24-6 to the target access point 24-7. For example, mobile device 26-6 is moving beyond range as determined by virtue of increased packet loss. In this example, the roaming server 22 also detects that mobile device 26-6 has moved within range of target access point 24-7 as its device identifier (e.g., Bluetooth address) can be heard by target access point 24-7 on enquiry logical channel. As a result, the roaming server 22 desires to move mobile device 26-6 from initial access point 24-6 to target access point 24-7. At this point, the target access point 24-7 is a master in piconet B, and the mobile device 26-6 is still a

slave in piconet A (see relationship 304 in Fig. 5).

In step 404 (Fig. 6) the roaming server 22 achieves the transfer by instructing the initial access point 24-6 to start a master-slave switch with mobile device 26-6 and perform a partial switch. It follows step 1) and step 2) of the above summarized conventional procedure for a MSS, but then stops, so mobile device 26-6 is now master of piconet A (as illustrated by relationship 306 in Fig. 5) but all the devices are still following the hop pattern and offset of initial access point 24-6.

The target access point 24-7 can be the master of piconet B at the same time it is the slave of another piconet (e.g., piconet A). In step 405, the roaming server 22 instructs the target access point 24-7 to connect to mobile device 26-6 as a slave. At this point, mobile device 26-6 is the master of piconet A that includes target access point 24-7 as one of the slaves (see relationship 308 in Fig. 5).

In step 406 (Fig. 6), the target access point 24-7 then instructs mobile device 26-6 to perform a complete master-slave switch.

Upon completion of the master-slave switch, in step 408, the initial access point 24-6 cancels its partially completed master-slave switch so it returns to being master of piconet A. This does not change the piconet parameters for piconet A which is still following a hop sequence based on AP device address 52 of the initial access point 24-6. Mobile device 26-6 cannot follow because it is now a slave of target access point 24-7 in piconet B (see relationship 310 in Fig. 5). Mobile device 26-6 is now following a hop pattern set by the AP device address 52 of target access point 24-7, so the mobile device 26-6 is part of piconet B.

As indicated by step 408 of Fig. 6, the seamless handoff of the mobile device 26-6 from the initial access point 24-6 (for piconet A) to the target access point 24-7 (for piconet B) is complete.

Fig. 7 is a block diagram of the communications interface 44 of Fig. 2 including a host controller interface (HCI) 60 and a packet encapsulation module 62. The host controller interface 60 is a conventional interface specified by the wireless technology (e.g., Bluetooth HCI) that enables a host (e.g., mobile device 26 or access point 24) to control the wireless technology link control hardware (e.g., Bluetooth link control hardware) that controls the radio transmission and reception, as well as digital signal

processing, specified by the wireless technology protocol. The packet encapsulation module 62 is a software or hardware module configured according to the present invention to encapsulate host controller commands in a network based encapsulated packet 64. The encapsulated packet 64 includes host device address 66, sequence number 68, acknowledgment number 70, and the host controller command 72 (e.g., HCI command). In one embodiment, the host device address 66 is based on the AP device address 52 of Fig. 3.

In order to have effective control of access points 24 based on a wireless technology (Bluetooth, IEEE 802.11, ETSI HIPERLAN/2, or other wireless technology), it is necessary to transfer control of the access points 24 to a central roaming server 22. For ease of deployment this roaming server 22 needs be connected to the access points 24 via a standard LAN 34 using a protocol that can pass through routers. The techniques of the invention described for FIGs. 7, 8, and 9 apply to Bluetooth wireless networks as well as other wireless standards such as IEEE 802.11 and ETSI HIPERLAN/2.

In a preferred embodiment, UDP (User Datagram Protocol) packets include the encapsulated packets 64 of the present invention, which include HCI (Host Controller Interface) commands. These encapsulation techniques of the invention described herein for a preferred embodiment allows devices (e.g., access points 24) to be physically separate from the hosts (e.g., roaming servers 22) that implement the higher-level protocols. In the system described herein, this separation enables session roaming between access points 24, and forms an abstraction barrier between the non-standard baseband implementation and a conventional off-the-shelf implementation of the Bluetooth protocol stack.

Fig. 8 is a block diagram of a server wireless protocol stack 74 and an associated complementary access point wireless protocol stack 76. The server wireless protocol stack 74 (for a roaming server 22 or master access point 24) includes the TCP/IP (Transmission Control Protocol/Internet Protocol) layer 84, the PPP (point to point) layer 86, the RFCOMM (serial cable emulation protocol) layer 88, the L2CAP (logical link controller adaptation protocol) layer 90, the HCI transport layer 92-1, and the UDP/IP (User Datagram Protocol/Internet Protocol) transport layer 94-1. The

access point wireless protocol stack 76 includes the HCI transport layer 92-2, the UDP/IP transport layer 94-2, the link manager layer 100 (e.g., Bluetooth link manager), the link controller layer 102 (e.g., Bluetooth link controller), and the radio layer 104. An encapsulated packet signal 108 is a communications signal (e.g., over a LAN) that transports an encapsulated packet 64 between the server wireless protocol stack 74 and the access point wireless protocol stack 76. In particular, the encapsulated packet signal 108 (and hence encapsulated packet 64) is transported between stacks 74 and 76 at the HCI transport layer 92 and the UDP/IP transport layer 94. In another embodiment, the encapsulated packet signal 108 includes multiple encapsulated packets 64.

The advantage of UDP over TCP is a lower overhead and less delay caused by packet re-transmissions. The advantage of UDP encapsulation over Ethernet encapsulation is that the UDP-based packets easily pass through routers.

The splitting of the wireless protocol stack into two stacks 74 and 76, which includes encapsulation of host controller commands, (Figs. 7, 8, and 9) represents one aspect of the invention. The present invention does not require that the wireless protocol stack be split in order to implement the session data transfer (AP device address spoofing) aspect of the present invention (Figs. 3 and 4) and/or the master-slave switch aspect of the present invention (Figs. 5 and 6). Furthermore, the session data transfer (AP device address spoofing) aspect of the present invention may be implemented without splitting of the wireless protocol stack or use of the master-slave switch. In one embodiment, the present invention provides for the implementation of both the session data transfer (AP device address spoofing) aspect of the present invention and the splitting of the wireless protocol stack aspect of the present invention.

Fig. 9 illustrates the HCI UDP packet format for an encapsulated packet 64 that includes a host controller interface command 72 (e.g., HCI command) based on a network based packet protocol (e.g., UDP). In Fig. 9, the encapsulated host controller command 72 is part of the payload 122 when UDP packets are used for the HCI transport layer.

The version field 112 is a 1-byte value that identifies the version of the packet format used. For the first version of the HCI UDP protocol, the value 0x01 is used.

The type field 114 specifies a 1-byte value that determines the interpretation of the payload 122. Values are defined in Table 1.

Table 1

Packet Type	Packet Indicator
HCI Command	0 x 01
HCI ACL Data	0 x 02
HCI SCO Data	0 x 03
HCI Event	0 x 04
Session Control	0 x 10
ZLB	0 x 11

The values 0x01 through 0x04 are interpreted as in the HCI UART Transport Layer (as described in the Bluetooth Core Specification version 1.0B, available from Bluetooth SIG, Inc. (see also the www.bluetooth.com web site). The value 0x10 is for control messages related to session initiation and tear down. The value 0x11 is a Zero-Length Body (ZLB) message used for acknowledgments.

Continuing with Fig. 9, the BD_ADDR field 116 contains a host device address 66, such as a 48-bit Bluetooth device identifier, with the MSB being transmitted first. The BD_ADDR field 116 is shown as six 8-bit fields, 116-1, 116-2, 116-3, 116-4, 116-5, and 116-6 that together make up the 48-bit Bluetooth device identifier. The BD_ADDR identifies the host controller (e.g., access point 24 or roaming server 22) that is the source or destination of the encapsulated HCI packet 64.

The sequence number field 118 is an unsigned 16-bit integer field that contains a sequence number 68 used to ensure reliable, in-order delivery of encapsulated HCI packets 64. Its use is described later.

The acknowledgment number field 120 is an unsigned 16-bit integer field used to contain the acknowledgment number 70 to ensure reliable, in-order delivery of encapsulated HCI packets 64. Its use is described later.

Sequence numbers 68 and acknowledgment numbers 70 together provide reliable and sequenced transport of encapsulated HCI packets 64. The following description of the use of these numbers 68, 70 is based on the use of Nr and Ns fields in L2TP (Layer Two Tunneling Protocol) control packets. See Section 5.8, "Reliable Delivery of Control Messages" of RFC2661, "Layer Two Tunneling Protocol: L2TP", Internet Engineering Task Force, the entire teachings of which are incorporated herein by reference.

The sequence numbers 68 begin at a value of 0, and are incremented with the transmission of every encapsulated packet 64. The sequence counter is a free running counter represented modulo 65536. The sequence number 68 in the header of a received message is considered less than equal to the last received sequence number 68 if its value lies in the range of the last received sequence number 68 and the preceding 32767 values, inclusive. For example, if the last received sequence number 68 was 15, then messages with sequence numbers 68 with values of 0 through 15, as well as values 32784 through 65535, would be considered less than or equal. Such a message would be considered a duplicate of a message already received and ignored from processing. However, in order to ensure that all messages are acknowledged properly, receipt of duplicate messages is acknowledged. This acknowledgment may be either piggybacked on a message in queue, or sent explicitly through a ZLB acknowledgment.

All encapsulated packets 64 take up one slot in the sequence number space, except the ZLB acknowledgment. Thus the sequence number 68 is not incremented after a ZLB message is sent.

The acknowledgment number 70 is used to acknowledge messages received by the peer. It contains the sequence number 68 of the message the peer expects to receive next (e.g., the last sequence of a non-ZLB message received plus 1, modulo 65536). While the acknowledgment number 70 in a received ZLB is used to flush out messages from the local retransmit queue, the sequence number 68 of the ZLB does not update the acknowledgment number 70 of the next message sent.

In one embodiment, a sliding window is implemented in order to deal with random transmission time delays.

While this invention has been particularly shown and described with references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.

For example, the techniques of the present invention can be applied to wireless technologies and wireless communication protocols other than the Bluetooth technology, IEEE 802.11 technology, and the ETSI HIPERLAN/2 technology. In particular, the techniques of the present invention can be applied to other wireless technologies and protocols suitable for wireless communications among mobile devices 26 and network devices (e.g., access points 24).

CLAIMS

What is claimed is:

1. A computer method for performing a seamless handoff of a mobile device from an initial access point to a target access point in a wireless local access network, comprising the steps of:

assigning session data to the initial access point to establish an initial connection from the mobile device through the initial access point to a roaming server;

detecting a triggering event that initiates a transfer of the mobile device from the initial access point to the target access point; and

transferring assignment of the session data from the initial access point to the target access point to establish a target connection from the mobile device through the target access point to the roaming server based on the session data in response to the step of detecting the triggering event has occurred, enabling the mobile device to use the session data to communicate with the target access point, such that the mobile device transfers seamlessly from the initial access point to the target access point.

2. The computer method of Claim 1, wherein the step of detecting the triggering event comprises detecting that the mobile device is moving out of range of the initial access point and within range of the target access point.

3. The computer method of Claim 1, wherein the step of detecting the triggering event comprises determining that the target access point has a preferable level of congestion compared to a level of congestion for the initial access point.

4. The computer method of Claim 1, wherein the step of detecting the triggering event comprises determining that the target connection has a preferable level of connection quality compared to a level of connection quality for the initial

connection.

5. The computer method of Claim 1, wherein:

the step of assigning the session data to the initial access point comprises assigning an access point device address to the initial access point; and

the step of transferring assignment of the session data comprises terminating the assigning of the access point device address to the initial access point and assigning the access point device address to the target access point.

6. The computer method of Claim 1, wherein:

the initial connection is a first version of a point to point link between the initial access point and the mobile device based on assigning the access point device address to the initial access point; and

the target connection is a second version of the point to point link based on assigning the access point device address to the target access point and re-establishing the point to point link between the target access point and the mobile device.

7. The computer method of Claim 1, further comprising a step of registering the session data in a database.

8. The computer method of Claim 1, wherein the session data comprises the access point device address and encryption data.

9. The computer method of Claim 1, further comprising a step of assigning a mobile device address to the mobile device, and wherein the session data includes the access point device address and the mobile device address.

10. The computer method of Claim 1, wherein the step of detecting the triggering event occurs in response to a transient situation affecting the initial access

point; and further comprising a step of reassigning the session data to the initial access point to re-establish the initial connection after a termination of the transient situation.

11. The computer method of Claim 10, wherein the transient situation is one of a congestion of the initial access point and a decline of connection quality in the initial connection.

12. A system comprising a digital processor for performing a seamless handoff of a mobile device from an initial access point to a target access point in wireless local access network, the system comprising:

a gateway application executing on the digital processor for assigning session data to the initial access point to establish an initial connection from the mobile device through the initial access point to a roaming server; and

a communications interface coupled with the gateway application for detecting a triggering event that initiates a transfer of the mobile device from the initial access point to the target access point; and

the gateway application transferring assignment of the session data from the initial access point to the target access point to establish a target connection from the mobile device through the target access point to the roaming server based on the session data, enabling the mobile device to use the session data to communicate with the target access point, such that the mobile device transfers seamlessly from the initial access point to the target access point.

13. The system of Claim 12, wherein the triggering event is based on roaming of the mobile device and wherein the communication interface detects that the mobile device is moving out of range of the initial access point and within range of the target access point.

14. The system of Claim 12, wherein the triggering event is based on congestion in the wireless area network and wherein the communications interface determines

that the target access point has a preferable level of congestion compared to a level of congestion for the initial access point.

15. The system of Claim 12, wherein the triggering event is based on connection quality and wherein the communications interface determines that the target connection has a preferable level of connection quality compared to a level of connection quality for the initial connection.

16. The system of Claim 12, wherein the session data includes an access point device address and the gateway application:

assigns the session data to the initial access point by making an assignment of the access point device address to the initial access point; and

transfers the session data by terminating the assignment of the access point device address to the initial access point and by assigning the access point device address to the target access point.

17. The system of Claim 12, wherein:

the initial connection is a first version of a point to point link between the initial access point and the mobile device based on assigning the access point device address to the initial access point; and

the target connection is a second version of the point to point link based on assigning the access point device address to the target access point and re-establishing the point to point link between the target access point and the mobile device.

18. The system of Claim 12, wherein the gateway application registers the session data in a database.

19. The system of Claim 12, wherein the session data comprises the access point device address and encryption data.

20. The system of Claim 12, wherein the gateway application assigns a mobile device address to the mobile device, and wherein the session data includes the access point device address and the mobile device address.

21. The system of Claim 12, wherein the communication interface detects the triggering event occurs in response to a transient situation affecting the initial access point; and the gateway application reassigns the session data to the initial access point to re-establish the initial connection after a termination of the transient situation.

22. The system of Claim 21, wherein the transient situation is one of a congestion of the initial access point and a decline of connection quality in the initial connection.

23. A computer program product that includes a computer usable medium having computer program instructions stored thereon for performing a seamless handoff of a mobile device from an initial access point to a target access point in a wireless local area network, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

assign session data to the initial access point to establish an initial connection from the mobile device through the initial access point to a roaming server;

detect a triggering event that initiates a transfer of the mobile device from the initial access point to the target access point; and

transfer assignment of the session data from the initial access point to the target access point to establish a target connection from the mobile device through the target access point to the roaming server based on the session data in response to the step of detecting the triggering event has occurred, enabling the mobile device to use the session data to communicate with the target access point, such that the mobile device transfers seamlessly from the initial access

point to the target access point.

24. A method in a roaming server in a wireless local area network for performing a seamless handoff of a mobile device from an initial piconet having an initial access point to a target piconet having a target access point;

assigning the mobile device associated with the initial access point a master role for the initial piconet;

assigning the target access point a slave role in the initial piconet while the target access point retains a master role in the target piconet; and

establishing an association of the mobile device with the target piconet by switching roles of the mobile device and target access point, so that the mobile device establishes the association with the target piconet as a slave of the target piconet, and the target access point terminates the slave role of the target access point with the initial piconet, while the target access point maintains the master role in the target piconet, such that the mobile device transfers seamlessly from the initial piconet to the target piconet.

25. The method of Claim 24, further comprising the step of assigning the initial access point that has the master role for the initial piconet a slave role in the initial piconet until the switching of the roles of the mobile device and target access point is completed, thereafter reassigning the initial access point for the initial piconet the master role for the initial piconet.

26. The method of Claim 24, further comprising the step of determining to initiate a transfer of the mobile device from the initial piconet to the target piconet by detecting an increased rate of packet loss for packets transmitted from the mobile device to the initial access point and by detecting that the mobile device is within range of the target access point.

27. A roaming server in a wireless local area network for performing a seamless handoff of a mobile device from an initial piconet having an initial access point

to a target piconet having a target access point, the roaming server comprising:

a communication interface for communicating with the initial access point and the target access point;

a digital processor coupled to the communication interface, the digital processor hosting and executing a gateway application that is configured to:

assign the mobile device associated with the initial access point a master role for the initial piconet;

assign the target access point a slave role in the initial piconet while the target access point retains a master role in the target piconet; and

establish an association of the mobile device with the target piconet by switching roles of the mobile device and target access point, so that the mobile device establishes the association with the target piconet as a slave of the target piconet, and the target access point terminates the slave role of the target access point with the initial piconet, while the target access point maintains the master role in the target piconet, such that the mobile device transfers seamlessly from the initial piconet to the target piconet.

28. The roaming server of Claim 27, wherein the gateway application assigns the initial access point that has the master role for the initial piconet a slave role in the initial piconet until the switching of the roles of the mobile device and the target access point is completed, and thereafter reassigns the initial access point for the initial piconet the master role for the initial piconet.

29. The roaming server of Claim 27, wherein the gateway application determines to initiate a transfer of the mobile device from the initial piconet to the target piconet by detecting an increased rate of packet loss for packets transmitted from the mobile device to the initial access point and by detecting that the mobile device is within range of the target access point.

30. A computer program product that includes a computer usable medium having computer program instructions stored thereon for performing a seamless handoff of a mobile device from an initial piconet having an initial access point to a target piconet having a target access point, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

assign the mobile device associated with the initial access point a master role for the initial piconet;

assign the target access point a slave role in the initial piconet while the target access point retains a master role in the target piconet; and

establish an association of the mobile device with the target piconet by switching roles of the mobile device and target access point, so that the mobile device establishes the association with the target piconet as a slave of the target piconet, and the target access point terminates the slave role of the target access point with the initial piconet, while the target access point maintains the master role in the target piconet, such that the mobile device transfers seamlessly from the initial piconet to the target piconet.

31. A method in a roaming server for enabling seamless roaming of mobile devices among access points in a wireless local area network, comprising the steps of:

establishing a host controller interface in the roaming server;

encapsulating host controller commands in a packet-based network protocol for use in communication with access points in the wireless area network, the host controller commands directed to a connection session of the mobile device with the wireless local area network; and

exchanging the encapsulated host controller commands with access points in the wireless area network to enable a mobile device to receive the host controller commands and maintain the connection session while roaming among the access points.

32. The method of Claim 31, wherein the step of encapsulating the host controller

commands comprises encapsulating each host controller command in an encapsulated packet based on the packet-based network protocol, and providing a device address of a host exchanging each encapsulated packet, a sequence number for use in a series of encapsulated packets, and an acknowledgment number for use in acknowledging a previously transmitted encapsulated packet.

33. The method of Claim 31, wherein the packet-based network protocol is a user datagram protocol.

34. A roaming server comprising a digital processor for enabling seamless roaming of mobile devices among access points in a wireless area network, comprising:

a host controller interface established in the roaming server;

a packet encapsulation module executing on the digital processor for encapsulating host controller commands in a packet-based network protocol for use in communication with access points in the wireless area network, the host controller commands directed to a connection session of the mobile device with the wireless local area network; and

a communications interface coupled with the digital processor for exchanging the encapsulated host controller commands with access points in the wireless area network to enable a mobile device to receive the host controller commands and maintain the connection session while roaming among the access points.

35. The roaming server of Claim 34, wherein the packet encapsulation module encapsulates each host controller command in an encapsulated packet based on the packet-based network protocol, and the packet encapsulation module provides a device address of a host exchanging each encapsulated packet, a sequence number for use in a series of encapsulated packets, and an acknowledgment number for use in acknowledging a previously transmitted encapsulated packet.

36. The roaming server of Claim 34, wherein the packet-based network protocol is a user datagram protocol.

37. A computer program product that includes a computer usable medium having computer program instructions stored thereon for enabling seamless roaming of mobile devices among access points in a wireless area network, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

establish a host controller interface in a roaming server;

encapsulate host controller commands in a packet-based network protocol for use in communication with access points in the wireless area network, the host controller commands directed to a connection session of the mobile device with the wireless local area network; and

exchange the encapsulated host controller commands with access points in the wireless area network to enable a mobile device to receive the host controller commands and maintain the connection session while roaming among the access points.

38. An encapsulated packet for encapsulating and communicating commands based on a host controller interface using a packet-based network protocol, the encapsulated packet comprising:

a host controller command based on the host controller interface;

device address of a host exchanging the encapsulated packet;

a sequence number for use in a series of encapsulated packets; and

an acknowledgment number for use in acknowledging a previously transmitted encapsulated packet.

39. An encapsulated packet signal embodied in a propagated signal on a propagated medium, the encapsulated packet signal for encapsulating and communicating commands based on a host controller interface using a packet-based network

protocol, the encapsulated packet signal comprising:

a host controller command based on the host controller interface;

device address of a host exchanging the encapsulated packet;

a sequence number for use in a series of encapsulated packets; and

an acknowledgment number for use in acknowledging a previously transmitted encapsulated packet.

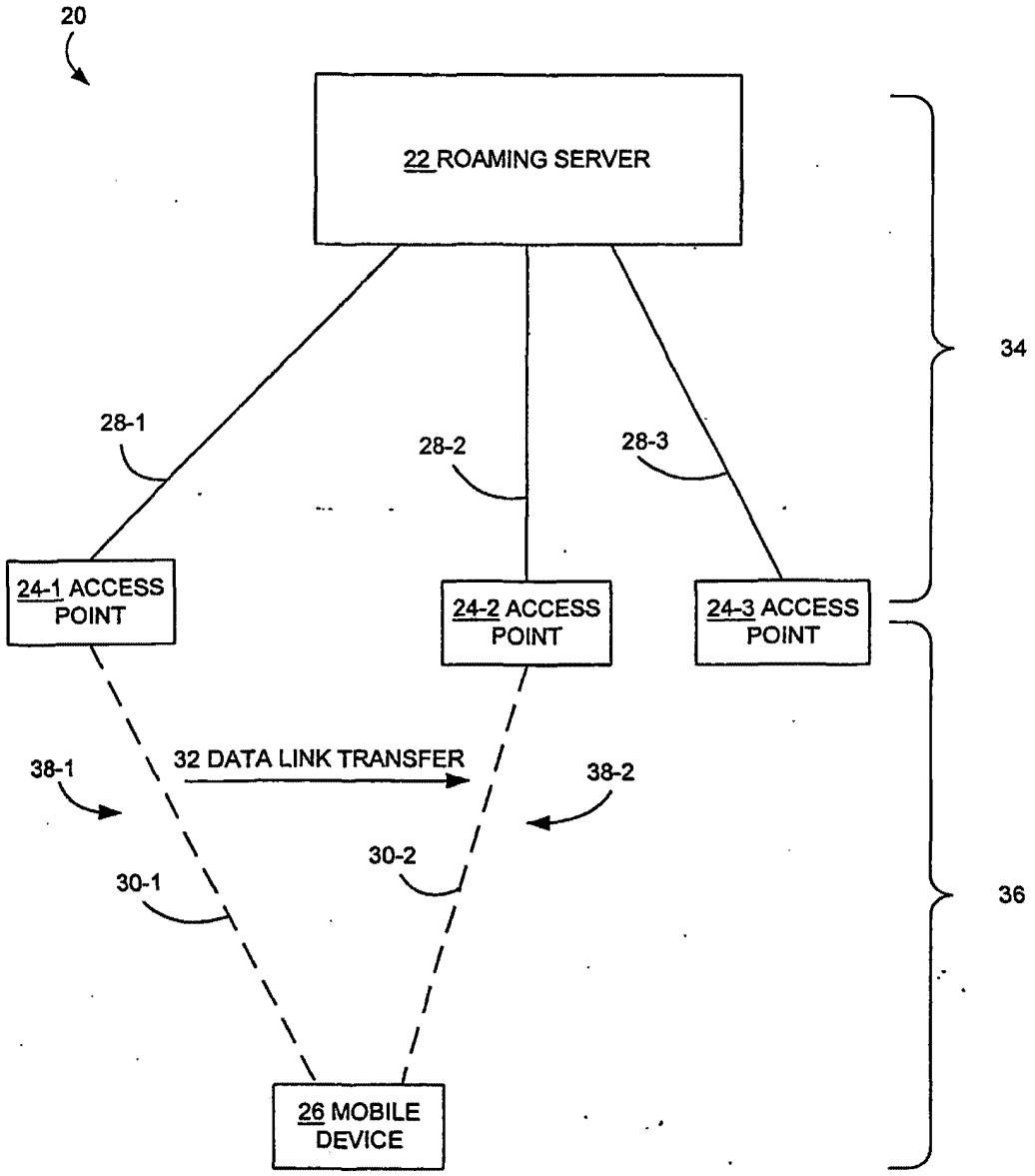

20
22 ROAMING SERVER
34
28-1
28-2
28-3
24-1 ACCESS POINT
24-2 ACCESS POINT
24-3 ACCESS POINT
38-1
32 DATA LINK TRANSFER
38-2
30-2
30-1
36
26 MOBILE DEVICE

FIG. 1

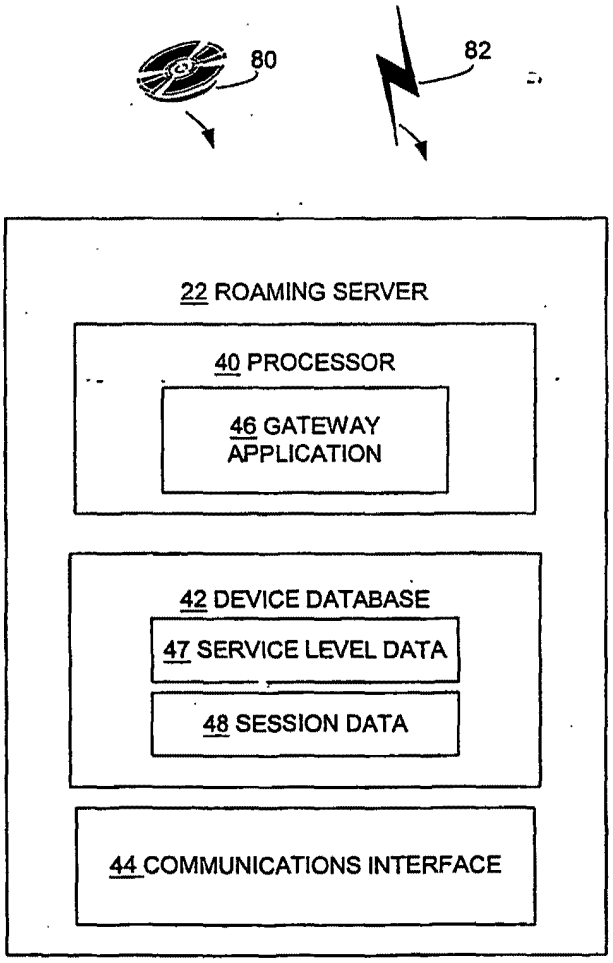

80
82
22 ROAMING SERVER
40 PROCESSOR
46 GATEWAY APPLICATION
42 DEVICE DATABASE
47 SERVICE LEVEL DATA
48 SESSION DATA
44 COMMUNICATIONS INTERFACE

FIG. 2

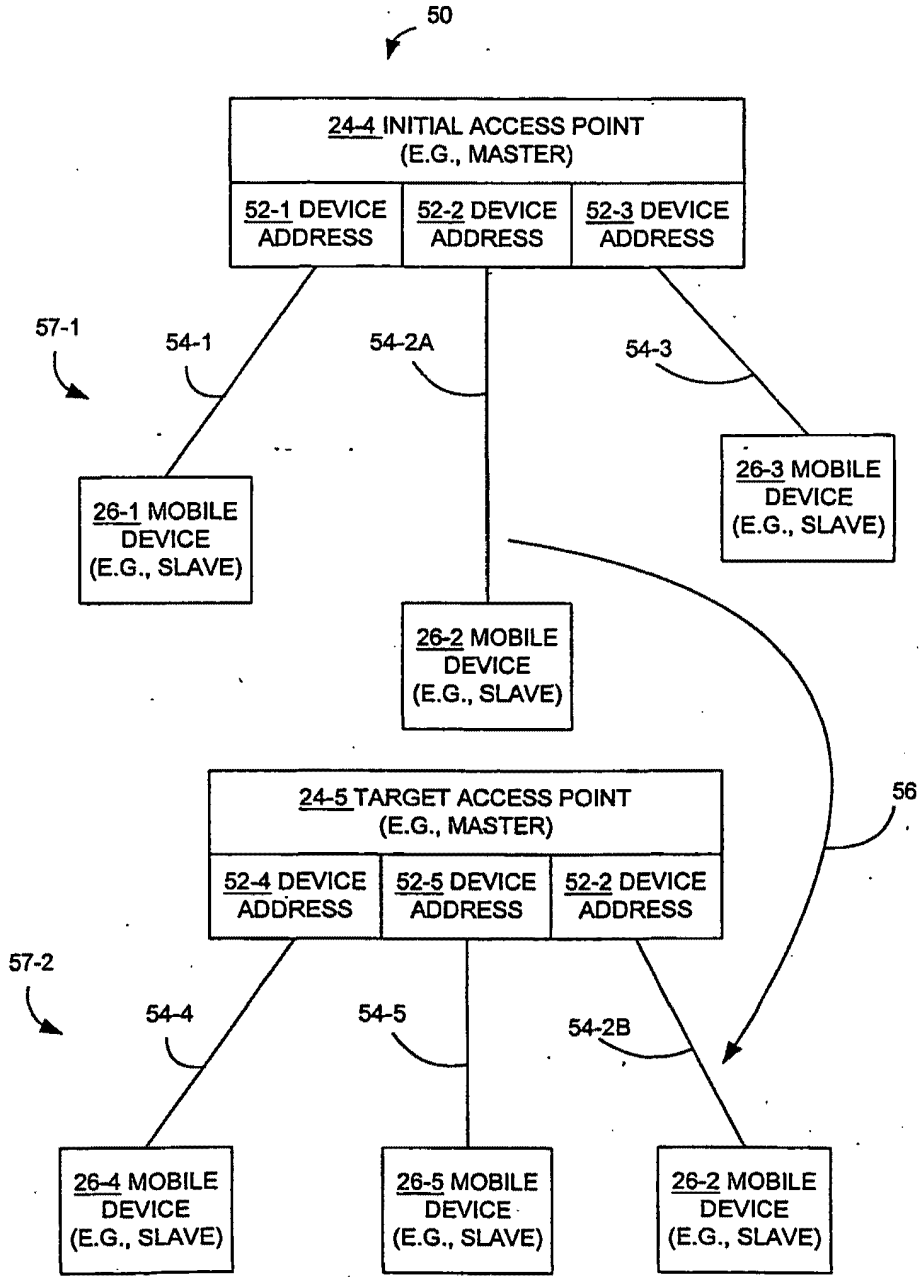

50
24-4 INITIAL ACCESS POINT (E.G., MASTER)
52-1 DEVICE ADDRESS
52-2 DEVICE ADDRESS
52-3 DEVICE ADDRESS
57-1
54-1
54-2A
54-3
26-1 MOBILE DEVICE (E.G., SLAVE)
26-3 MOBILE DEVICE (E.G., SLAVE)
26-2 MOBILE DEVICE (E.G., SLAVE)
56
24-5 TARGET ACCESS POINT (E.G., MASTER)
52-4 DEVICE ADDRESS
52-5 DEVICE ADDRESS
52-2 DEVICE ADDRESS
57-2
54-4
54-5
54-2B
26-4 MOBILE DEVICE (E.G., SLAVE)
26-5 MOBILE DEVICE (E.G., SLAVE)
26-2 MOBILE DEVICE (E.G., SLAVE)

FIG. 3

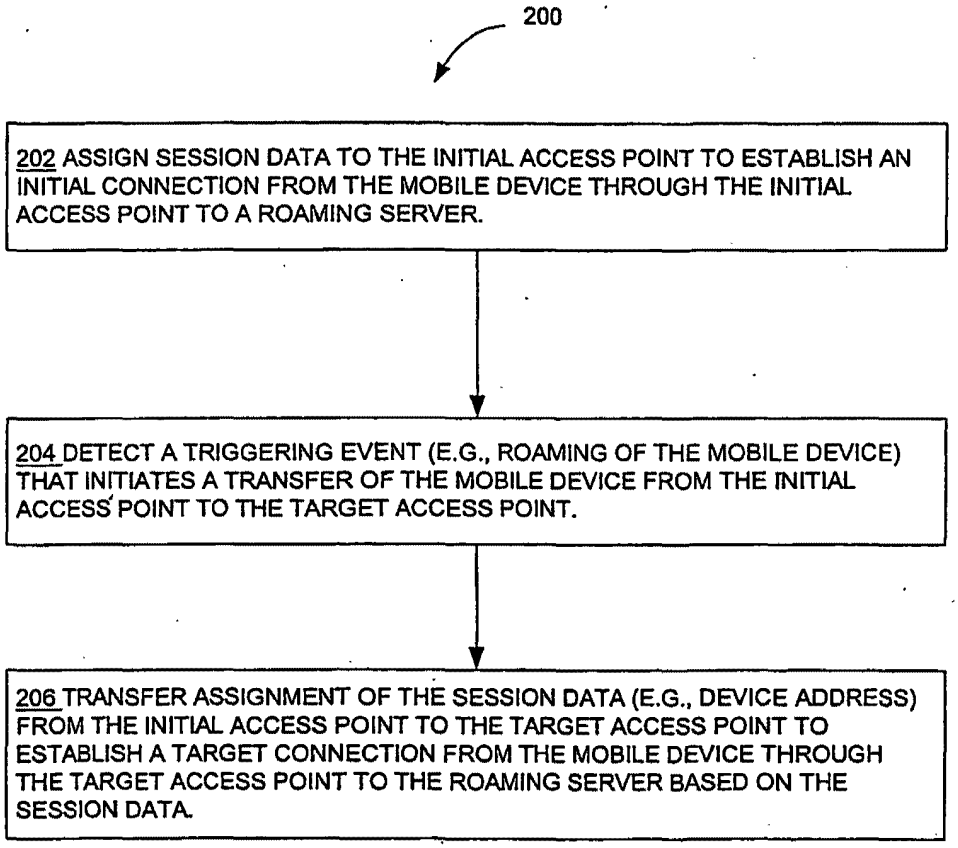

200
202 ASSIGN SESSION DATA TO THE INITIAL ACCESS POINT TO ESTABLISH AN INITIAL CONNECTION FROM THE MOBILE DEVICE THROUGH THE INITIAL ACCESS POINT TO A ROAMING SERVER.
204 DETECT A TRIGGERING EVENT (E.G., ROAMING OF THE MOBILE DEVICE) THAT INITIATES A TRANSFER OF THE MOBILE DEVICE FROM THE INITIAL ACCESS POINT TO THE TARGET ACCESS POINT.
206 TRANSFER ASSIGNMENT OF THE SESSION DATA (E.G., DEVICE ADDRESS) FROM THE INITIAL ACCESS POINT TO THE TARGET ACCESS POINT TO ESTABLISH A TARGET CONNECTION FROM THE MOBILE DEVICE THROUGH THE TARGET ACCESS POINT TO THE ROAMING SERVER BASED ON THE SESSION DATA.

FIG. 4

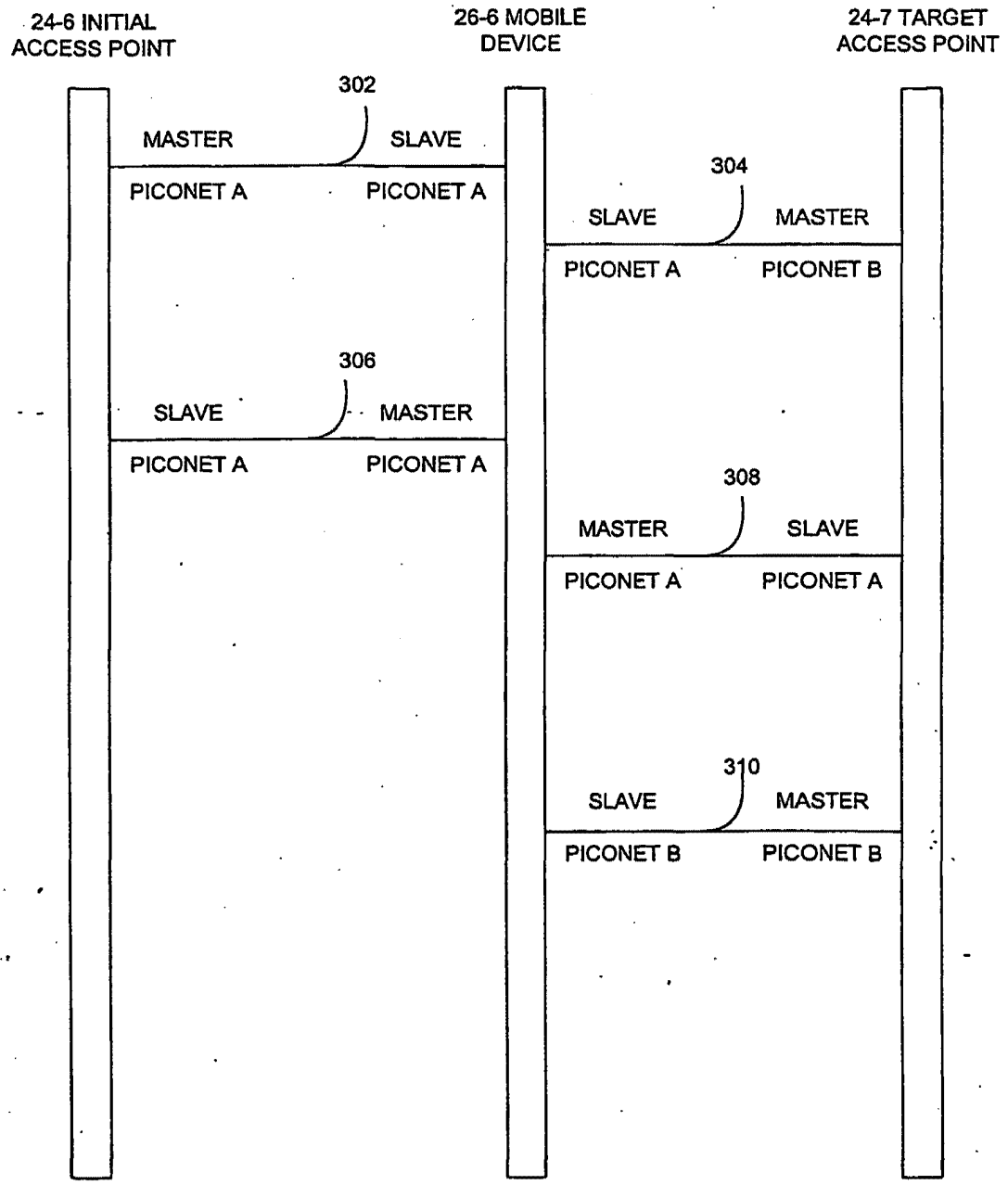

24-6 INITIAL ACCESS POINT
26-6 MOBILE DEVICE
24-7 TARGET ACCESS POINT
302
MASTER
SLAVE
PICONET A
PICONET A
304
SLAVE
MASTER
PICONET A
PICONET B
306
SLAVE
MASTER
PICONET A
PICONET A
308
MASTER
SLAVE
PICONET A
PICONET A
310
SLAVE
MASTER
PICONET B
PICONET B

FIG. 5

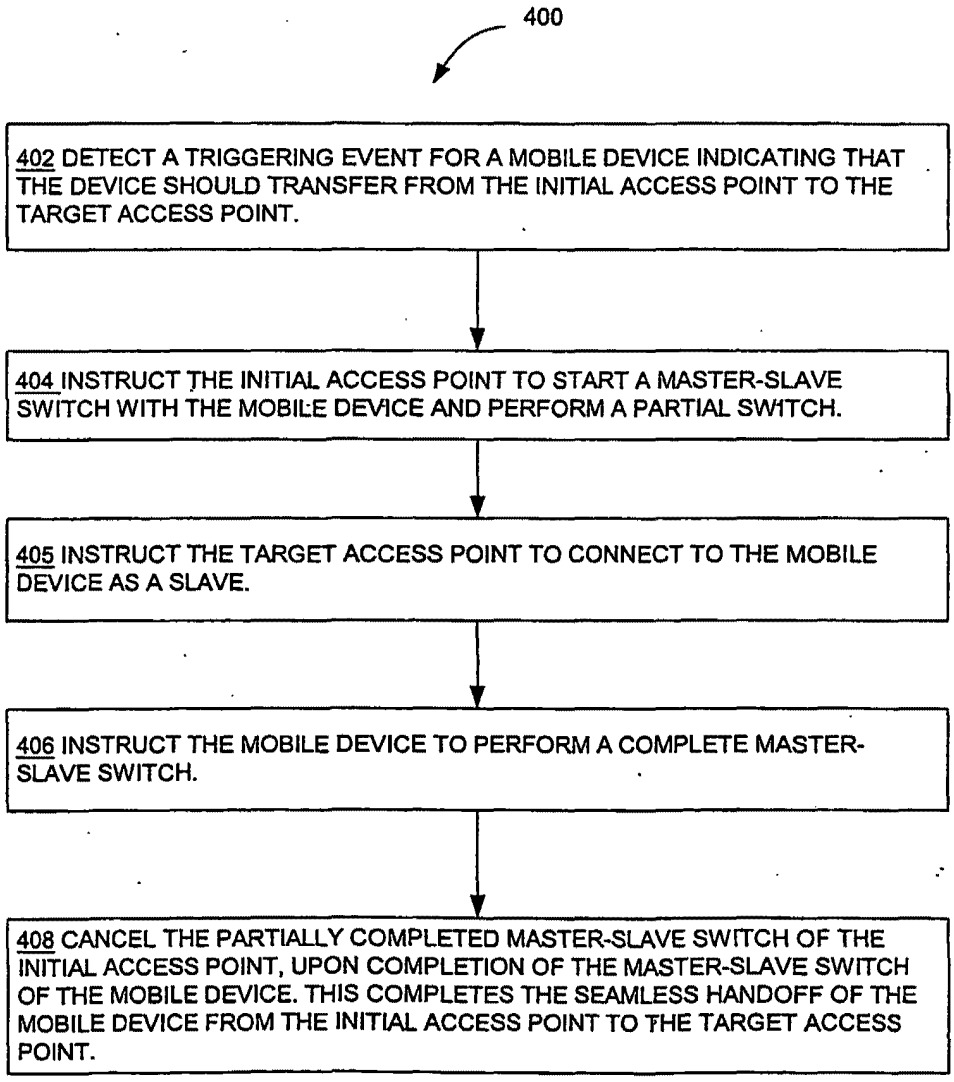

400
402 DETECT A TRIGGERING EVENT FOR A MOBILE DEVICE INDICATING THAT THE DEVICE SHOULD TRANSFER FROM THE INITIAL ACCESS POINT TO THE TARGET ACCESS POINT.
404 INSTRUCT THE INITIAL ACCESS POINT TO START A MASTER-SLAVE SWITCH WITH THE MOBILE DEVICE AND PERFORM A PARTIAL SWITCH.
405 INSTRUCT THE TARGET ACCESS POINT TO CONNECT TO THE MOBILE DEVICE AS A SLAVE.
406 INSTRUCT THE MOBILE DEVICE TO PERFORM A COMPLETE MASTER-SLAVE SWITCH.
408 CANCEL THE PARTIALLY COMPLETED MASTER-SLAVE SWITCH OF THE INITIAL ACCESS POINT, UPON COMPLETION OF THE MASTER-SLAVE SWITCH OF THE MOBILE DEVICE. THIS COMPLETES THE SEAMLESS HANDOFF OF THE MOBILE DEVICE FROM THE INITIAL ACCESS POINT TO THE TARGET ACCESS POINT.

FIG. 6

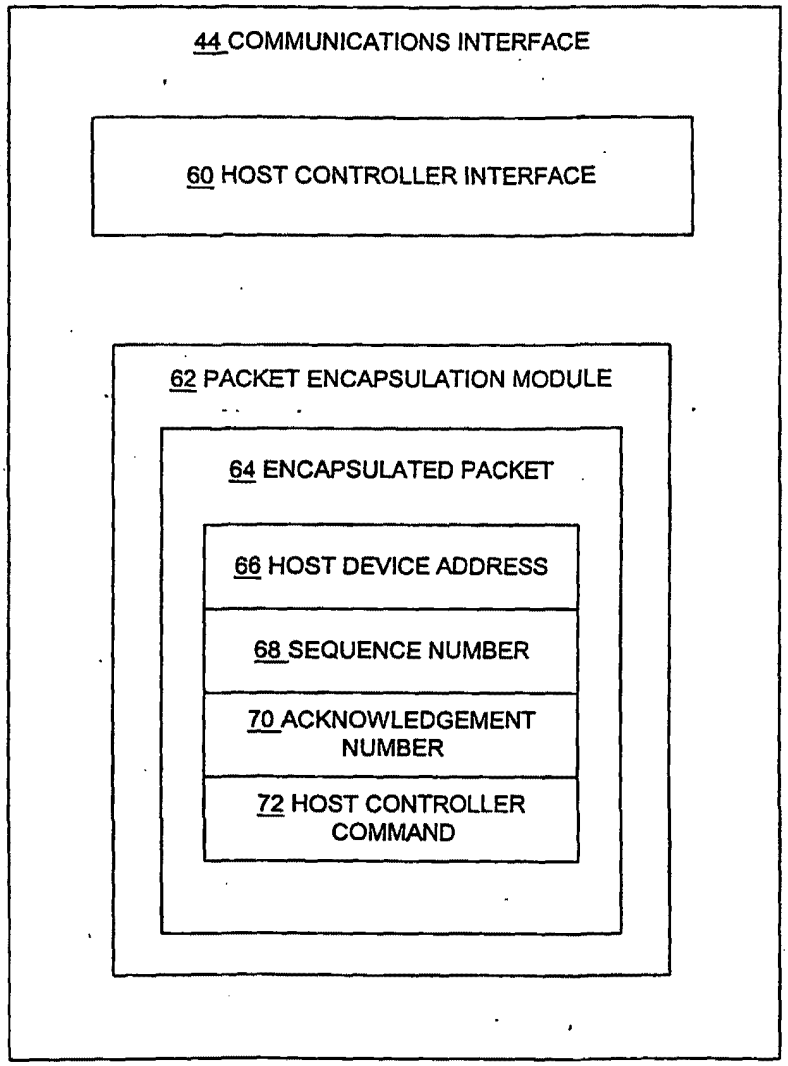

44 COMMUNICATIONS INTERFACE
60 HOST CONTROLLER INTERFACE
62 PACKET ENCAPSULATION MODULE
64 ENCAPSULATED PACKET
66 HOST DEVICE ADDRESS
68 SEQUENCE NUMBER
70 ACKNOWLEDGEMENT NUMBER
72 HOST CONTROLLER COMMAND

FIG. 7

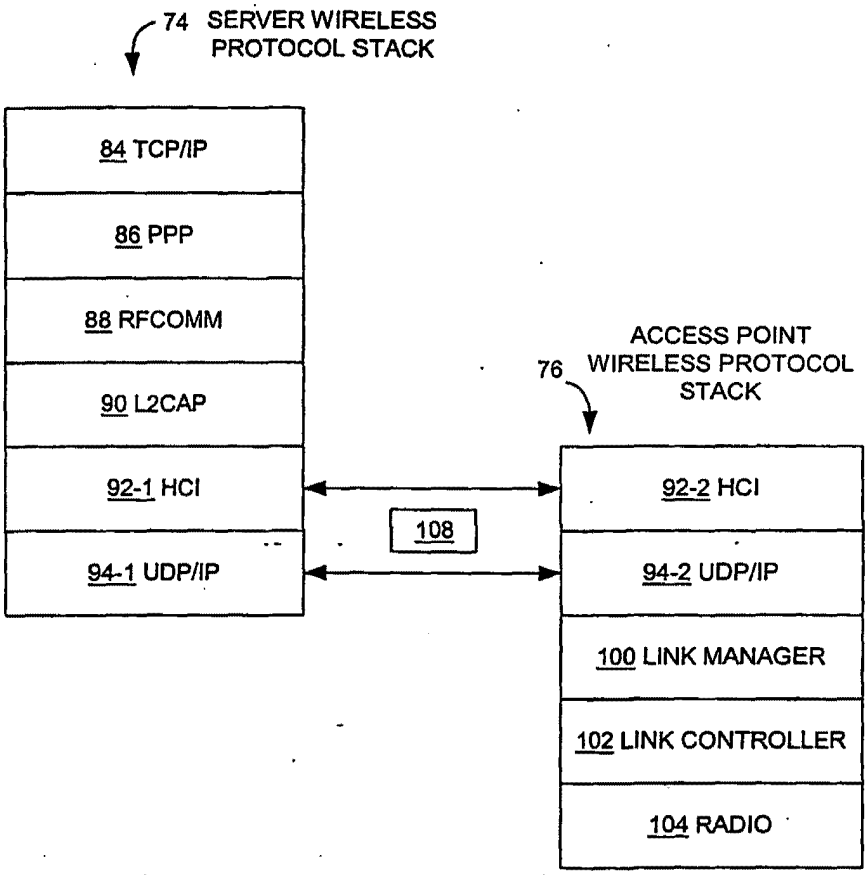
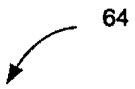

74 SERVER WIRELESS PROTOCOL STACK
84 TCP/IP
86 PPP
88 RFCOMM
90 L2CAP
92-1 HCI
94-1 UDP/IP
108
ACCESS POINT WIRELESS PROTOCOL STACK
76
92-2 HCI
94-2 UDP/IP
100 LINK MANAGER
102 LINK CONTROLLER
104 RADIO

FIG. 8



112 VERSION	114 TYPE	116-1 BD_ADDR	116-2 BD_ADDR
116-3 BD_ADDR	116-4 BD_ADDR	116-5 BD_ADDR	116-6 BD_ADDR
118 SEQUENCE NUMBER		120 ACKNOWLEDGEMENT NUMBER	
122 PAYLOAD (E.G., HOST CONTROLLER COMMAND 72)			

FIG. 9

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 October 2002 (03.10.2002)

PCT

(10) International Publication Number
WO 02/077820 A1

(51) International Patent Classification[7]: G06F 11/30, H04L 9/00

(21) International Application Number: PCT/US02/08986

(22) International Filing Date: 21 March 2002 (21.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/278,450	26 March 2001 (26.03.2001)	US
60/300,531	25 June 2001 (25.06.2001)	US
09/911,092	23 July 2001 (23.07.2001)	US
10/055,028	23 January 2002 (23.01.2002)	US

(71) Applicant: **BLUESOCKET, INC.** [US/US]; 7 New England Executive Park, Burlington, MA 01803 (US).

(72) Inventors: **CHRISTOFFEL, Thomas, W.**; 256 Bedford Street, Concord, MA 01742 (US). **JUITT, David, N.**; 77 Wollaston Avenue, Arlington, MA 02476 (US). **CRAWSHAW, Geoff**; 96 Wyoming Avenue, Needham, MA 02492 (US). **CROSBIE, David, B.**; 47 Bay State Avenue, Somerville, MA 02144 (US).

(74) Agent: **HEFFAN, Ira**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

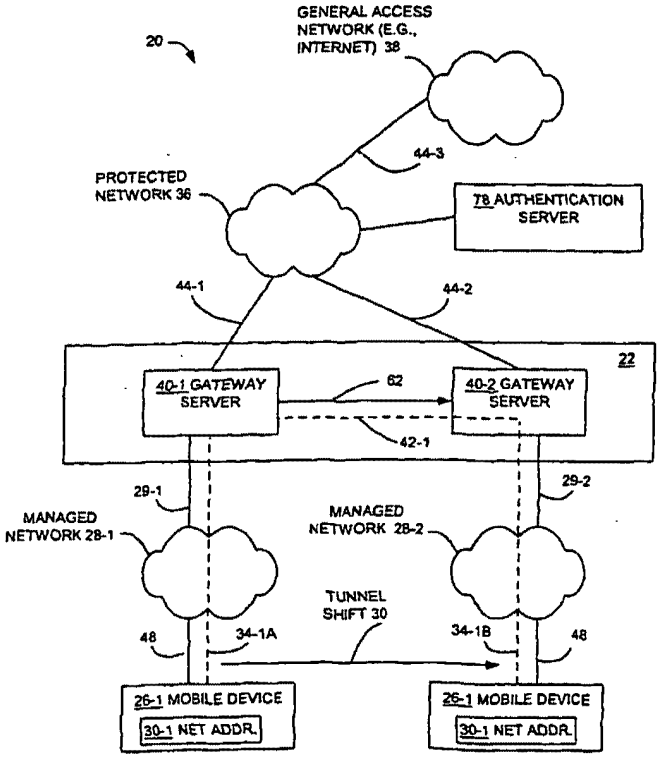
(81) Designated States *(national)*: AU, CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHODS AND SYSTEMS FOR ENABLING SEAMLESS ROAMING OF MOBILE DEVICES AMONG WIRELESS NETWORKS



(57) Abstract: A mobile device (180) roams (182) between two wireless network (28-3, 28-4).

WO 02/077820 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHODS AND SYSTEMS FOR ENABLING SEAMLESS ROAMING OF MOBILE DEVICES AMONG WIRELESS NETWORKS

BACKGROUND OF THE INVENTION

Networked desktop computing is typical in both the office and home. Networking of mobile devices, such as mobile telephones, laptop computers, headsets, and PDAs (Personal Digital Assistants), is more difficult. Wireless standards, such as IEEE 802.11 and Bluetooth (BT) are designed to enable these devices to communicate with each other and a wired LAN (Local Area Network). Such mobile devices are capable of transferring between wireless LANs (WLANs), and some mobile devices can transfer between different types of wireless networks (e.g., a WLAN and a cellular mobile telecommunications network). Such transfers typically require establishing a new connection with the new WLAN for the mobile device making the transfer.

These technologies provide for a common attachment approach for different devices, and so enables mobile phones, laptops, headsets, and PDAs to be easily networked in the office and eventually in public locations. The Bluetooth technology is described in the Bluetooth specification, available from Bluetooth SIG, Inc. (see also the www.bluetooth.com web site), the entire teachings of which are herein incorporated by reference. Other standards, such as the IEEE 802.11 (Institute of Electrical & Electronics Engineers) and ETSI (European Telecommunications Standards Institute) HIPERLAN/2, provide a generally similar wireless connection function as Bluetooth and may be used to support WLAN (wireless LAN) communications. See the IEEE 802.11 "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," the entire teachings of which are herein incorporated by reference. See also the ETSI specifications for HIPERLAN/2, such as ETSI document number TR 101 683, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview," the entire teachings of which are herein incorporated by reference.

The IEEE 802.11 Wireless LAN standard focuses on access points on the same subnet. Security is handled via WEP (Wireless Equivalent Protocol). This sets up an encrypted link (data, not headers) between the mobile device and the access point. If a mobile device decides to associate itself with a new access point on the same subnet then it uses a series of Associate and Disassociate commands defined within the IEEE 802.11 specification to signal its move from the old to the new access point. The new access point then uses its DS (distribution system) layer to route the encrypted data back to the original access point (as 802.3 frames) in order to be encrypted and decrypted. Hence the unencrypted data enters and leaves the original access point irrespective of the actual access point that the mobile is using. This is done because setting up a new encrypted link is a relatively slow process and hence transferring the entire connection to the new access point, so that if the old access point was no longer involved at all, would result in a break in the communication. If a mobile device transfers to a new subnet, a new secure (WEP) session is typically established between the mobile device and the new access point with a new encryption link.

WLAN access points (LAP's) such as those used by 802.11 and Bluetooth are part of an IP subnet; that is, a range of IP addresses that are normally used by all the devices connected to a section of the network delineated by a router (which may also be known as a gateway) that directs packets to and from devices that are outside the subnet.

In one conventional approach, devices (e.g., a router, gateway, or mobile devices) inside the subnet for a WLAN are primarily identified by their MAC address. This is a fixed address tied to the Ethernet card. IP addresses are associated with MAC addresses. There can be multiple IP addresses associated with a single MAC address. Each router or gateway device on the subnet maintains a cache which maps IP addresses within the subnet to the associated MAC addresses. Data packets are sent to the MAC address associated with the IP address by the cache. (For destinations outside the sub-net the data is sent to the router which then forwards them.)

In order for a device (e.g., router or gateway) to find the MAC address associated with a particular IP address, an ARP (address resolution protocol) is used. The device (e.g., router or gateway) follows the ARP and sends out a broadcast message asking for the device associated with the included IP address to respond with its MAC address. Once received it is added to the cache.

For a situation where there are mobile devices attached to an access point then the mobiles MAC address is associated with an IP address from within the subnet IP address space. If the mobile device moves to another access point that is in the same subnet then all that is required is for the new access point to realize that it must respond to the MAC address of the mobile device that has just associated itself, and the previous access point to cease to respond to that MAC address. The MAC to IP address cache does not need to be changed.

If, however, the mobile device moves to an access point connected to another subnet then the original IP address will be unusable. The mobile device would typically be required to obtain a new IP address and so break the previous connection. The user of the mobile device is typically required to re-establish a stateful end-to-end connection such as IPSec (IP Security Protocol, an encryption protocol from the Internet Engineering Task Force (IETF), an organized activity of the Internet Society), and so the user may be required to re-register with the WLAN. For example, the user may be required to re-enter a PIN (personal identification number) or some other password when connecting to a new subnet.

Thus, in order for mobile clients to roam from one subnet to another, one connection (and all its attributes including security) must be dropped and then re-established in the other subnet. In other words, seamless hand-offs can only be done within a subnet and not across different subnets.

Some mobile devices also have the capability of moving among different types of wireless communication networks, such as between a WLAN network (Bluetooth or IEEE 802.11, as described above) and a mobile telecommunications network, such as one based on a mobile telephone communication protocol (e.g., CMTS or cellular mobile telephone system, GSM or Global System for Mobile communications, PCS or Personal Communications Services, or UMTS or Universal

Mobile Telecommunications System). For example, the mobile device (e.g., laptop computer or PDA) includes communications interfaces (e.g., communications hardware and software) that allow the mobile device to communicate with two (or more) different types of wireless networks. Typically, when the mobile device moves to access a different type of wireless network, the current communication session with the current wireless network terminates, and the mobile device establishes a new communication session (new communication) with the newly accessed wireless network.

SUMMARY OF THE INVENTION

To be truly effective, mobile users must be able to move their mobile devices freely from location to location. For example, users must be able to move their mobile devices from the office to their own conference room to the airport lounge to their client's conference room, while maintaining access to the same set of resources without manually registering anew in each location. They should also be able to send and receive messages and voice calls, wherever they are located. Connection servers, such as routers, WLAN gateways, and security servers, should be able to handle a mobile device that moves its connection to the network from access point to access point, from public to private networks, or from one wireless network system to a different type of wireless network system.

Wireless networks, such as two wireless networks that a mobile device roams between, can be characterized as homogenous networks or heterogenous networks, based on whether or not they follow the same (or very similar) wireless communications protocols for communicating with a roaming mobile device. To roam between homogenous networks, the mobile device need have only one wireless communication interface that supports the same wireless communication protocol as used by the homogenous networks. To roam between two heterogenous networks, the mobile device must have two corresponding wireless communications interfaces that support two different wireless communication protocols. By using these two interfaces, the mobile device can communicate over the two heterogenous networks and roam between them. ,

In conventional approaches, mobile devices have difficulties in roaming among networks in a seamless manner that does not require the termination and establishment of communication session with a home network server for the mobile device when leaving one network and accessing another network.

For homogenous networks, the mobile device typically has difficulties maintaining a secure connection (e.g., WEP based session) that was established in one network when moving to another homogenous network, even if there are no access problems in accessing the other homogenous network. For an IEEE 802.11 based secure wireless connection using WEP, the mobile device must establish a new secure connection when moving to another homogenous network. In addition, a related problem is that IP (Internet Protocol) Layer III security associations exist only with one server and cannot easily or quickly be transferred. In order to roam between subnets (homogenous networks), a mobile device (client for that server) would have to break down one security association and rebuild it for the new association with another subnet. The approach of the present invention avoids subnets by creating one logical server (a gateway system composed of gateway servers intercommunicating with each other) from a collection of servers.

For heterogenous networks, the mobile device typically has difficulties in accessing a second heterogenous network after roaming from a first heterogeneous network. In traditional approaches the mobile device requires reauthentication that leads to establishing a new connection with the second heterogenous network, and to losing concurrently the previous connection to the first heterogenous network. The present invention describes an approach by which mobile stations can roam between one type of wireless network (e.g., a WLAN) and another (e.g., a cellular network) without having to reauthenticate itself.

Thus, the present invention provides techniques for maintaining connections (such as to a home network server for the mobile device) during a seamless transfer of a mobile device between wireless networks, for both homogenous wireless networks and heterogenous wireless networks.

In one aspect of the present invention related to homogenous networks, the present invention provides a method and gateway system (e.g., two or more gateway

servers associated with two or more homogenous wireless networks) for enabling a mobile device to roam among access points in a wireless local area network, the mobile device capable of communicating with the access points. The gateway system includes an initial gateway server for establishing a secure connection (e.g., tunnel) from the mobile device through an initial access point to the initial gateway server, and a target gateway server in communication with the initial gateway server. The initial gateway server provides connection information to the target gateway server about the secure connection, based on a triggering event that initiates a transfer of the mobile device from the initial access point to a target access point associated with the target gateway server. The target gateway server receives the connection information to maintain the secure connection from the mobile device through the target access point back to the initial gateway server.

In another aspect, the mobile device is assigned an internet protocol address by the initial gateway server. The secure connection is based on the internet protocol address and standard authenticating credentials. The initial gateway server maintains the connection based on the internet protocol address assigned to the mobile device.

In a further aspect, the initial gateway server and the target gateway server are coupled by a nested tunnel between the initial gateway server and the target gateway server. The nested tunnel serves to maintain the secure connection from the mobile device back to the initial gateway server.

The nested tunnel between the initial gateway server and the target gateway server, in another aspect, is based on a hard wired connection between the initial gateway server and the target gateway server.

In one aspect, the triggering event is a movement of the mobile device out of range of the initial access point and within range of the target access point.

The triggering event, in another aspect, is a determination that the target access point has a preferable level of congestion compared to a level of congestion for the initial access point.

In a further aspect, the target gateway server extends the secure connection from the target gateway server to the initial gateway server, so that the initial gateway server decrypts secure messages originating from the mobile device.

The target gateway server, in another aspect, establishes a virtual representation of the initial gateway server at the target gateway server.

In another aspect related to heterogenous networks, the present invention provides a method and network gateway (e.g., computer system serving as a gateway to a network system composed of network devices, mobile devices, one or more wireless networks, and communication links) for enabling a mobile device to roam between a first wireless network and a second wireless network. The first wireless network is substantially heterogeneous with the second wireless network. Both the first wireless network and the second wireless network are capable of communicating with an intermediary network. The mobile device is capable of accessing the first wireless network and the second wireless network. The network gateway includes a digital processor coupled with a communications interface. The digital processor hosts and executes a gateway application that configures the digital process to receive a request to access the second wireless network. The gateway application and the mobile device are associated with the first wireless network. The request is on behalf of the mobile device and indicates a network system specifying the second wireless network. For example, the mobile device makes a request to the network gateway through the first wireless network and the communications interface for the mobile device to gain access to the second wireless network (e.g., if the mobile device is moving out of range of the first wireless network and into range of the second wireless network). The gateway application also configures the digital processor to obtain through the communications interface and through the intermediary network an access identifier for the second wireless network and to provide the access identifier to the mobile device to use when accessing the second wireless network.

In another aspect, the first wireless network is a wireless local area network, the second wireless network is a cellular telecommunications network, and the mobile device is a personal digital assistant.

In a further aspect, the request includes a user identification of a user of the mobile device. The gateway application configures the digital processor to determine the identity of the network system as a function of the user identification.

In another aspect, the gateway application configures the digital processor to provide through the communications interface an authentication request based on the request to a dynamic host configuration server.

The access identifier, in one aspect, is an internet protocol address and the intermediary network is the internet.

In a further aspect, the gateway application configures the digital processor to request through the communications interface the access identifier from a second network gateway for the second wireless network. The second network gateway provides the access identifier from a predefined range of access identifiers allocated to the second wireless network.

In another aspect, the gateway application configures the digital processor to store the access identifier in a device database that includes a device identification for the mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

Fig. 1 is a block diagram of a homogenous network environment including a gateway system according to the present invention.

Fig. 2 is a block diagram of one example of the physical connections for the homogenous network environment of Fig. 1.

Fig. 3 is a flow chart of a procedure for transferring a secure connection for a mobile device from one access point to another access point for Fig. 2.

Fig. 4 is a block diagram of an example of a portion of the homogenous network environment with sample network addresses.

Fig. 5 is a block diagram of a virtual network interface in a gateway server in the gateway system of Fig. 4.

Fig. 6 is a block diagram of a gateway system, multiple gateway servers, and multiple mobile devices, configured according to the present invention.

Fig. 7 is a schematic diagram illustrating an initial IP assignment for a mobile device in a homogenous network environment according to the present invention.

Fig. 8 is a schematic diagram illustrating an authentication request made on behalf of a mobile device in the homogenous network environment 20 of Fig. 7.

Fig. 9 is a schematic diagram illustrating a third-party IP address request made on behalf of the mobile device in the homogenous network environment of Fig. 7.

Fig. 10 is a schematic diagram illustrating an ARP (address resolution protocol) request made on behalf of a mobile device in a homogenous network environment according to the present invention.

Fig. 11 is a schematic diagram illustrating a location update message made on behalf of the mobile device in the homogenous network environment of Fig. 10.

Fig. 12 is a schematic diagram illustrating an information message made on behalf of the mobile device in the homogenous network environment of Fig. 10.

Fig. 13 is a schematic diagram illustrating a nested tunnel for the mobile device in the homogenous network environment of Fig. 10.

Fig. 14 is a block diagram of a heterogenous network environment illustrating a device transfer between two heterogenous network systems according to the present invention.

Fig. 15 is a flow chart of a procedure for providing an access identifier to the mobile device to enable the device transfer of Fig. 14.

Fig. 16 is a schematic diagram illustrating a WLAN gateway and a mobile telephone network gateway in a heterogenous network environment according to the present invention.

Fig. 17 is a schematic diagram illustrating a heterogenous network environment with two heterogenous network systems and a mobile device, according to the present invention.

Fig. 18 is a schematic diagram illustrating a mobile device connected to a cellular network system, according to the present invention.

Fig. 19 is a schematic diagram illustrating an ARP request made on behalf of a mobile device in a heterogenous network environment, according to the present invention.

Fig. 20 is a schematic diagram illustrating an authentication query made on behalf of the mobile device in the heterogenous network environment of Fig. 19.

Fig. 21 is a schematic diagram illustrating an internetwork tunnel for the mobile device in the heterogenous network environment of Fig. 19.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed to techniques for enabling the seamless transfer of mobile devices between wireless communication networks. Such networks may be homogenous, that is, based on the same or similar wireless communication protocols that allow for the transfer of mobile devices between the homogenous wireless networks. Figs. 1-13 are directed to preferred embodiments of the present invention for the seamless transfer of mobile devices between homogenous networks. Other networks are heterogenous, that is, based on dissimilar wireless communication protocols that do not allow for (or readily allow for) the transfer of mobile devices between the heterogenous networks. Figs. 14-21 are directed to preferred embodiments of the present invention for the seamless transfer of mobile devices between heterogenous wireless networks.

Fig. 1 is a block diagram of a homogenous network environment 20 including a gateway system 22 that includes two gateway servers 40-1 and 40-2 according to the present invention. The network environment 20 also includes a mobile device 26-1, homogenous managed networks 28-1, 28-2, a protected network 36, and a general access network 38. The protected network 36 connects to the gateway system 22 by network connections 44-1 and 44-2, and the general access network 38

connects to the protected network 36 by network connection 44-3. The gateway system 22 connects to managed networks 28-1, 28-2 by managed network connections 29-1 and 29-2. A mobile device 26-1 connects to the managed network 28-1 by wireless connection 48, and the same mobile device 26-1 connects to the managed network 28-2 by a wireless connection 48. Each mobile device includes a network address 30.

The gateway server 40 (e.g., 40-1 and 40-2) is any suitable computing device or digital processing device that may serve as a network device or server in the networked environment 20. Such a gateway server 40 can be a server, a router, a bridge, a switch or other network communications or computing device (or any combination thereof) that may serve the purpose of a central control or gateway in the networked environment 20. The gateway system 22 is a system of two or more gateway servers 40 that provides communications between a mobile device 26 through a managed network 28 through the gateway system 22 to the protected network 36 and the general access network 38. The gateway servers 40-1, 40-2 in the gateway system 22 communicate with each other, such as through the network connections 44-1, 44-2, which would enable gateway servers, such as gateway servers 40-1 and 40-2, to communicate through the protected network 36. Alternatively, the gateway servers 40-1, 40-2 and the gateway system 22 communicate through direct connections such as hard wired cables through a LAN or other connections, such as wireless connections between the gateway servers 40-1, 40-2.

In a preferred embodiment, the gateway system 22 includes two or more gateway servers 40, and a mobile device 26 can transfer to any gateway server 40 (e.g., 40-2) and transfer among gateway servers 40 in the gateway system 22 while maintaining a connection 42 (e.g., 42-1) to an initial gateway server 40 (e.g., 40-1).

The protected network 36 is a network that is limited by an access control scheme that would prevent, for example, any unauthorized user from accessing the protected network 36. One function of a gateway server 40-1,40-2 in the gateway system 22 is to control access to the protected network 36. For example, the gateway server 40-1 may determine whether the user of a mobile device 26-1 can be

authenticated and then authorized to allow access over the network connection 44-1 to the protected network 36 through the gateway server 40-1. The protected network 36, for example, can be an enterprise network, such as a LAN based on an Ethernet or other LAN protocol that is suitable for use in a corporation or other organization. That is, the enterprise network 36 provides services and resources for the individuals in that corporation or other organization. The protected network 36 can also be an internet service provider or ISP as well as a wireless ISP or WISP.

The general access network 38 is a generally available network that is not necessarily protected and that is available to a wide range of users (although specific parts of the general access network 38 may be protected). One example of a general access network 38 is a packet-based general access network based on the IP (Internet Protocol) such as the Internet. The general access network 38 provides resources that may be accessed by the users of mobile devices 26 through the gateway system 22 and protected network 36. For example, a general access network 38 provides web servers and web sites that users of mobile devices 26 may wish to access.

The mobile device 26 (referred to in Figs. 1-21) is any suitable type of device that will support a wireless technology, such as a wireless connection 48 from the mobile device 26 to the managed network 28. The mobile device 26 may be a computer with a wireless connection adapter, a PDA (personal digital assistant) or a mobile telephone, such as a cellular telephone or other mobile telephone adapted through a managed network 28. The managed network 28 (referred to in Figs. 1-21) is a homogenous network of network devices managed by the gateway server 40. The managed network 28 provides connections (e.g., 48) to mobile devices 26 and serves as an intermediary between the mobile device 26 and a gateway server 40. The managed networks 28 are homogenous in the sense that they are all based on the same networking protocol (e.g., wireless technology protocols) or similar protocols that readily allow transfers of mobile devices 26. In one example, a managed network 28 includes access points 24 as illustrated in Figure 2. The present invention does not require that the managed network 28 be composed of access points 24, only that the managed network 28 be composed of any suitable network

device, such as a switch, router, access point or gateway that can serve as an intermediary between a mobile device 26 and a gateway server 40.

The wireless connection 48 provides for a connection from the mobile device 26-1 to the managed network 28-1 or 28-2. The wireless connection 48 is any suitable wireless connection based on a wireless technology, such as a Bluetooth technology, an IEEE 802.11 technology, an ETSI HIPERLAN/2 technology, or other wireless technology suitable for use in a WLAN typically providing coverage of 10 to 100 meters. The managed network connections 29-1, 29-2 connects the gateway servers 40-1, 40-2 to the managed networks 28-1 and 28-2. The managed network connection 29 (e.g., 29-1, 29-2) can be any suitable connection for connecting the gateway server 40 to the intermediary devices in the managed network 28. The managed network connection 29 (e.g., 29-1, 29-2) can be a wireless connection or a hard wired cable, such as hard wired cables for an Ethernet LAN.

The mobile device 26-1 also includes a network address 30, which is an address that indicates the network address for the mobile device 26-1. The mobile device 26-1 is connected to the gateway server 40-1 by a tunnel connection 34-1A. In general, the tunnel connection 34 (e.g., 34-1A and 34-1B) is a virtual connection or tunnel through the physical connections 48, 29 to the gateway server 40-1 or 40-2. The tunnel connection 34-1A, 34-1B is referred to herein as "tunnel connection 34-1" to indicate that the tunnel connection 34-1A and 34-1B are the same tunnel from the standpoint of the mobile device 26-1. As shown in Fig. 1, the tunnel 34-1A may be shifted by a tunnel shift 30 to a tunnel connection 34-1B that maintains the same virtual tunnel connection 34-1 for the mobile device 26-1. The tunnel connection 34-1 is based on a secure tunneling protocol such as IPSec (IP Security Protocol) or PPTP (point to point tunneling protocol). Such a secure protocol can be any routing and security protocol that has encryption built in, and thus guarantees the confidentiality and integrity of all of the data transmitted. The connection information 62 is provided by the initial gateway server 40-1 to the target gateway server 40-2 to provide information about a secure connection (e.g., 34-1A).

The nested tunnel connection 42 (e.g., 42-1 through 42-5 in Figs. 1, 2, and 6) continues the tunnel connection 34-1B from the gateway server 40-2 to the gateway

server 40-1 so that the mobile device 26-1 operates with the same connection through the tunnel connection 34-1B that the mobile device 26-1 had with the connection 34-1A. For example, the tunnel 34-1B is nested within the tunnel 42-1. The mobile device 26-1 cannot distinguish whether it is communicating with the gateway server 40-1 through the tunnel connection 34-1A or the tunnel connection 34-1B. That is, the transfer of a mobile device 26-1 from gateway server 40-1 through the tunnel shift 30 to gateway server 40-2 is transparent to the mobile device 26-1. Furthermore, the mobile device 26-1 maintains the same network address 30 which is not altered during the tunnel shift 30 (see Fig. 4). That is, the mobile device uses the same network address 30 when communicating through the tunnel connection 34-1A as when communicating through the tunnel connection 34-1B. In one embodiment, the nested tunnel connection 42 is an IP Layer III security tunnel and may be based on a security tunneling protocol such as described for the tunnel connection 34-1. For example, the nested tunnel 42 is a tunnel based on IPsec/PPTP protocols nested within another tunnel based on the SSL (Secure Socket Layer) protocol over the GRE (Generic Routing Encapsulation) protocol.

In one embodiment, an authentication server 78 (a network computing device or network server) provides one or more of the access control functions in coordination with a gateway server 40. For example, the authentication server 78 provides RADIUS (Remote Authentication Dial-in Service), LDAP (Lightweight Directory Access Protocol), and/or Diameter (authentication) protocol services. In a further example, the authentication server 78 can also provide network address services, such as IP (Internet Protocol) addresses and DHCP (Dynamic Host Configuration Protocol) services. In another embodiment, some or all of these services can be provided by one or more of the gateway servers 40-1, 40-2.

Fig. 2 is a block diagram of one example of the physical connections 29, 48, 54 for the homogenous network environment 20 of Fig. 1.

Fig. 2 shows a managed network 28-3 which is one example of the managed network 28-1 of Fig. 1. The managed network 28-3 includes access points 24-1, 24-2, 24-3, connected by managed network connections 29-3, 29-1, 29-4 to the gateway

server 40-1. The managed network 28-3 includes wireless connections 48 to mobile devices 26-1 and 26-2.

The managed network 28-4 shown in Fig. 2 is one example of the managed network 28-2 of Fig. 1. The managed network 28-4 includes access points 24-4, 24-5 and 24-6, connected by managed network connections 29-5, 29-2, 29-6 to the gateway server 40-2. The managed network 28-4 also includes wireless connections 48 to mobile devices 26-1 and 26-2 which are transferred from managed network 28-3 to the managed network 28-4 in one example of the mobile device transfer or tunnel shift 30 shown in Fig. 1. One tunnel shift 30 moves the tunnel connection 34-1 by shifting tunnel connection 34-1A to 34-1B for mobile device 26-1. Another tunnel shift 30 moves the tunnel connection 34-2 by shifting tunnel connection 34-2A to 34-2B for mobile device 26-1.

The gateway server 40-1 is connected to the gateway server 40-2 by a gateway intercommunications line 54. The gateway intercommunications line 54 is a wireless or hard wired connection between the gateway servers 40-1 and 40-2. The gateway intercommunications line 54, in one embodiment, is a hard wired cable or dedicated line connecting the gateway server 40-1 to the gateway server 40-2. In another embodiment, the intercommunications line 54 is provided through an Ethernet LAN that provides communications among gateway servers 40 in a gateway system 22. The gateway system 22 may include more than two gateway servers 40 and is not restricted by the present invention in the number of gateway servers 40, that may be included in a gateway system 22. In another embodiment, the intercommunications line 54 is provided by connections through a network such as the connections 44-1 and 44-2 through the protected network 36 shown in Fig. 1. In one embodiment, the intercommunications line 54 serves as the physical link (hard wired or wireless) between the gateway server 40-1 and 40-2 that provides the underlying physical link or physical communications for the virtual nested tunnel 42 (e.g., 42-1 or 42-2). Thus, the virtual nested tunnel 42 serves as an abstraction layer or virtual layer of communications between the gateway server 40-1 and gateway server 40-2, while the intercommunications line 54 serves as the lower level or physical connection between the gateway servers 40-1 and 40-2. In another

embodiment, the virtual nested tunnel 42 is a virtual connection between the gateway servers 40-1 and 40-2 based on communications over a network, for example, over an IP network using an Internet tunneling protocol such as GRE.

The access point 24 (e.g., 24-1 through 24-6) is a network communication device capable of handling the wireless connections 48 from mobile devices 26-1 and 26-2 based on a wireless technology. The access points 24 (e.g., 24-1 through 24-6) act as a receiving points or connecting points to establish the wireless connections 48 with the mobile devices 26-1 and 26-2.

The gateway server 40-1 includes a digital processor 50-1 and the gateway server 40-2 includes a digital processor 50-2. The digital processor 50 (e.g., 50-1 and 50-2) is a digital processing chip or device such as a microprocessor, suitable for use in a digital processing system or computer. Each digital processor, 50-1 or 50-2, hosts and executes a preferred embodiment of a gateway application 52-1 or 52-2 that manages the communications with mobile devices 26-1 and 26-2 through managed networks 28-3 and 28-4. Each gateway application 52-1 or 52-2 serves as a gateway between the mobile device 26-1 or 26-2 and other resources such as a protected network 36 or general access network 38, that the mobile device 26-1 or 26-2 is trying to access. Each gateway application 52-1 and 52-2 provides access control (e.g., authentication and authorization) for the mobile devices 26-1 and 26-2 that are communicating through the gateway system 22. When the gateway server 40 is referred to herein as performing some function, this means that the digital processor 50-1, 50-2 of the gateway server 40-1, 40-2 is performing that function based on the instructions of the gateway application 52-1, 52-2 that is hosted and executing on the digital processor 50-1, 50-2.

The gateway server 40 also includes a communications interface (e.g., 55-1, 55-2) that includes hardware and software that provides communications over network or other connections (wireless or hard wired) (e.g., intercommunications line 54, network connection 29, or network connection 44) to other entities (e.g., mobile devices 26, gateway servers 40, or one or more authentication servers 78).

In one embodiment, a computer program product 180, including a computer readable or usable medium (e.g., one or more CDROMs, diskettes, tapes, etc.),

provides software instructions for the gateway application 52 (e.g., 52-1 and 52-2 in Fig. 2, and 52-3 and 52-4 in Fig. 14). The computer program product 180 may be installed by any suitable software installation procedure, as is well known in the art. In another embodiment, the software instructions may also be downloaded over a wireless connection. A computer program propagated signal product 182 embodied on a propagated signal on a propagation medium (e.g., a radio wave, an infrared wave, a laser wave, a sound wave, or an electrical wave propagated over the Internet or other network) provides software instructions for the gateway application 52. In alternate embodiments, the propagated signal is an analog carrier wave or digital signal carried on the propagated medium. For example, the propagated signal may be a digitized signal propagated over the Internet or other network. In one embodiment, the propagated signal is a signal that is transmitted over the propagation medium over a period of time, such as the instructions for a software application sent in packets over a network over a period of milliseconds, seconds, minutes, or longer. In another embodiment, the computer readable medium of the computer program product 180 is a propagation medium that the computer may receive and read, such as by receiving the propagation medium and identifying a propagated signal embodied in the propagation medium, as described above for the computer program propagated signal product 182.

Fig. 3 is a flow chart of a procedure 200 for transferring a secure connection (e.g., 34-1) for a mobile device 26 from one access point 24 to another access point 24. In step 202, an initial gateway server 40 establishes a secure connection from a mobile device 26 through an initial access point 24 to the initial gateway server 40. For example, the mobile device 26-1 (Fig. 2) and the gateway server 40-1 establish a tunnel connection 34-1A that connects the mobile device 26-1 through an initial access point 24-2 to the gateway server 40-1, thus establishing a secure connection based on the tunnel connection 34-1A.

In step 204, the initial gateway server 40 determines that a triggering event has occurred and initiates a transfer of the mobile device 26 from the initial access point 24 to a target access point 24 associated with the target gateway server 40.

In one embodiment, gateway application 52 of gateway server 40 detects a

triggering event that initiates a transfer of the mobile device 26 from the initial gateway server 40 to another (target) gateway server 40. This transfer is indicated by a tunnel shift 30 as in Fig. 1. Such a triggering event can be the moving of the mobile device 26 (e.g., when the user moves the mobile device 26 from one location to another), or receiving a request from a mobile device 26 or gateway server 40 to move the mobile device 26. For example, the gateway server 40-1 (or an access point 24) initiates the transfer of the mobile device 26-1 from the initial access point 24-2 (Fig. 2) in managed network 28-3 to the access point 24-5 in managed network 28-4.

For example, the triggering event occurs when the mobile device 26-1 is moved by the user from one location to another so that the mobile device 26-1 is moving out of range of the managed network 28-3 of the gateway server 40-1 and into range of the managed network 28-4 of the gateway server 40-2. The triggering event can also be indicated by congestion or the need for load balancing for the managed network 28-3. For example, the managed network 28-3 may become congested in comparison to transferring the tunnel connection 34-1A to tunnel connection 34-1B (e.g., so that the mobile device 26-1 can be moved to another managed network 28-3 to obtain a higher level of service, such as more bandwidth). The triggering or initiating event can also be receiving an indication of the quality of service level assigned to the user of the mobile device 26-1 (e.g., moving the mobile device 26-1 to a new managed network 28-4 to fulfill a predefined service level for the user of the mobile device 26-1). Furthermore, the triggering event can also be an indication of a poor or declining quality of the connection 48 (e.g., radio link) between a mobile device 26-1 and an access point 24-2 (e.g., resulting in a transfer of the mobile device 26-1 from one access point 24-2 to another access point 24-5, as shown in Fig. 2, that provides an improved quality of service for the mobile device 26-1 over the connection 48 from mobile device 26-1 to gateway server 40-2).

A triggering event is indicated, in one example, by a weakening reception of the wireless signal from the mobile device 26-1 as indicated by increased packet loss on the link 48 to that particular mobile device 26-1, and/or by another indication of weakening reception, such as RSSI (Received Signal Strength Indication).

In step 206, the initial gateway server 40 provides connection information 62 to the target gateway server 40 about the secure connection that was established in step 202. The initial gateway server 40 may provide this connection information 62 or registry connection information 62 with the gateway server 40 prior to or after step 204. For example, in the gateway system 22 the gateway servers 40-1, 40-2 may register connection information 62 with each other about the mobile devices 26-1, 26-2 that they are aware of and that are connected to through managed networks 28-3, 28-4, without waiting for a triggering effect to occur. The initial gateway server 40-1 may provide connection information 62 related to the mobile device 26-1 such as the network address 30, and may or may not provide security information such as encryption information that may be required to decrypt communications from the mobile device 26-1 that are sent to the gateway server 40-1 over the tunnel connection 34-1A.

In step 208, the target gateway server 40 receives the connection information 62 at the target gateway server 40 to maintain the secure connection (e.g., 34-1) from the mobile device through the target access point 24 and through the target gateway server 40 back to the initial gateway server 40. As shown in Fig. 2, the connection 34-1 is maintained through a tunnel connection 34-1B from a mobile device 26-1 to the target gateway server 40-2 and through the nested tunnel connection 42-1 to the initial gateway server 40-1. Through these connections 34-1B and 42-1, the mobile device 26-1 may communicate in a secure manner with the initial gateway server 40-1 and in a manner that is transparent to the mobile device 26-1. In one embodiment, each transferred tunnel 34-1B and 34-2B has its own nested tunnel connection 42-1 and 42-2, respectively, from target gateway server 40-2 to initial gateway server 40-1.

In a traditional transfer of a mobile device 26 between different subnets, typically, a new secure connection (e.g., WEP or Wireless Equivalent Protocol session) is established. The problem of maintaining the WEP sessions when mobile devices 26 move between access points 24 on different subnets (e.g., managed networks 28) is solved in the present invention by moving the encryption and decryption from the access point 24 to the gateway server 40. Hence a mobile device

26 moving between access points 24 controlled by one gateway server 40 does not require any change in the connection. When a mobile device 26 moves from the coverage area of one gateway server 40 to another, then the encrypted traffic is naturally routed back to the original gateway server 40 for decryption through a tunnel connection 34 and nested tunnel 42, hence there is no break in the encryption path.

Using the approach of the present invention, as described in Fig. 3, portability is enhanced since hand-offs of mobile devices 26 can be done within any address space. Roaming complexity is reduced from roaming between access points 24 to roaming between gateway servers 40. Routing is simplified, since the address of a mobile client (mobile device 26) remains fixed once it joins the network environment 20. Since the backbone (e.g., gateway system 22) can be wired, there can be significant physical separation between servers 40. For this reason, the architecture of the present invention can be scaled to provide geographically dispersed entities with the look and feel of a local area network. Furthermore, access points 24 can be dumb and therefore inexpensive; they are essentially reduced to transparent wireless-to-Ethernet bridges. In one embodiment, this creates the opportunity for cost-effective picocell network architectures. The wireless environment is managed as a single network entity through one gateway system 22 that manages multiple managed networks 28.

Fig. 4 is a block diagram of an example of a portion of the homogenous networked environment 20 of Fig. 1 with sample network addresses 30 (e.g., IP addresses). In addition to what is shown in Fig. 1, in Fig. 4 the gateway server 40-1 has an assigned network address 30-1 with a value of 10.0.1.1, and the gateway server 40-2 has an assigned network address 30-5 with a value of 10.0.2.1. The managed network 28-1 has an assigned network address of 10.0.1.N, and the managed network 28-2 has an assigned network address of 10.0.2.N. The mobile device 26 has an assigned network address 30-3 with a value of 10.0.1.2.

In a conventional approach using a traditional wireless technology, the transfer of the mobile device 26-1 indicated by the tunnel shift 30 is likely to fail because the mobile device 26-1 has a network address, 10.0.1.2, indicating a subnet

value ("1" in the third position in the address) that is not compatible with the subnet value ("2" in the third position) of the network address, 10.0.2.N, of the managed network 28-2 being transferred to. In a traditional approach, the mobile device 26-1 is typically required to change its network address 30-3 in order to attach to the new managed network 28-2. However, because the mobile device 26-1 has a new network address 30 in the traditional approach, then the existing tunnel connection 34-1A would be broken down and the mobile device 26-1 would be required to establish a new connection 34 with the gateway server 40-2 (including new security information).

With the tunneling approach of the present invention, the mobile device 26-1 transfers to the managed network 28-2 while maintaining the same tunnel connection 34-1B (and can maintain existing security information that is transferred in the connection information 62), because the gateway server 40-2 and gateway server 40-1 establish a nested tunnel connection 42-1 that extends the tunnel connection 34-1B back to the initial gateway server 40-1 (see Fig. 4).

Fig. 5 is a block diagram of a virtual network interface 56 in a gateway server 40-2 in the gateway system 22 of Fig. 4. The virtual network interface 56 has a network address 30-6 with the same value as the network address 30-1 of the gateway server 40-1. The virtual network interface 56 is part of the gateway application 52-2 of the gateway server 40-2 and functions to provide an interface for the gateway end of the tunnel connection 34-1B (originating from the mobile device 26-1). The virtual network interface 56 is a virtual representation of the gateway server 40-1 at the gateway server 40-2 based on connection information 62 transferred from the gateway application 52-1. Thus, the virtual network interface 56 provides an interface at the gateway server 40-2 for the tunnel connection 34-1B that is identical to the interface at the gateway server 40-1 for the tunnel connection 34-1A. Thus, when the tunnel shift 30 occurs for mobile device 26-1, the mobile device 26-1 is able to maintain the same tunnel connection 34-1 that connected to gateway server 40-1 as tunnel connection 34-1A that now connects as tunnel connection 34-1B to the virtual network interface 56 of gateway server 40-2. The mobile device 26-1 communicates with tunnel connection 34-1B after the tunnel shift 30 in a similar

manner as communications using the tunnel connection 34-1A before the tunnel shift 30, without any breaking down or interruption of the tunnel connection 34-1. That is, during the tunnel shift 30, there is no significant interruption of packet communications through tunnel 34-1B and nested tunnel 42-1 between the gateway server 40-1 and the mobile device 26-1. In other words, any interruption of packet communications that do occur during the tunnel shift 30 is within the parameters of the communications protocol for an acceptable delay or interruption in the transmission of packets (between the mobile device 26-1 and the gateway server 40-1) that does not require a breaking down and re-establishment of the tunnel connection 34-1.

The virtual network interface 56 receives communications from the mobile device 26-1 through the tunnel connection 34-1B and sends the communications through the nested tunnel 42-1 to the gateway application 52-1 of the gateway server 40-1. The virtual network interface 56 also handles communications from the gateway application 52-1 of the gateway server 40-1 intended for the mobile device 26-1. The virtual network interface 56 receives these communications through the nested tunnel 42-1 and transfers them through the tunnel connection 34-1B to the mobile device 26-1. The mobile device 26-1 thus receives the communications from the gateway server 40-1 in a transparent manner over the tunnel connection 34-1B, as though the mobile device 26-1 was receiving the communications over the tunnel connection 34-1A.

Fig. 6 is a block diagram of a gateway system 22, multiple gateway servers, 40-3, 40-4, 40-5, 40-6 and multiple mobile devices 26-3, 26-4, 26-5, 26-6, configured according to the present invention. Mobile device 26-3 has a tunnel connection 34-3A to initial gateway server 40-3, and the mobile device 26-3 transfers to target gateway server 40-4 using a tunnel shift 30 from tunnel connection 34-3A to a new tunnel connection 34-3B from mobile device 26-3 to target gateway server 40-4, with communications back to the initial gateway server 40-3 through the nested tunnel 42-3. Mobile device 26-4 has a tunnel connection 34-4A to initial gateway server 40-3, and mobile device 26-4 transfers to target gateway server 40-5 using a tunnel shift 30 to a new tunnel connection 34-4B from mobile device 26-4 to target

gateway server 40-5, with communications back to the initial gateway server 40-3 through the nested tunnel 42-4. Mobile device 26-5 has a tunnel connection 34-5A to initial gateway server 40-6, and mobile device 26-5 transfers to target gateway server 40-5 using a tunnel shift 30 to tunnel connection 34-5B from mobile device 26-5 to target gateway server 40-5, with communications back to the initial gateway server 40-6 through the nested tunnel 42-5.

The gateway servers 40-3, 40-4, 40-5, 40-6 communicate connection information 62 about the connections to mobile devices 26-3, 26-4, 26-5 for each gateway server 40-3, 40-4, 40-5, 40-6. In one embodiment, the gateway servers 40-3, 40-4, 40-5, 40-6 communication connection information 62 about a mobile device 26-3, 26-4, 26-5 as the result of a triggering event that indicates that a mobile device 26-3, 26-4, or 26-5 is transferring to another gateway server 40-3, 40-4, 40-5, or 40-6. For example, mobile device 26-3 is moving out of range of gateway server 40-3 (i.e., out of range of any access points 24 connected to gateway server 40-3 in a managed network 28). Thus the gateway server 40-3 sends connection information 62 about the tunnel connection 34-3A to gateway server 40-4 (if the gateway server 40-3 knows that the transfer is to gateway server 40-4) or distributes (e.g., broadcasts) the connection information 62 throughout the gateway system 22 to all of the other gateway servers 40-4, 40-5, and 40-6. In another embodiment, each gateway server 40-3, 40-4, 40-5, or 40-6 distributes (registers) the connection information 62 to the other gateway servers 40-3, 40-4, 40-5, 40-6 whenever a mobile device 26-3, 26-4, or 26-5 connects to one of the gateway servers 40-3, 40-4, 40-5, or 40-6. For example, if mobile device 26-5 establishes a tunnel connection 34-5A with gateway server 40-6, then that gateway server 40-6 distributes connection information 62 about the tunnel connection 34-5A and the mobile device 26-5 to the other gateway servers 40-4, 40-5, and 40-3 to register the mobile device 26-5 with those gateway servers 40-4, 40-5, and 40-3.

In another embodiment, one gateway server 40 serves as a registry of connection information 62 for each mobile device 26 that is connected to or associated with the gateway system 22. In a further embodiment, connection information 62 is stored in a data server or registry server available to, but outside of,

the gateway system 22.

In one embodiment, the gateway servers 40 in Fig. 6 are connected by a backbone (e.g., connections such as gateway intercommunications line 54) that could be wireless or wireline (hard wired). In one embodiment, the backbone is based on a hard wired LAN, such as an Ethernet, connecting the gateway servers 40 (e.g., 40-3, 40-4, 40-5, and 40-6). Fig. 6 shows four gateway servers 40, but the number that could be accommodated in a gateway system 22 that is much larger than this, limited in general by the address structure of the enterprise. Each gateway server 40 has its own pool of addresses 30 with values such as: 10.0.1.0, 10.0.2.0, etc. Once an address 30 is assigned to a mobile device 26, the address 30 stays with the mobile device 26 as it moves from one access point 24 to another access point 24 managed in managed networks 28 by the gateway system 22. The maximum number of available network addresses 30 can be accommodated in this way.

The present invention does not require the mobile device 26 to transfer to any particular gateway server 40, and, generally, the mobile device 26 can transfer from one gateway server 40 to another gateway server 40 while maintaining a connection 42 back to the same initial gateway server 40. For example, the mobile device 26-3 could transfer to one target gateway server 40 (e.g., 40-4) and then to another target server 40 (e.g., 40-5, or 40-6) and still maintain a connection 42 to the initial gateway server 40-3.

Figs. 7 through 13 illustrate an example of stages in the IP address assignment process for a mobile device 26-12 transferring between homogenous WLAN networks for a preferred embodiment of the invention.

Fig. 7 is a schematic diagram illustrating an initial IP assignment for mobile device 26-12 in a homogenous network environment 20 according to the present invention. The mobile device 26-12 associates with the access point 24-11 that has an IP address 100b with a value of 10.0.30.128. The IP address 100b is one example of a network address 30. Before the user authentication is completed (see Fig. 8) mobile device 26-12 makes an IP address (DHCP) request 102 for an IP address 100 to the gateway server 40-7 in order to receive the initial IP address assignment 100 for the mobile device 26-12.

The IP address request 102 is answered by the gateway server 40-7 in one of two approaches. The first approach is an answer from the gateway server 40-7 itself (through internal DHCP functionality within the gateway server 40-7) with an IP address 100 for the mobile device 26-12 and an IP address 100c for a gateway (e.g., gateway server 40-7 or some other gateway server 40, if one is available) appropriate to that sub-net. The second approach is an answer from a MAC address driven IP server 94-1 (e.g., DHCP server) that issues and returns an IP address 100a (e.g., 10.0.30.15) for use by the mobile device 26-12.

In both cases the DHCP "time to live" for the IP address is set very short so that, if necessary, this address 100a (e.g., 10.0.30.15) for the mobile device 26-12 can be changed immediately after the user authentication (see Fig. 8).

Fig. 8 is a schematic diagram illustrating an authentication request 104 for the mobile device 26-12 in the homogenous network environment 20 of Fig. 7. The gateway server 40-7 redirects all HTTP (Hypertext Transfer Protocol) requests so the user is presented with a secure web page (e.g., displayed by the mobile device 26-12) through which the user enters a name and password. The gateway server 40-7 then authenticates the user against an authentication server 78 (e.g., RADIUS/LDAP server). The authentication server 78 then returns "role" (e.g., user's role in an organization) and "domain" (e.g., network system 72, see Fig. 14).

The role indicates the role of the user of the mobile device 26-12, for example, "Executive" for a user who is a manager or an executive in an organization, "Admin" for a worker with an administrative function, "Visitor" for someone visiting the organization or site. Depending on the user's role, each user (or a group of users) has a different level of access to (or different set of privileges for) resources that are available to the mobile device 26-12, such as through the protected network 36.

The domain tells the gateway server 40-7 which network grouping (e.g., network system 72, see Fig. 14) the mobile device 26-12 "belongs to". So, for example, if the user is in fact an employee from the United Kingdom visiting the United States office of an company or organization, then it may be most appropriate to give the user an IP address 100 from the range (of IP addresses) reserved for the

U.K., even though the user is actually connected to a U.S. subnet.

In order to switch IP addresses 100 (if required) after the authentication process, the gateway server 40-7 waits until the mobile device 26-12 asks to renew its DHCP lease. The gateway server 40-7 then obtains a new IP address 100 that has a much longer time to live and replies to the mobile device 26-12 with the new IP address 100.

Fig. 9 is a schematic diagram illustrating a third-party IP address request 106 for the mobile device 26-12 in the homogenous network environment 20 of Fig. 7. In some cases, the gateway server 40-7 may also interconnect with third party public or semi-public access providers (e.g., WISP or Wireless Internet Service Providers). The gateway server 40-7 (as well as authenticating users against a third party authentication server 78) may also obtain the IP address 100 from the third party remote IP address (e.g., DHCP) server 96 as well.

As described above, the domain (e.g., network system 72) received from the authentication server 78 tells the gateway server 40-7 which network group the mobile device 26-12 "belongs to". So, for example, if the user is a customer of a GPRS cellular operator who is temporarily using a WISP, then the domain would be the network system 72 (see Fig. 14) of the cellular operator. In such a case the user needs an IP address 100 from the cellular operator's address space. In this case, the domain represents, for example, a network system 72 -1 that provides an access identifier 84 (e.g., IP address) for use when accessing a wireless network 92 associated with the network system 72-1 (see Fig. 14).

Fig. 10 is a schematic diagram illustrating an ARP (address resolution protocol) request 108-1 for a mobile device 26-12 in a homogenous network environment 20 according to the present invention. The network environment 20 includes gateway servers 40-7, 40-8, 40-9, access points 24-12, 24-13, mobile device 26-12, protected network 36 (alternatively network 38), token driven IP address server 94-2 (e.g., DHCP server), and authentication server 78.

After receiving the IP address 100a (as described for Fig. 7 through Fig. 9), suppose that the mobile device 26-12 associates with access point 24-12 (or is assigned access point 24-12 by the home gateway server 40-7 for the mobile device

26-12). The mobile device 26-12 thus communicates with gateway server 40-8 rather than directly to the home gateway server 40-7. (The mobile device 26-12 can still communicate through this server 40-8 to the home gateway server 40-7.) In one embodiment, the gateway server 40-8 uses a virtual network interface 56 (see Fig. 5) that uses the network address 100c (10.0.30.1) of the home gateway server 40-7 to enable the mobile device 26-12 to associate with the access point 24-12 and the gateway server 40-8.

Suppose that the mobile device 26-12 leaves the coverage area of the gateway server 40-8 (and the home gateway server 40-7). Thus, the mobile device 26-12 moves from the coverage area of access point 24-12 to the coverage area of the access point 24-13, which is associated with the gateway server 40-9.

The mobile device 26-12 tries to associate with access point 24-13. The mobile device 26-12 sends data packets to the MAC address of the gateway server 40-8 that the mobile device 26-12 has been previously using. There is no reply from the gateway server 40-8, so the mobile device 26-12 makes an ARP broadcast request 108-1 with the IP address 100f having a value of 10.0.10.1 (which is the address of the gateway server 40-8 that it was using previously).

The gateway server 40-9 on the local subnet responds to the ARP request 108-1 with the MAC address of the gateway server 40-9, so the gateway server 40-9 becomes the gateway for the mobile device 26-12. In one embodiment, the gateway server 40-9 uses a virtual network interface 56 (see Fig. 5) that uses the network address 100c (10.0.30.1) of the home gateway server 40-7 to enable the mobile device 26-12 to associate with the access point 24-13 and the gateway server 40-9.

Fig. 11 is a schematic diagram illustrating a location update message 110 for the mobile device 26-12 in the homogenous network environment 20 of Fig. 10. Each time the gateway server 40-9 receives either an ARP request 108-1 or a packet from a new mobile device 26, then the gateway server 40-9 sends the location update message 110 to the authentication server 78 server to inform the authentication server 78 of the new location of the mobile device 26-12. The authentication server 78 server then returns the IP address 100c (e.g., 10.0.30.1) of the home gateway server 40-7 for the mobile device 26-12.

Fig. 12 is a schematic diagram illustrating an information message 112 for the mobile device 26-12 in the homogenous network environment 20 of Fig. 10. The information message 112 invalidates the previous route (e.g., communication route or tunnel from the mobile device 26-12 to the gateway server 40-8 that the mobile device 26-12 was previously attached to). The authentication server 78 sends the information message 112 to the gateway server 40-8 informing the gateway server 40-8 of the move of the mobile device 26-12 to its current association with gateway server 40-9.

Fig. 13 is a schematic diagram illustrating a nested tunnel 42-10 for the mobile device 26-12 in the homogenous network environment 20 of Fig. 10. The gateway server 40-9 receives the IP address 100c of the home gateway server 40-7 for the mobile device 26-12 and sets up a nested tunnel 42-10 back to the home gateway server 40-7. The home gateway server 40-7 now knows (due to the update message 110, Fig. 11) the network location of the mobile device 26-12 and so can forward packets for the mobile device 26-12 received through the protected network 36 to the mobile device 26-12 through the gateway server 40-9.

Fig. 14 is a block diagram of a heterogenous network environment 70 illustrating a device transfer 88 between two heterogenous network systems 72-1, 72-2, according to the present invention. The heterogenous network environment 70 further includes an authentication server 78, an intermediary network 74, wireless networks 90, 92, and a mobile device 26-16.

The network system 72 (e.g., 72-1, 72-2) is a system of networked devices (e.g., mobile telephones, PDA's, laptop computers, personal computers, server computers, access points, routers, bridges, and/or gateways) in communication with each other using a communications protocol. Beyond the wireless communications protocol used for communicating with one or more mobile devices 26, each network system 72 generally may include one or more networking protocols, networking standards, and/or wireless technologies that provide communications within the network system 72. When used to associate mobile devices 26 with a network system 72-1, 72-2, the wireless communications protocols are heterogenous because the protocol is the same within each network system 72-1 or 72-2, but different

(heterogenous) relative to or across the other network system 72-1 or 72-2. For example, a network system 72-1 is a WLAN that includes mobile devices 26, access points 24, and gateway servers 40. The network system 72-1 is based on a Bluetooth, IEEE 802.11 wireless technology, or other wireless communication technology suitable for communicating with the mobile device 26-16. However, in addition, the network system 72-1 can also use a hard-wired LAN (e.g., cable based Ethernet) for communications between the access points 24 and the network gateway 76-1. In a particular example, a network system 72 for a WLAN is based on the gateway system 22 of Fig. 1. In another example, a network system 72 is a mobile telephone system, such as a cellular phone system that uses mobile telephone protocols to communicate with mobile devices 26.

Each network system 72 includes a network gateway 76 (e.g., 76-1, 76-2). The network gateway 76 (e.g., 76-1 and 76-2) is any suitable computing device or digital processing device that may serve as a gateway to the network system 72 in the heterogenous networked environment 70. Such a network gateway 76 can be a server, a router, a bridge, a switch or other network communications or computing device. In one embodiment, the network gateway 76-1 includes a digital processor 50-3, and the network gateway 76-2 includes a digital processor 50-4. Each digital processor, 50-3 or 50-4, hosts and executes a preferred embodiment of a gateway application 52-3 or 52-4 that serves as a gateway for each network system 72-1, 72-2. For example, the gateway application 52-3 provides access control (e.g., authentication and authorization) for the mobile device 26-16 communicating through the wireless network 90 to the network system 72-1. When the network gateway 76-1 or 76-2 is referred to herein as performing some function, this means that the digital processor 50-3 or 50-4 of each network gateway 76-1 or 76-2 is performing that function based on the instructions of each gateway application 52-3 or 52-4 that is hosted and executing on each digital processor 50-3 or 50-4.

Each network gateway 76 (e.g., 76-1, 76-2) also includes a communications interface 55 (e.g., 55-3, 55-4) that includes hardware and software that provides communications over network or other connections (wireless or hard wired) (e.g., wireless networks 90, 92, or intermediary network 74) to other entities (e.g., mobile

devices 26, one or more authentication servers 78, or network systems 72).

One example of a network gateway 76 is the gateway server 40 (e.g., 40-1, 40-2) shown in Fig. 1. In another example, the network gateway 76 is the gateway system 22 (including both servers 40-1, 40-2) of Fig. 1. That is, in the gateway system 22, the functions of the network gateway 76 are performed by two or more servers 40.

In one embodiment, an authentication server 78 (a network computing device or network server) provides one or more of the access control functions in coordination with the network gateway 76 (e.g., 76-1, 76-2), in a similar manner to what was described previously for the authentication server 78 for Fig. 1. For example, the authentication server 78 can also provide network address services, such as IP addresses and DHCP services. In another embodiment, some or all of these services can be provided by the network gateway 76 (e.g., 76-1, 76-2), or through the coordinated functioning of the network gateway 76 (e.g., 76-1, 76-2) and the authentication server 78.

An intermediary network 74 connects the authentication server 78, network system 72-1, and network system 72-2. In one embodiment, the intermediary network 74 is a packet-based network, such as one based on the TCP/IP protocols. In other embodiments, the intermediary network 74 is a WAN (wide area network) link, satellite connection or network, frame relay connection, PSTN (public switched telephone network), or virtual circuits (virtual connections or pathways that may rely on various underlying lower level physical or media connections). The intermediary network 74 provides the connections and handshakes between the network systems 76-1 and 76-2 so that the mobile device 26-16 can perform a device transfer 88 to seamlessly transfer from one network system 76-1 to another 76-2. The protected network 36 and general access network 38 (of Fig. 1) are examples of intermediary networks 74, if, for example, these networks 36, 38 provide a connection from the gateway system 22 of Fig. 1 (which serves as a network system 72) to another network system 72 through one or both of the networks 36, 38.

A wireless network 90 provides communications for the network system 72-1 to the mobile device 26-16, when the mobile device 26-16 is associated with the

network system 72-1 (i.e., before the device transfer 88 of the mobile device 26-16 to the network system 72-2). A wireless network 92 provides communications for the network system 72-2 to the mobile device 26-16, when the mobile device 26-16 is associated with the network system 72-2 (i.e., after the device transfer 88). The wireless networks 90, 92 are based on any suitable wireless communications protocols, such as WLAN wireless technologies (e.g., Bluetooth, or IEEE 802.11) or mobile telephone communication technologies (e.g., CMTS, GSM, PCS, or UMTS). The wireless networks 90 and 92 are heterogenous; that is, that do not use the same communications protocol or standard, and do not typically allow (or readily allow) for the transfer of mobile devices between the wireless networks 90, 92. For example, wireless network 90 is a Bluetooth WLAN and wireless network 92 is a UMTS system, or vice versa.

The mobile device 26-16 includes communications interfaces (e.g., communications hardware and software) that allow the mobile device 26-16 to communicate with two (or more) heterogenous wireless networks 90, 92. Thus, the mobile device 26-16 is capable of transferring (or moving) from one heterogenous wireless network 90 to another heterogenous wireless network 92. However, in a traditional approach, the mobile device 26-16 must establish a new connection and new communication session when moving between wireless networks 90,92.

The wireless connection 83 provides an association for the mobile device 26-16 with the network systems 72-1 or 72-2 through a connection that is suitable 83 (e.g., 83-1 or 83-2) for the wireless communications protocol supported by the respective network system 72-1 or 72-2.

The request 80 is a signal, message, network packet, or other communication from one (initial) network system (e.g., 72-1) to the other (target) network system (e.g., 72-2) that requests an access identifier 84 to be provided to the mobile device 26-16 that the mobile device 26-16 uses when first accessing the other network system (e.g., 72-2) during the device transfer 88. The request 80 indicates that the mobile device 26-16 is transferring (or likely to transfer) to the target network system 72–2. In one embodiment, the request 80 includes information about the mobile device 26-16 (e.g., device identification or address), the user of the mobile device 26-

16 (e.g., user identification), a home network gateway (e.g., 76-1), a home network system (e.g., 72-1), authentication information (e.g., address of authentication server 78 to use for the mobile device 26-16 or its user), and/or any other information that may be useful to the target network gateway 76-2 in identifying and authenticating the mobile device 26-16

The response 82 is a signal, message, network packet, or other communication from one network system (e.g., 72-2) to the other (e.g., 72-1) that provides the access identifier 84. The access identifier 84 is a unique identifier (e.g., network address, IP address, MAC address, cookie, digital certificate, or other identifier) that identifies the mobile device 26-16 to the target network system (e.g., 72-2).

The present invention does not require that all of the request messages 80 and response messages 82 be completed, if not required. For example, if one network gateway 76-1 does not use the authentication server 78 for access control and network address services, but uses the other network gateway 76-2 for these services, the present invention does not require that the request 80 also be made to the authentication server 78 and that a response 82 be returned from the authentication server 78. In another example, if the network gateway 76-1 does use the authentication server 78 for access control and network address services, and does not use the other network gateway 76-2 for these services, the present invention does not require that the request 80 also be made to the network gateway 76-2 and that a response 82 be returned from the network gateway 76-2.

The internetwork tunnel 86 is a tunnel connection between the network gateway 76-2 and the network gateway 76-1 formed after the device transfer 88 so that the mobile device 26-16 continues to communicate in a seamless manner with the network gateway 76-1 that the mobile device 26-16 was communicating with before the device transfer 88. The internetwork tunnel 86 is a virtual connection that may be based on a direct physical connection (e.g., cable) between the network systems 72-1, 72-2, or based on a communications through the intermediary network 74.

Fig. 15 is a flow chart of a procedure 300 for providing an access identifier 84

to a mobile device 26-16 to enable the device transfer 88 of Fig. 14 from an initial wireless network 90 to a target wireless network 92.

In step 302, the network gateway 76-1 detects a triggering event that indicates that a mobile device 26-16 will be transferring (or should transfer) from the initial wireless network 90 to the target wireless network 92. In one example, the triggering event is the movement of the mobile device 26-16 (as the user moves the device 26-16) out of range of the initial wireless network 90 and into range of the target wireless network 92 or some other triggering event as described previously for Fig. 3. For example, the mobile device 26-16 is a PDA with voice communication capabilities, and the user of the PDA 26-16 is moving the device 26-16 from a WLAN (e.g., 90) to a mobile telecommunications network (e.g., 92). The gateway server 76-1 can determine from a decreasing signal strength from the PDA 26-16 that the mobile device 26-16 is moving out of range of the WLAN (e.g., 90), and also determine that the mobile device 26-16 is likely to transfer to the target wireless network 92 (e.g., from a signal from the mobile device 26-16 indicating that it has detected that it is moving within range of the target wireless network 92).

Alternatively, the triggering event occurs when the mobile device 26-16 registers with the network gateway 76-1, and the network gateway 76-1 determines that the mobile device 26-16 is also capable of accessing another network system 72-2 (e.g., when the network gateway 76-1 receives this information from the authentication server 78). Then, the network gateway 76-1 anticipates that the mobile device 26-16 may try to access the other network system 72-2, and this anticipation by the network gateway 76-1 serves as the triggering event to trigger the request 80 (see step 304).

In step 304, the gateway application 52-3 of the network gateway 76-1 receives the request 80 through the communication interface 55-3 and the initial wireless network 90 on behalf of the mobile device 26-16. The request 80 indicates a network system 72-2 that specifies the target wireless network 92 that the mobile device 26-16 is transferring to (or anticipates transferring to). As described for step 302, the request 80 originates, for example, from the mobile device 26-16 as it moves out of range of the initial wireless network 90 and into range of the target wireless

network 92. In another example, the request 80 originates with the network gateway 76-1 anticipating the transfer 88 of the mobile device 26-16 to another wireless network 92. The request 80 indicates another network system 72-2 that the mobile device 26-16 is transferring to. For example, the network system 72-2 is a mobile telephone network operated by a specific service provider, and the target wireless network 92 is the mobile phone network supported by this service provider.

In step 306, the gateway application 52-3 of the network gateway 76-1 obtains an access identifier 84 for the target wireless network 92 through the communications interface 55-3 and the intermediary network 74 (e.g., Internet). The network gateway 76-1 transfers the request 80 for the access identifier 84 from the network gateway 76-1 through the intermediary network 74 to the network gateway 76-2 of the target network system 72-2. For example, the network gateway 76-1 receives a request 80 from the mobile device 26-16 to transfer to the target wireless network 92 and repackages this request 80 as a request using a network protocol (e.g., IP) suitable for use over the intermediary network 74. The network gateway 72-2 (or authentication server 78) authenticates the mobile device 26-16 (and/or user of the mobile device 26-16) based on the information provided in the request 80. The network gateway 72-2 (or authentication server 78) returns a response 82 that contains the access identifier 84.

In step 308, the gateway application 52-3 of the network gateway 76-1 provides the response 82 to the mobile device 26-16 through the communications interface 55-3 and the initial wireless network 90. In one embodiment, the gateway application 52-3 stores the access identifier in a device database that includes data for mobile devices 26. For example, the device database is associated with a network gateway 76-1 (or network system 72-1 or intermediary network 74) and includes data for mobile device identification, access identifiers 84, and other data for one or more mobile devices 26 (e.g., 26-16).

In step 310, the network gateway 76-1 transfers the mobile device 26-16 from the initial wireless network 90 to the target wireless network 92, which the mobile device 26-16 accesses by using the newly received access identifier 84. Alternatively, the mobile device 26-16 transfers itself to the target wireless network

92 after it receives the access identifier 84. Thus, when the mobile device 26-16 makes the device transfer 88, the mobile device 26-16 can transfer seamlessly because the network gateway 76-2 rapidly identifies the mobile device 26-16 from the access identifier 84. The network gateway 76-2 sets up the tunnel 86 back to the home network gateway 76-1 for the mobile device 26-16 so that the mobile device 26-16 transfers seamlessly and does not experience any loss of connection or interruption in the current session (e.g. voice communication session) between the mobile device 26-16 and the home network gateway 76-1.

In one embodiment, the mobile device 26-16 stores the access identifier 84 for future use. That is, the mobile device 26-16 does not immediately perform the transfer 88 to the target wireless network 92, but keeps the access identifier 84 in anticipation of moving to another wireless network 92 at some point in the future.

Fig. 16 illustrates heterogenous network environment 70 for a WLAN gateway 76-3 (for a WLAN network system 72-3) and a mobile telephone network gateway 76-4 (for a cellular network system 72-4), according to the present invention. The network environment 70 includes a common authentication server 78 (which may also provide IP address services), intermediary network 74, gateway servers 40-10, 40-11, access points 24-17 through 24-20, and mobile devices 26-18 through 26-21. The network addresses 100 may be based on IPv4 (Internet Protocol version 4) or IPv6 (Internet Protocol version 6). In the embodiments shown in Figs. 16-21 the IP address 100 is one example of an access identifier 84. A mobile device 26 moves from the wide area cellular network system 72-4 (e.g., with network gateway 76-4) keeps its IPv4 address 100 and has its traffic tunneled back to the relevant gateway (e.g., 76-4) through an internetwork tunnel (e.g., 86) as in Fig. 14. The wireless data network gateway 76-3 acts as Foreign and Home Agent for mobile devices 26 that moves. A mobile station (e.g., mobile device) 26 registered with a cellular operator (e.g., through network gateway 76-4) can be assigned an IP address 100 by the common authentication server 78. (The mobile device 26 first receives a temporary IP address 100 from the network gateway 76-3 in order to authenticate. Then the IP address 100 is changed to that supplied by the authentication server 78 (with a very short DHCP time to live), in a manner similar to what was described for

Fig. 7 and 8. Figs 17 through 21 illustrate further details of one example of the mobile device transfer process of the present invention.

In one embodiment, the configuration shown in Fig. 16 acts as an interface between the IPv4 and IPv6 network addressing protocols. For example, the network gateway 76-3 can act as an interface between the IPv4 and IPv6.

Fig. 17 is a schematic diagram illustrating heterogenous a network environment 70 with two heterogenous network systems 72-5, 72-6 and a mobile device 26-23, according to the present invention. The WLAN network system 72-5 includes a network gateway 76-7 (e.g., Bluetooth, IEEE 802.11, or other WLAN wireless technology) and an access point 24-22. The cellular network system 72-6 (e.g., mobile telephone cellular network) includes a cellular network gateway 76-8 and cellular base station 98. In one embodiment, the cellular network gateway 76-8 is a GGSN (Gateway GPRS Support Node) Internet gateway supporting 2.5G or 3G mobile telephone communication technology (e.g., UMTS). The intermediary network 74 (e.g., Internet) provides communications to the network gateways 76-7 and 76-8. The mobile device 26-23 can connect to the access point 24-22 through a WLAN wireless connection 48 or to the cellular base station 98 through a cellular wireless connection 120 suitable for a cellular mobile telephone connection. The wireless connection 48 and 120 are examples of the wireless connection 83 of Fig. 14.

The mobile device 26-23 such as a laptop computer, can have multiple radio interfaces such as both WLAN (e.g., Bluetooth, IEEE 802.11, or other WLAN wireless technology) and mobile telephone communication technology (e.g., 2.5G or 3G). These multiple radio interfaces can either be built into a single PCMCIA (Personal Computer Memory Card International Association) card or be two separate interface units (PCMCIA card and cellular telephone interface). In the later case, an operating system, such as the Microsoft® Windows® 2000 or XP operating system hosted and executing on a microprocessor in the mobile device 26-23 (e.g., laptop computer), can dynamically select which interface to use.

WLAN to cellular roaming is the ability of the mobile device 26-23 to change its route to the Internet 74 from the WLAN network system 72-5 to the cellular

network system 72-6 or visa-versa without changing the IP address 100r of the mobile device 26-23 and hiding the change in routing or pathway to the Internet 74 from the Internet part of the connection. The second constraint is not required if an IPv6 network protocol is in use.

To avoid any changes to the network gateway 76-8, the user of the mobile device 26-23 must authenticate first with the cellular network system 72-6 before using the WLAN network system 72-5. Authenticating first with the WLAN system 72-5 is possible but requires that software (e.g., gateway application 52) hosted and executing on a processor 50 in the network gateway 76-8 be adapted appropriately.

Fig 18 is a schematic diagram illustrating a mobile device 26-24 connected to a cellular network system 72-6, according to the present invention. For example, when a mobile device 26-24 connects to an IPv4 cellular packet data network 72-6 then the mobile device 26-24 connects to the network gateway 76-8 (e.g., GGSN) via the cellular base station 98 and an SGSN (Serving GPRS Support Node). For the sake of simplicity this connection is treated herein as a connection to the network gateway 76-8 (e.g., serving the function of both SGSN & GGSN). The network gateway 76-8 authenticates the user against an authentication server 78, and provides the mobile device 26-24 with an IP address 100u. The cellular network system 72-6 connects to an authentication server 78 and a billing system 122.

Fig. 19 is a schematic diagram illustrating an ARP request 108-2 for a mobile device 26-24 in a heterogenous network environment 70, according to the present invention. When the mobile device 26-24 moves from the cellular network system 72-6 into the coverage area of a WLAN network system 72-5, then the mobile device 26-24 detects the availability of the WLAN network system 72-5 and tries to connect (e.g., associate with access point 24-22 and WLAN network gateway 76-7). Some other triggering event (as described for Fig. 3) may also initiate the transfer of the mobile device 26-24 from the cellular network system 72-6 to the WLAN network system 72-5. The mobile device 26-24 sends data-packets to the MAC address of the network gateway 76-8 that the mobile device 26-24 had been using previously. Because the mobile device 26-24 no longer has a connection 120 to the cellular base station 98 (e.g., has moved out of range), there is no reply, so the mobile device 26-

24 makes an ARP broadcast 108-2 with an IP address 100v having a value of 4.0.10.1 (which is the IP address 100v of the network gateway 76-8).

Before authenticating the mobile device 26-24, the network gateway 76-7 on the local subnet of the WLAN network system 72-5 responds to the ARP request 108-2 with the MAC address of the network gateway 76-7, so that the network gateway 76-7 becomes the gateway for the mobile device 26-24. The mobile device 26-24 still must be authenticated (see Fig. 20).

Fig. 20 is a schematic diagram illustrating an authentication query 118 for the mobile device 26-24 in the heterogenous network environment 70 of Fig. 19. After the gateway server 76-7 detects the arrival of the new mobile device 26-24, the gateway server 76-7 sends a query 118 to the authentication server 78 for the cellular network system 72-6. The authentication server 78 then confirms that the mobile device 26-24 had already been authenticated by the cellular network system 72-6, and provides the IP address 100v (e.g., 4.0.10.1) of the home network gateway 76-8 for the mobile device 26-24.

Fig. 21 is a schematic diagram illustrating an internetwork tunnel 86 for the mobile device 26-24 in the heterogenous network environment 70 of Fig. 19. After the network gateway 76-7 has obtained the IP address 100v of the home network gateway 76-8 for the mobile device 26-24, the network gateway 76-7, in one embodiment, sets up the internetwork tunnel 86 back to the network gateway 76-8 by emulating a cellular network gateway (e.g., GGSN interface) interface in the network gateway 76-7. In another embodiment, the network gateway 76-7 emulates an SGSN interface.

The current session that the mobile device 26-24 was conducting when connected to the cellular base station 98 then can continue without interruption or requiring the establishment of a new session with the network gateway 76-8. No changes are required to the cellular network gateway 76-8, because the network gateway 76-7 emulates the cellular network gateway (e.g., GGSN interface) using known tunneling protocols (e.g., inter GGSN tunneling protocols that are part of the 3G protocol).

While this invention has been particularly shown and described with

references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.

CLAIMS

What is claimed is:

1. A method for enabling a mobile device to roam among access points in a wireless local area network, the mobile device capable of communicating with the access points, the method comprising the computer-implemented steps of:

establishing a secure connection from the mobile device through an initial access point to an initial gateway server;

providing connection information to a target gateway server from the initial gateway server about the secure connection, based on a triggering event that initiates a transfer of the mobile device from the initial access point to a target access point associated with the target gateway server; and

receiving the connection information at the target gateway server to maintain the secure connection from the mobile device through the target access point back to the initial gateway server.

2. The method of Claim 1, wherein the mobile device is assigned an internet protocol address by the initial gateway server and the secure connection is based on the internet protocol address, and the step of providing the connection information includes maintaining the secure connection based on the internet protocol address assigned to the mobile device.

3. The method of Claim 1, further comprising a step of providing a nested tunnel to couple the initial gateway server and the target gateway server.

4. The method of Claim 3, wherein the step of providing the nested tunnel to couple the initial gateway server and the target gateway server is based on a hardwired connection between the initial gateway server and the target gateway server.

5. The method of Claim 1, wherein the triggering event is a movement of the mobile device out of range of the initial access point and within range of the target access point.

6. The method of Claim 1, wherein the triggering event is a determination that the target access point has a preferable level of congestion compared to a level of congestion for the initial access point.

7. The method of Claim 1, wherein the step of providing the connection information comprises extending the secure connection from the target gateway server to the initial gateway server, so that the initial gateway server decrypts secure messages originating from the mobile device.

8. The method of Claim 1, wherein the step of providing the connection information comprises establishing a virtual representation of the initial gateway server at the target gateway server.

9. A gateway system for enabling a mobile device to roam among access points in a wireless local area network, the mobile device capable of communicating with the access points, the gateway system comprising:

an initial gateway server, and

a target gateway server in communication with the initial gateway server; wherein:

the initial gateway server establishes a secure connection from the mobile device through an initial access;

the initial gateway server provides connection information to the target gateway server about the secure connection, based on a triggering event that initiates a transfer of the mobile device from the initial access point to a target access point associated with the target gateway server; and

the target gateway server receives the connection information

to maintain the secure connection from the mobile device through the target access point back to the initial gateway server.

10. The gateway system of Claim 9, wherein the mobile device is assigned an internet protocol address by the initial gateway server, the secure connection is based on the internet protocol address, and the initial gateway server maintains the connection based on the internet protocol address assigned to the mobile device.

11. The gateway system of Claim 9, wherein the initial gateway server and the target gateway server are coupled by a nested tunnel between the initial gateway server and the target gateway server.

12. The gateway system of Claim 11, wherein the nested tunnel between the initial gateway server and the target gateway server is based on a hard wired connection between the initial gateway server and the target gateway server.

13. The gateway system of Claim 9, wherein the triggering event is a movement of the mobile device out of range of the initial access point and within range of the target access point.

14. The gateway system of Claim 9, wherein the triggering event is a determination that the target access point has a preferable level of congestion compared to a level of congestion for the initial access point.

15. The gateway system of Claim 9, wherein the target gateway server extends the secure connection from the target gateway server to the initial gateway server, so that the initial gateway server decrypts secure messages originating from the mobile device.

16. The gateway system of Claim 9, wherein the target gateway server

establishes a virtual representation of the initial gateway server at the target gateway server.

17. A computer program product that includes a computer usable medium having computer program instructions stored thereon for enabling a mobile device to roam among access points in a wireless local area network, the mobile device capable of communicating with the access points, such that the computer program instructions, when performed by a digital processor, cause the digital processor to:

establish a secure connection from the mobile device through an initial access point to an initial gateway server;

provide connection information to a target gateway server from the initial gateway server about the secure connection, based on a triggering event that initiates a transfer of the mobile device from the initial access point to a target access point associated with the target gateway server; and

receive the connection information at the target gateway server to maintain the secure connection from the mobile device through the target access point back to the initial gateway server.

18. A method for enabling a mobile device to roam between a first wireless network and a second wireless network, the first wireless network substantially heterogeneous with the second wireless network, both the first wireless network and the second wireless network capable of communicating with an intermediary network, and the mobile device capable of accessing the first wireless network and the second wireless network, the method comprising the computer-implemented steps of:

receiving a request at the first wireless network to access the second wireless network, the request being on behalf of the mobile device and indicating a network system specifying the second wireless network;

through the intermediary network, obtaining an access identifier for the second wireless network, the access identifier for use by the mobile

device when accessing the second wireless network; and

providing the access identifier for the mobile device to use when accessing the second wireless network.

19. The method of Claim 18, wherein the first wireless network is a wireless local area network, the second wireless network is a cellular telecommunications network, and the mobile device is a personal digital assistant.

20. The method of Claim 18, wherein the request includes a user identification of a user of the mobile device, and the step of receiving the request includes determining an identity of the network system as a function of the user identification.

21. The method of Claim 18, wherein the step of obtaining the access identifier includes providing an authentication request based on the request to a dynamic host configuration server.

22. The method of Claim 18, wherein the access identifier is an internet protocol address and the intermediary network is the internet.

23. The method of Claim 18, wherein the step of obtaining the access identifier includes requesting the access identifier from a network gateway for the second wireless network, the network gateway providing the access identifier from a predefined range of access identifiers allocated to the second wireless network.

24. The method of Claim 18, wherein the step of providing the access identifier includes storing the access identifier in a device database that includes a device identification for the mobile device.

25. A network gateway for enabling a mobile device to roam between a first wireless network and a second wireless network, the first wireless network substantially heterogeneous with the second wireless network, both the first wireless network and the second wireless network capable of communicating with an intermediary network, and the mobile device capable of accessing the first wireless network and the second wireless network, the network gateway comprising:

a digital processor that hosts and executes a gateway application for receiving a request to access the second wireless network, the gateway application and the mobile device associated with the first wireless network, and

a communications interface coupled with the gateway application, the gateway application configuring the digital processor to:

receive the request through the communication interface and the initial wireless network to access the second wireless network, the request being on behalf of the mobile device and indicating a network system specifying the second wireless network;

obtain through the communications interface and the intermediary network an access identifier for the second wireless network, the access identifier for use by the mobile device when accessing the second wireless network, and

provide through the communications interface the access identifier to the mobile device to use when accessing the second wireless network.

26. The network gateway of Claim 25, wherein the first wireless network is a wireless local area network, the second wireless network is a cellular telecommunications network, and the mobile device is a personal digital assistant.

27. The network gateway of Claim 25, wherein the request includes a user

identification of a user of the mobile device, and the gateway application configures the digital processor to determine an identity of the network system as a function of the user identification.

28. The network gateway of Claim 25, wherein the gateway application configures the digital processor to provide through the communications interface an authentication request based on the request to a dynamic host configuration server.

29. The network gateway of Claim 25, wherein the access identifier is an internet protocol address and the intermediary network is the internet.

30. The network gateway of Claim 25, wherein the gateway application configures the digital processor to request through the communications interface the access identifier from a second network gateway for the second wireless network, the second network gateway providing the access identifier from a predefined range of access identifiers allocated to the second wireless network.

31. The network gateway of Claim 25, wherein the gateway application configures the digital processor to store the access identifier in a device database that includes a device identification for the mobile device.

32. A computer program product that includes a computer usable medium having computer program instructions stored thereon for enabling a mobile device to roam between a first wireless network and a second wireless network, the first wireless network substantially heterogeneous with the second wireless network, both the first wireless network and the second wireless network capable of communicating with an intermediary network, and the mobile device capable of accessing the first wireless network and the second wireless network, such that the computer program instructions,

when performed by a digital processor, cause the digital processor to:

receive a request at the first wireless network to access the second wireless network, the request being on behalf of the mobile device and indicating a network system specifying the second wireless network;

through the intermediary network, obtain an access identifier for the second wireless network, the access identifier for use by the mobile device when accessing the second wireless network; and

provide the access identifier to the mobile device to use when accessing the second wireless network.

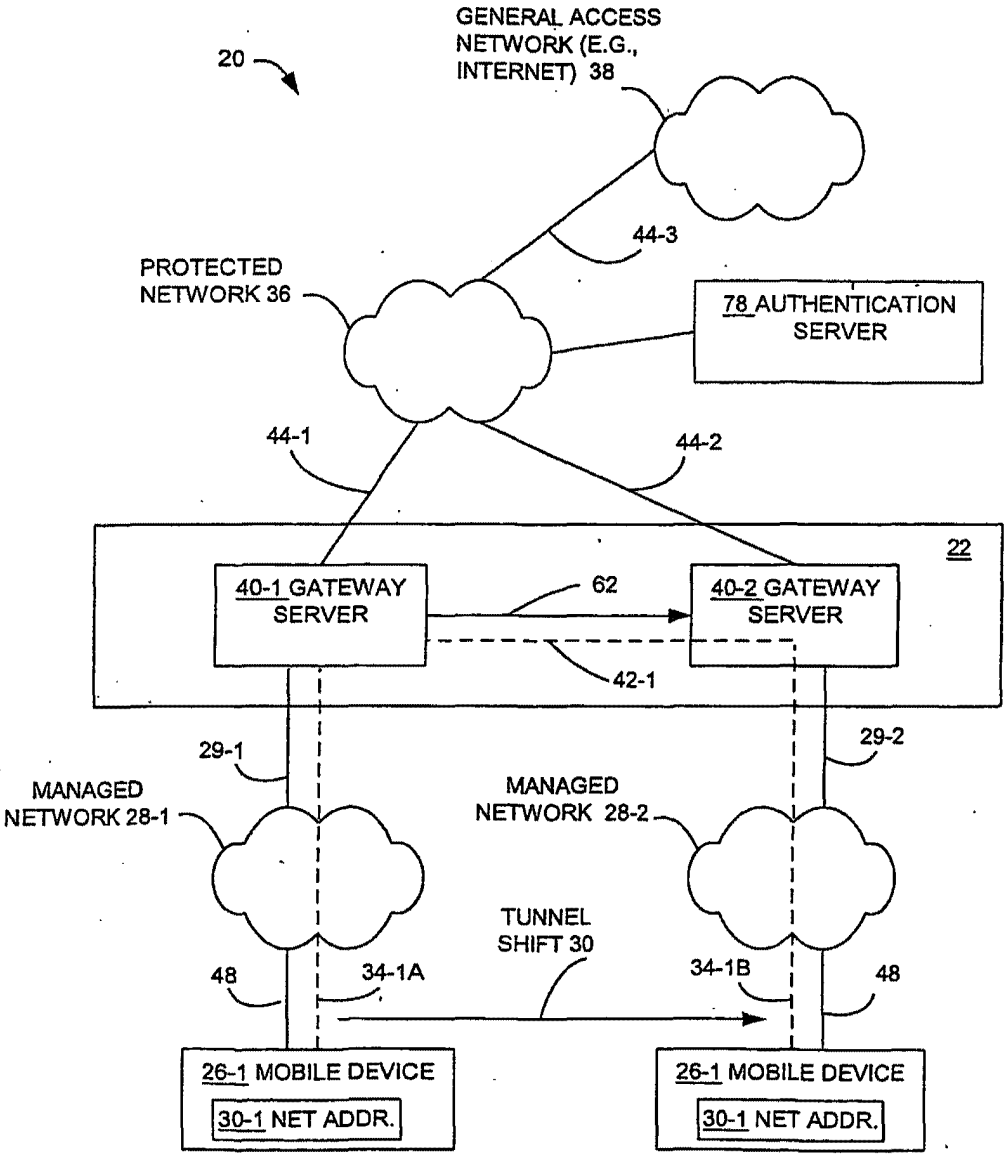

20
GENERAL ACCESS NETWORK (E.G., INTERNET) 38
44-3
PROTECTED NETWORK 36
78 AUTHENTICATION SERVER
44-1
44-2
22
40-1 GATEWAY SERVER
62
40-2 GATEWAY SERVER
42-1
29-1
29-2
MANAGED NETWORK 28-1
MANAGED NETWORK 28-2
TUNNEL SHIFT 30
48
34-1A
34-1B
48
26-1 MOBILE DEVICE
30-1 NET ADDR.
26-1 MOBILE DEVICE
30-1 NET ADDR.

FIG. 1

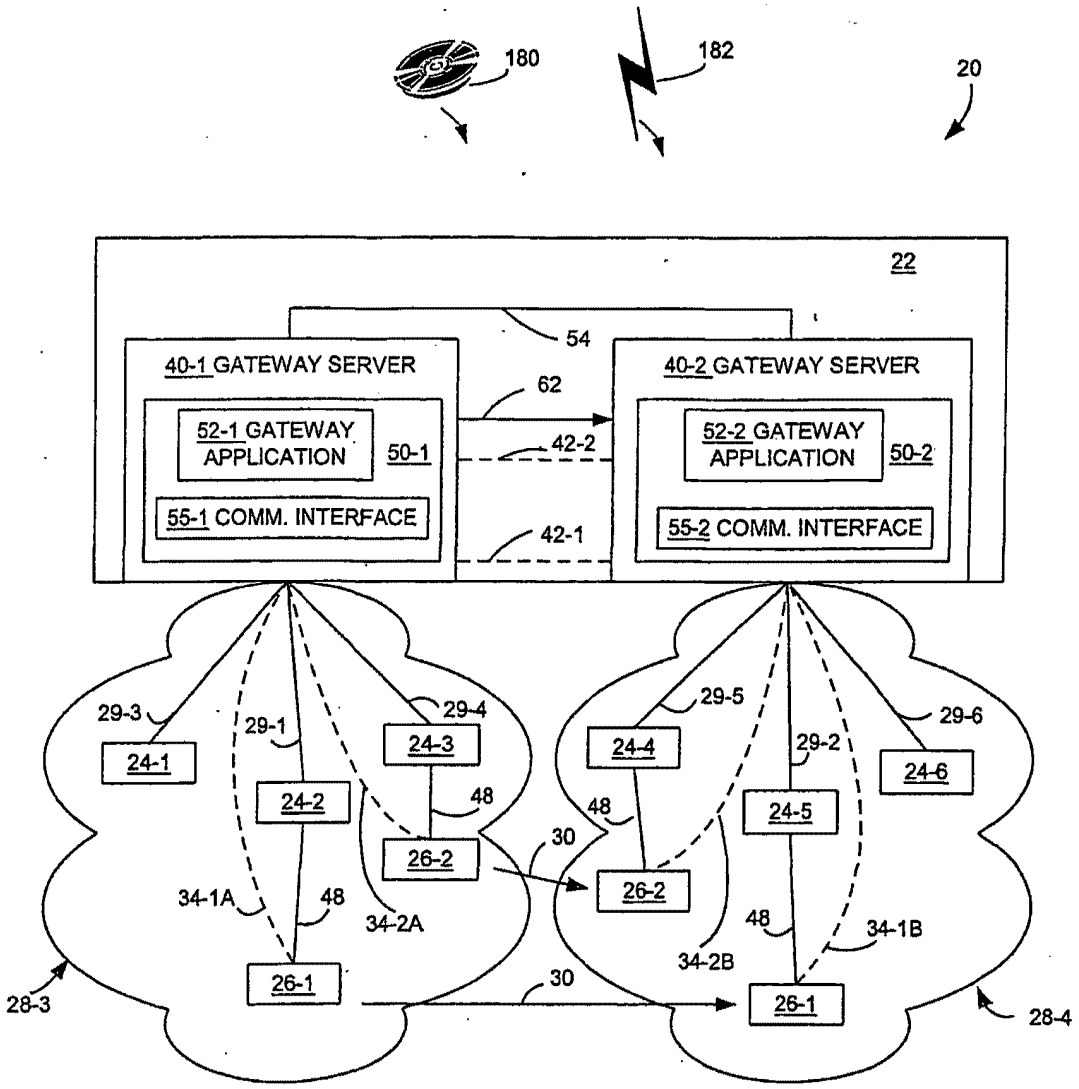

180
182
20
22
54
40-1 GATEWAY SERVER
40-2 GATEWAY SERVER
62
52-1 GATEWAY APPLICATION
50-1
42-2
52-2 GATEWAY APPLICATION
50-2
55-1 COMM. INTERFACE
42-1
55-2 COMM. INTERFACE
29-3
29-1
29-4
29-5
29-6
29-2
24-1
24-2
24-3
24-4
24-5
24-6
48
26-2
30
34-1A
34-2A
34-2B
34-1B
26-1
28-3
28-4

FIG. 2

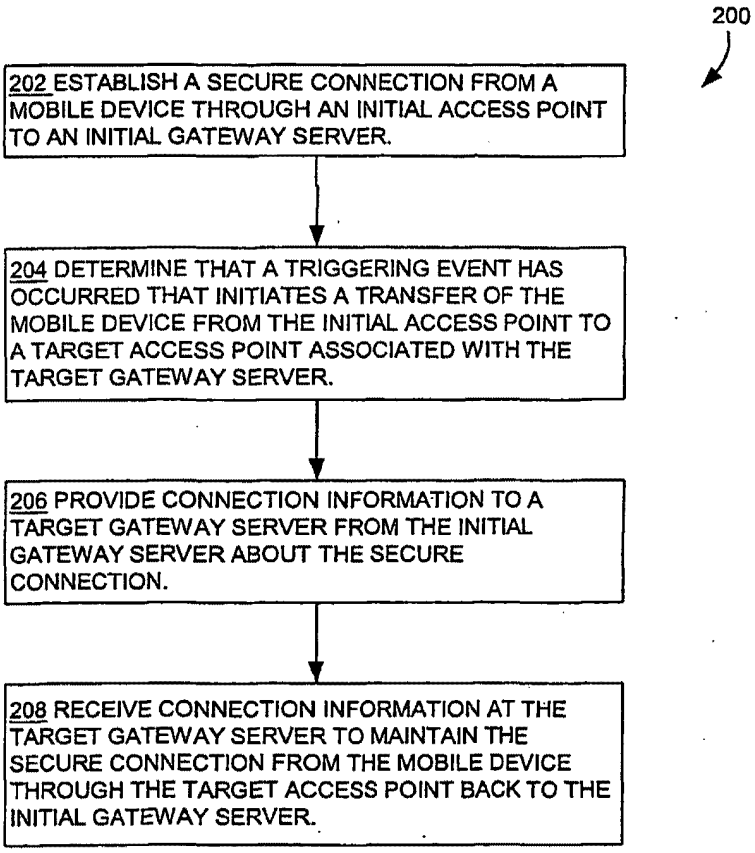

200
202 ESTABLISH A SECURE CONNECTION FROM A MOBILE DEVICE THROUGH AN INITIAL ACCESS POINT TO AN INITIAL GATEWAY SERVER.
204 DETERMINE THAT A TRIGGERING EVENT HAS OCCURRED THAT INITIATES A TRANSFER OF THE MOBILE DEVICE FROM THE INITIAL ACCESS POINT TO A TARGET ACCESS POINT ASSOCIATED WITH THE TARGET GATEWAY SERVER.
206 PROVIDE CONNECTION INFORMATION TO A TARGET GATEWAY SERVER FROM THE INITIAL GATEWAY SERVER ABOUT THE SECURE CONNECTION.
208 RECEIVE CONNECTION INFORMATION AT THE TARGET GATEWAY SERVER TO MAINTAIN THE SECURE CONNECTION FROM THE MOBILE DEVICE THROUGH THE TARGET ACCESS POINT BACK TO THE INITIAL GATEWAY SERVER.

FIG. 3

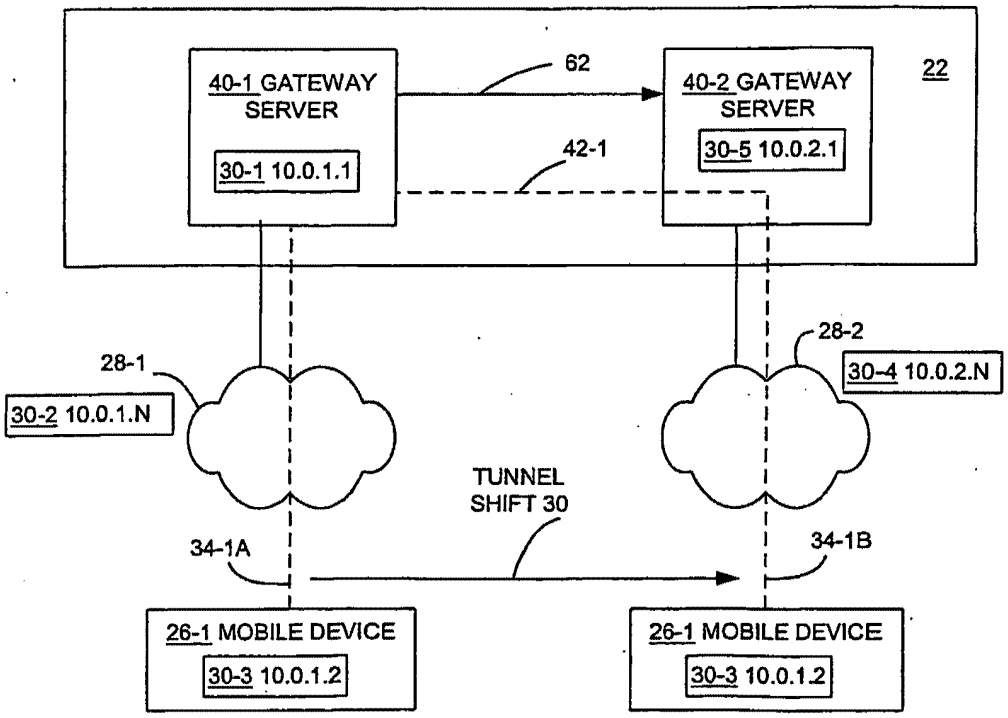

40-1 GATEWAY SERVER
30-1 10.0.1.1
62
40-2 GATEWAY SERVER
30-5 10.0.2.1
22
42-1
28-1
30-2 10.0.1.N
28-2
30-4 10.0.2.N
TUNNEL SHIFT 30
34-1A
34-1B
26-1 MOBILE DEVICE
30-3 10.0.1.2
26-1 MOBILE DEVICE
30-3 10.0.1.2

FIG. 4

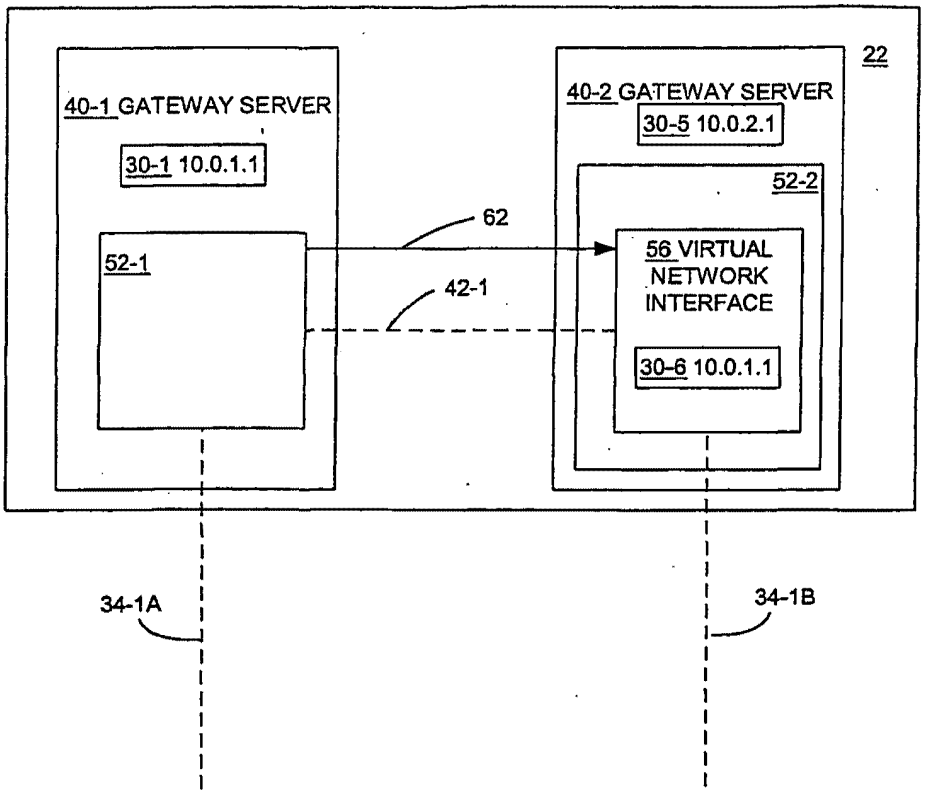

22
40-1 GATEWAY SERVER
30-1 10.0.1.1
52-1
62
42-1
40-2 GATEWAY SERVER
30-5 10.0.2.1
52-2
56 VIRTUAL NETWORK INTERFACE
30-6 10.0.1.1
34-1A
34-1B

FIG. 5

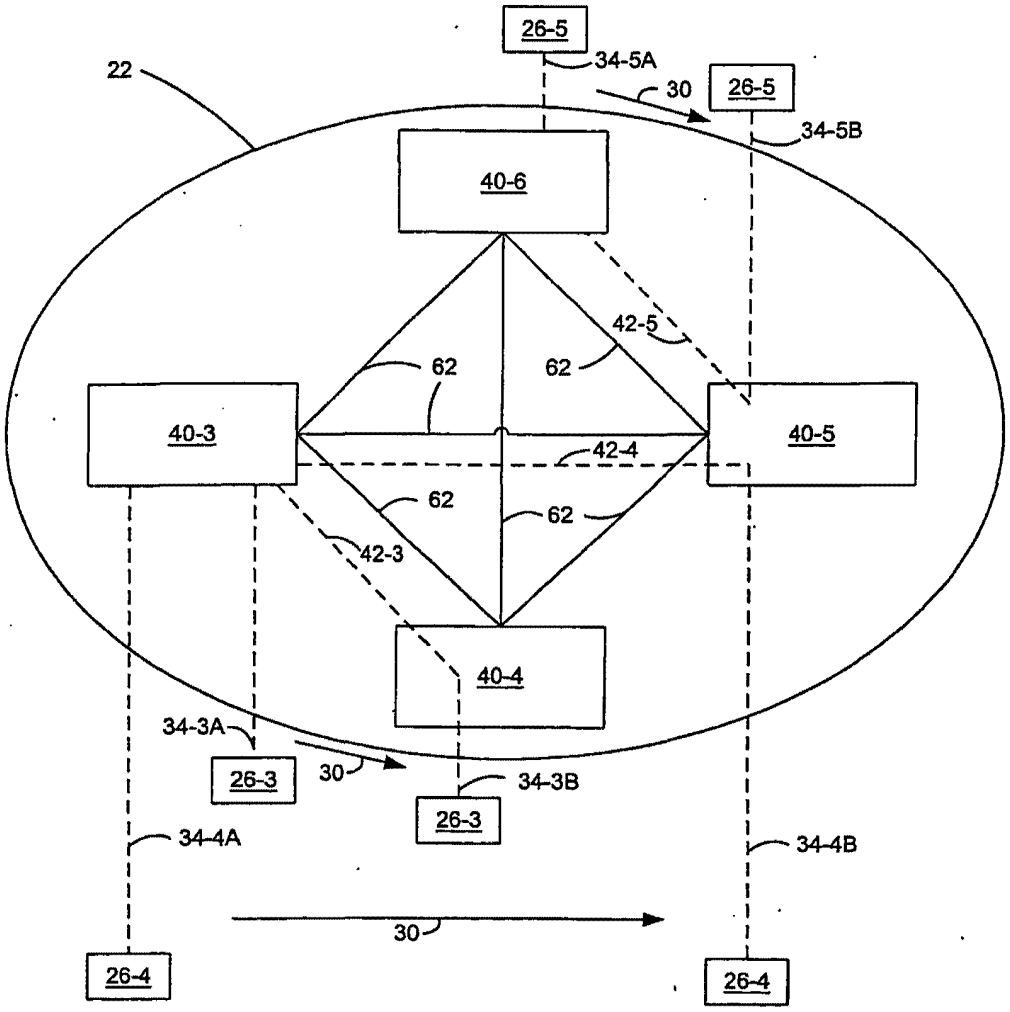

26-5
34-5A
22
30
26-5
34-5B
40-6
42-5
62
62
40-3
40-5
42-4
62
62
42-3
40-4
34-3A
26-3
30
34-3B
26-3
34-4A
34-4B
30
26-4
26-4

FIG. 6

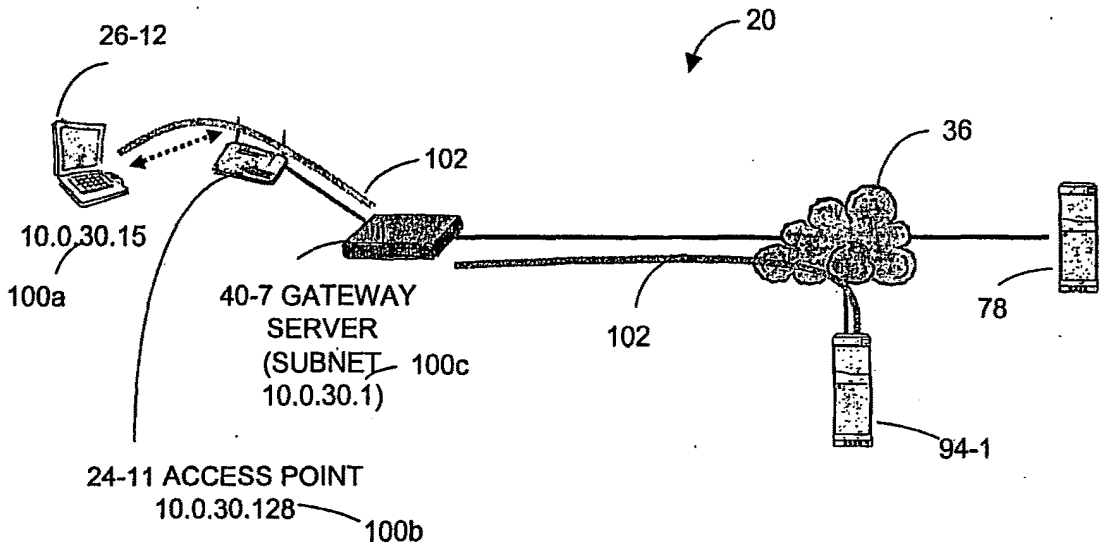

26-12
20
36
102
10.0.30.15
100a
40-7 GATEWAY
SERVER
(SUBNET
10.0.30.1)
100c
102
78
94-1
24-11 ACCESS POINT
10.0.30.128
100b

Fig. 7

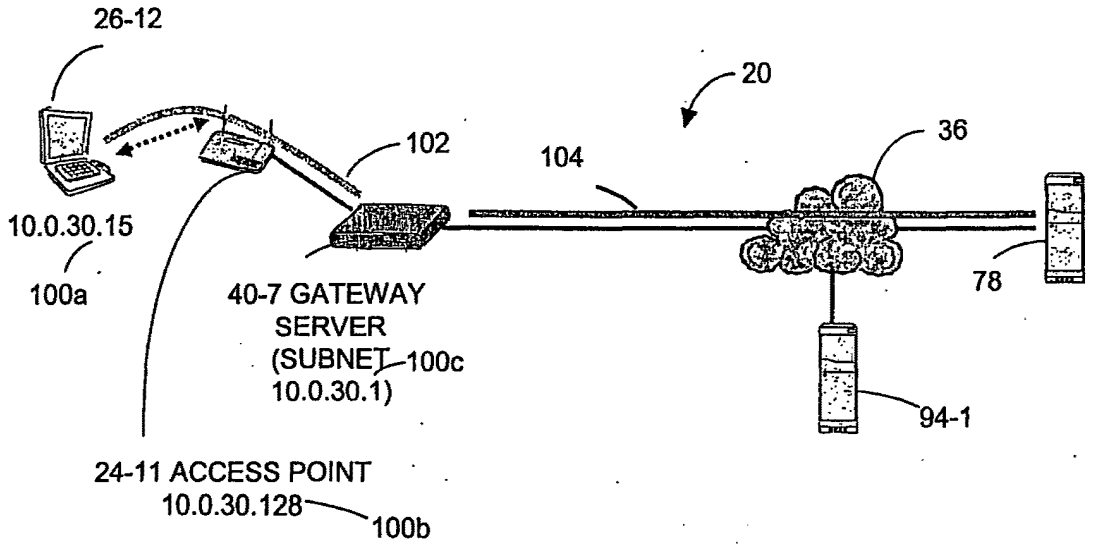

26-12
20
102
104
36
10.0.30.15
100a
40-7 GATEWAY
SERVER
(SUBNET
10.0.30.1)
100c
78
94-1
24-11 ACCESS POINT
10.0.30.128
100b

Fig. 8

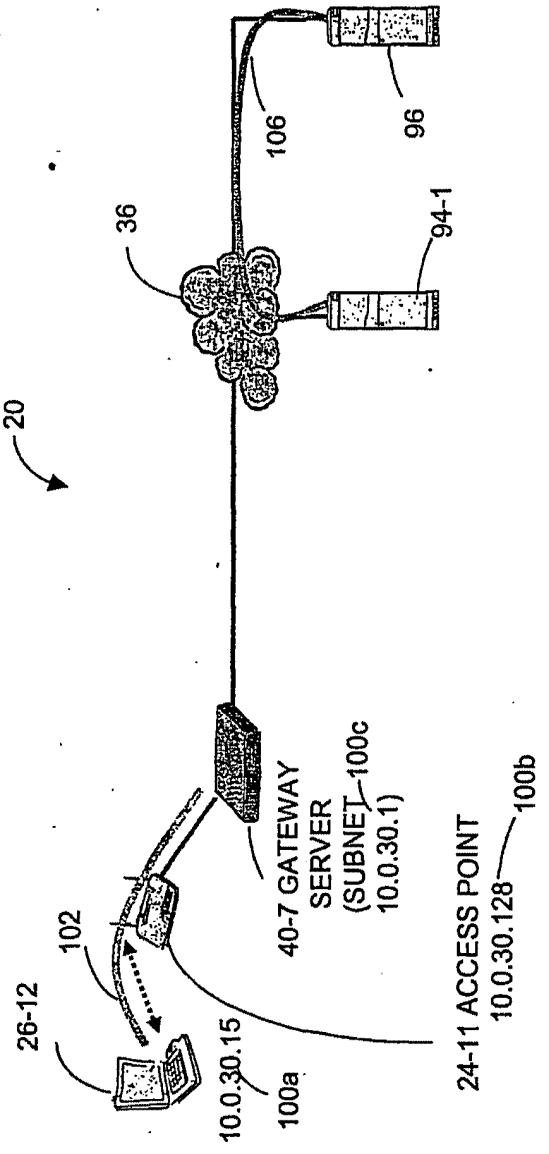

20
36
106
96
94-1
40-7 GATEWAY SERVER (SUBNET 10.0.30.1)
100c
24-11 ACCESS POINT 10.0.30.128
100b
102
26-12
10.0.30.15
100a

Fig. 9

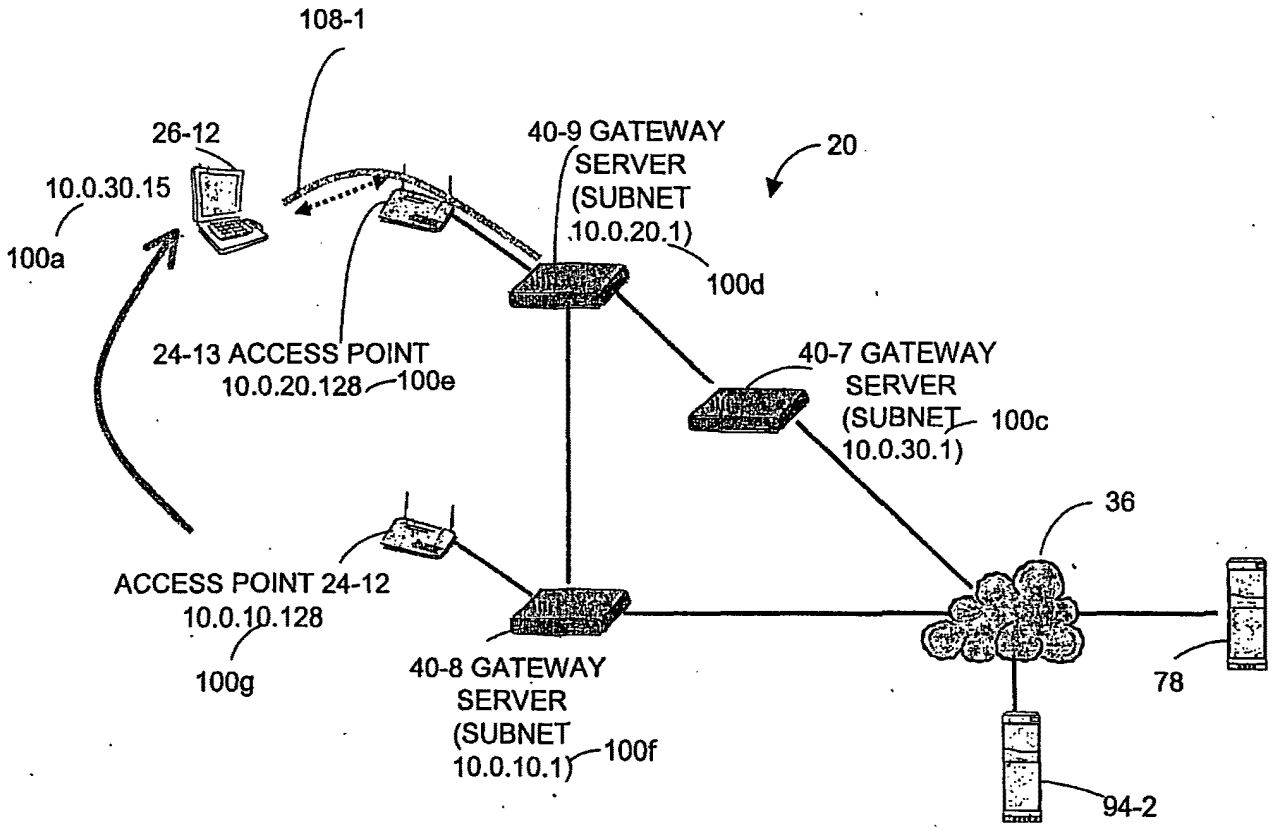

108-1
26-12
10.0.30.15
100a
40-9 GATEWAY SERVER (SUBNET 10.0.20.1)
20
100d
24-13 ACCESS POINT 10.0.20.128
100e
40-7 GATEWAY SERVER (SUBNET 10.0.30.1)
100c
36
ACCESS POINT 24-12 10.0.10.128
100g
40-8 GATEWAY SERVER (SUBNET 10.0.10.1)
100f
78
94-2

Fig. 10

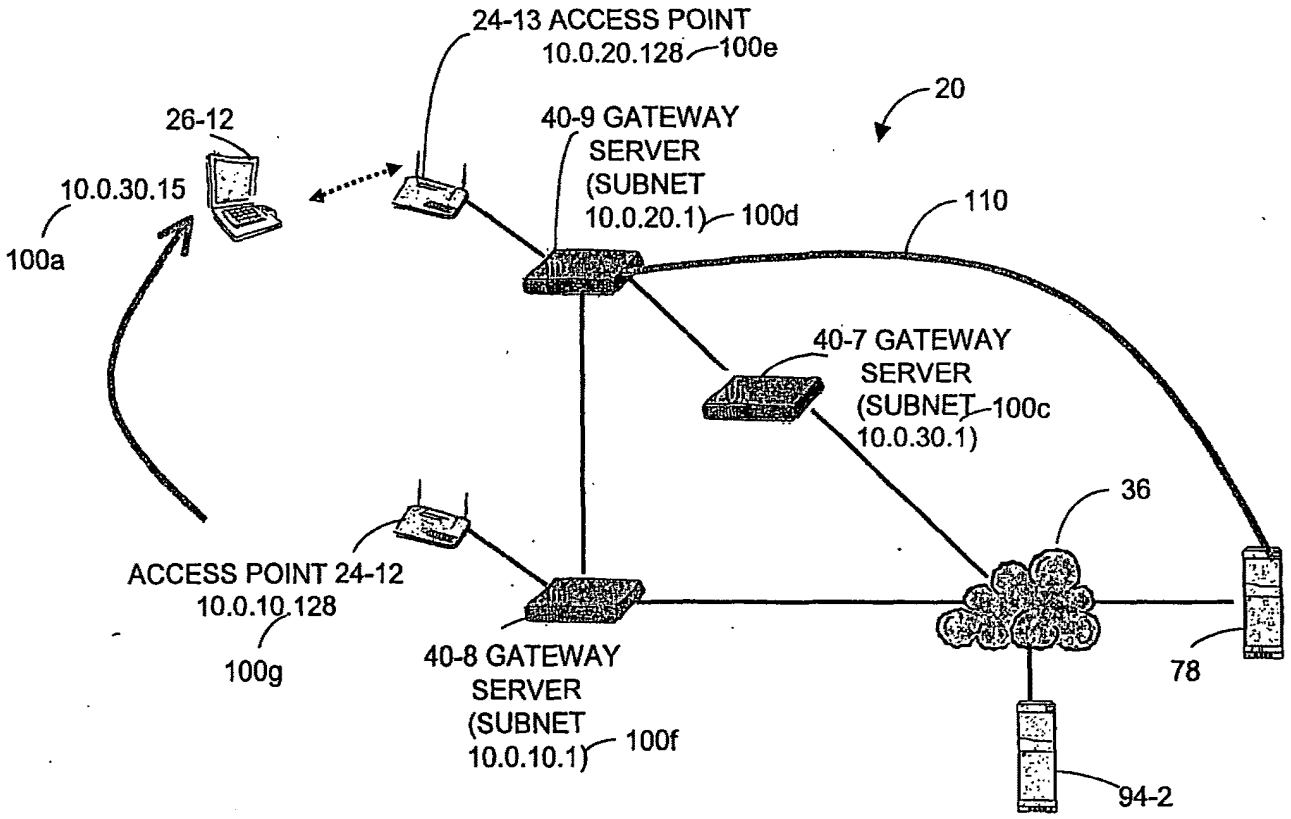

24-13 ACCESS POINT
10.0.20.128
100e
20
26-12
40-9 GATEWAY
SERVER
(SUBNET
10.0.20.1)
100d
10.0.30.15
100a
110
40-7 GATEWAY
SERVER
(SUBNET
10.0.30.1)
100c
36
ACCESS POINT 24-12
10.0.10.128
100g
40-8 GATEWAY
SERVER
(SUBNET
10.0.10.1)
100f
78
94-2

Fig. 11

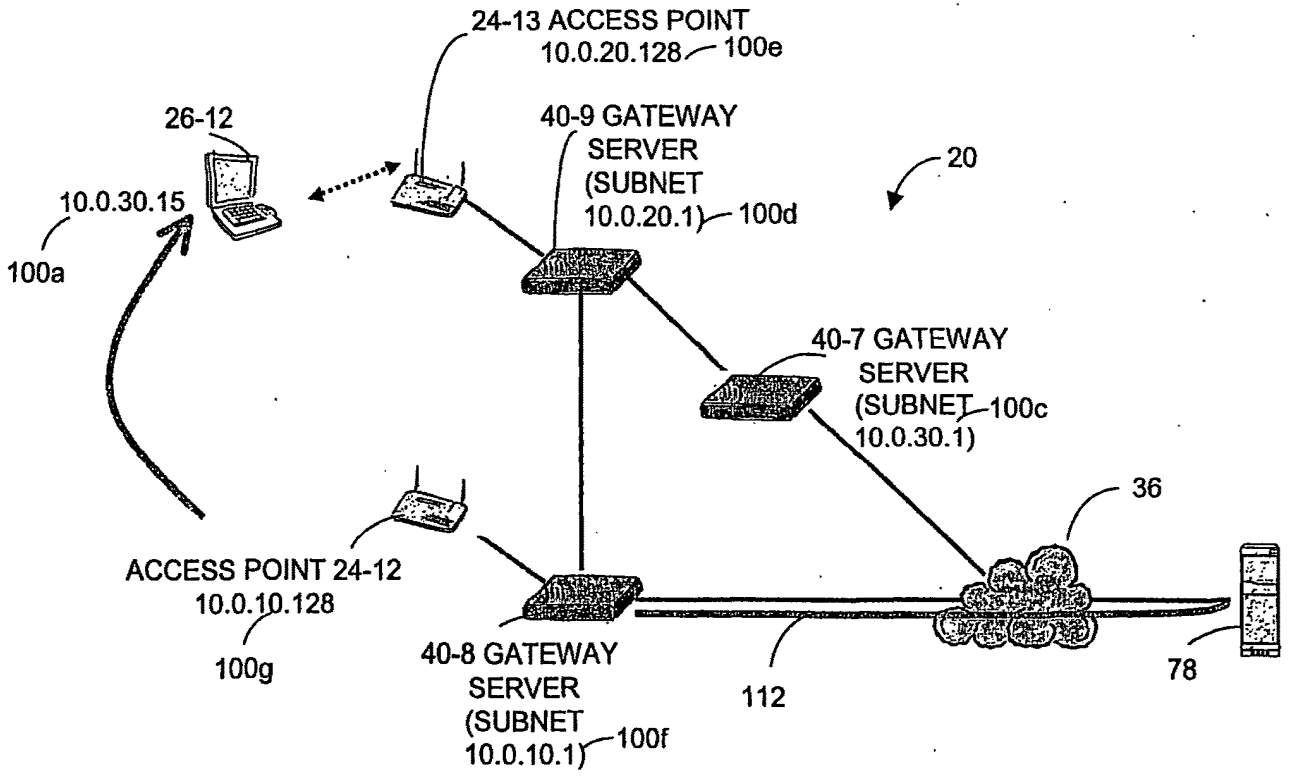

24-13 ACCESS POINT
10.0.20.128
100e
26-12
40-9 GATEWAY
SERVER
(SUBNET
10.0.20.1)
100d
20
10.0.30.15
100a
40-7 GATEWAY
SERVER
(SUBNET
10.0.30.1)
100c
36
ACCESS POINT 24-12
10.0.10.128
100g
40-8 GATEWAY
SERVER
(SUBNET
10.0.10.1)
100f
112
78

Fig. 12

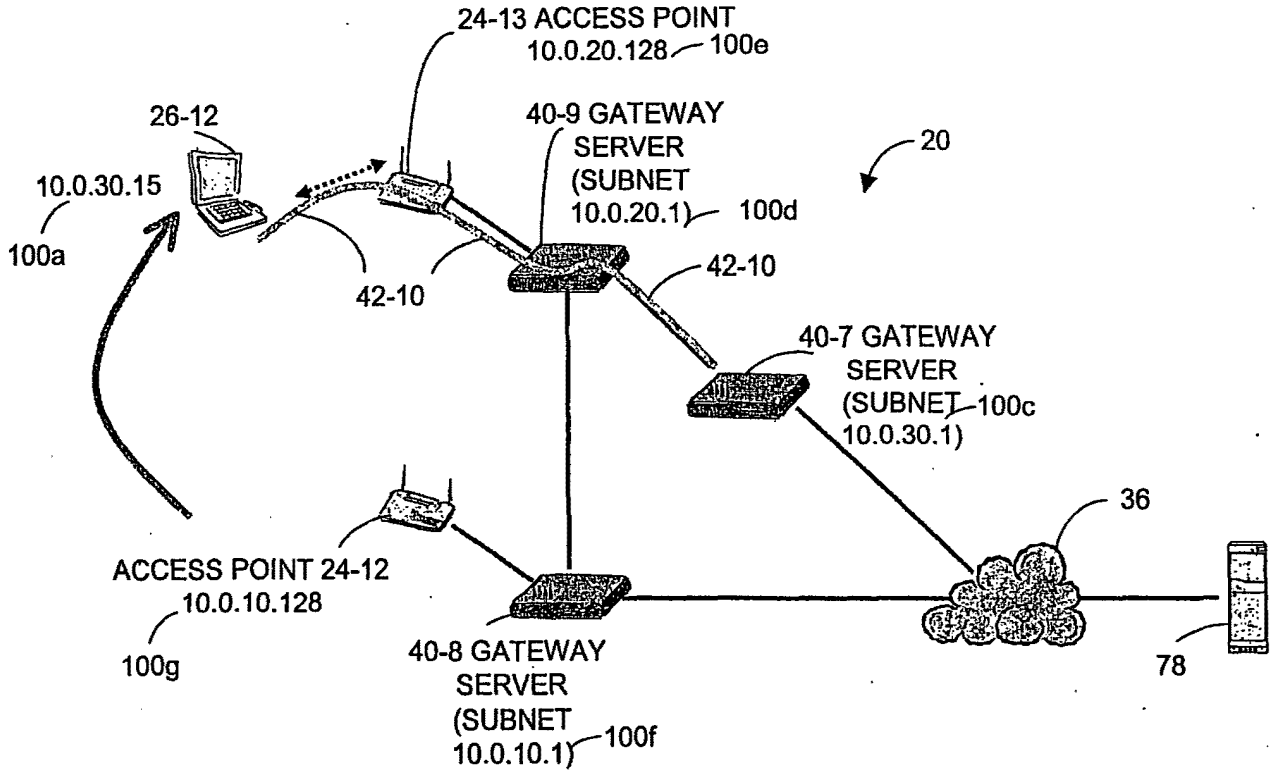

24-13 ACCESS POINT
10.0.20.128
100e
26-12
40-9 GATEWAY
SERVER
(SUBNET
10.0.20.1)
100d
20
10.0.30.15
100a
42-10
42-10
40-7 GATEWAY
SERVER
(SUBNET
10.0.30.1)
100c
36
ACCESS POINT 24-12
10.0.10.128
100g
40-8 GATEWAY
SERVER
(SUBNET
10.0.10.1)
100f
78

Fig. 13

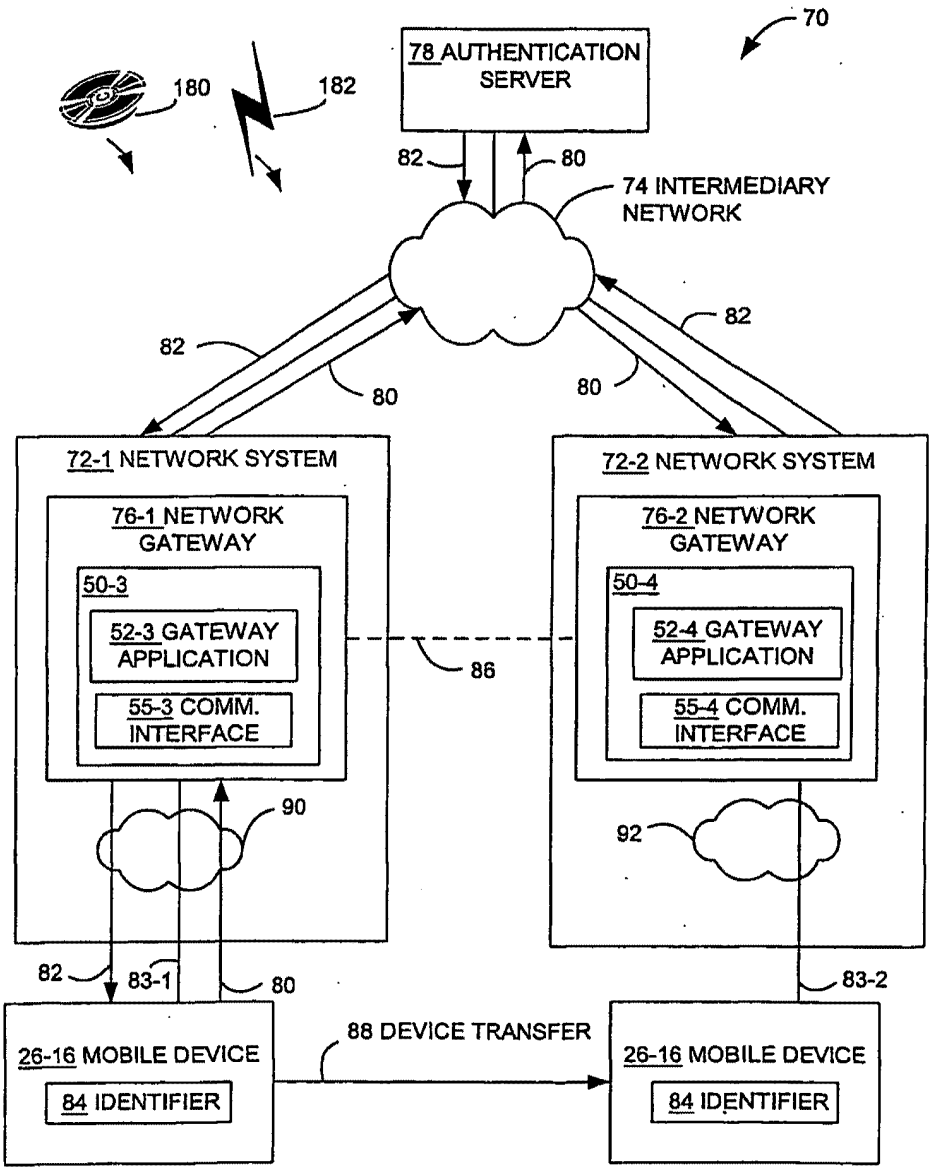

70
78 AUTHENTICATION SERVER
180
182
82
80
74 INTERMEDIARY NETWORK
82
80
82
80
72-1 NETWORK SYSTEM
76-1 NETWORK GATEWAY
50-3
52-3 GATEWAY APPLICATION
55-3 COMM. INTERFACE
86
72-2 NETWORK SYSTEM
76-2 NETWORK GATEWAY
50-4
52-4 GATEWAY APPLICATION
55-4 COMM. INTERFACE
90
92
82
83-1
80
83-2
26-16 MOBILE DEVICE
84 IDENTIFIER
88 DEVICE TRANSFER
26-16 MOBILE DEVICE
84 IDENTIFIER

FIG. 14

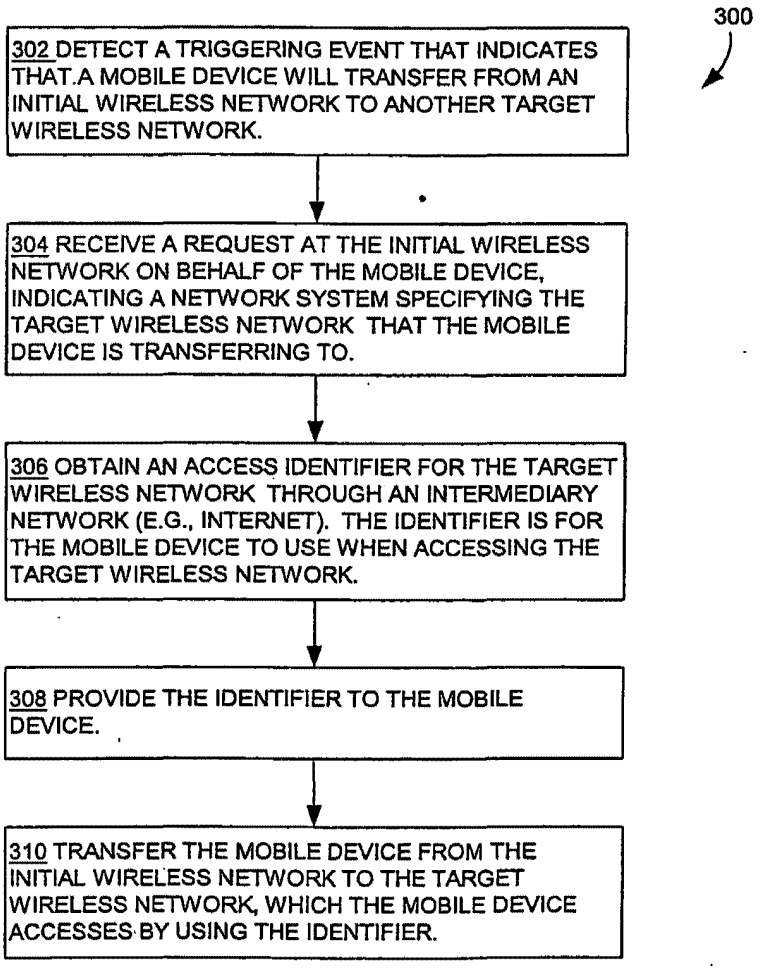

300
302 DETECT A TRIGGERING EVENT THAT INDICATES THAT A MOBILE DEVICE WILL TRANSFER FROM AN INITIAL WIRELESS NETWORK TO ANOTHER TARGET WIRELESS NETWORK.
304 RECEIVE A REQUEST AT THE INITIAL WIRELESS NETWORK ON BEHALF OF THE MOBILE DEVICE, INDICATING A NETWORK SYSTEM SPECIFYING THE TARGET WIRELESS NETWORK THAT THE MOBILE DEVICE IS TRANSFERRING TO.
306 OBTAIN AN ACCESS IDENTIFIER FOR THE TARGET WIRELESS NETWORK THROUGH AN INTERMEDIARY NETWORK (E.G., INTERNET). THE IDENTIFIER IS FOR THE MOBILE DEVICE TO USE WHEN ACCESSING THE TARGET WIRELESS NETWORK.
308 PROVIDE THE IDENTIFIER TO THE MOBILE DEVICE.
310 TRANSFER THE MOBILE DEVICE FROM THE INITIAL WIRELESS NETWORK TO THE TARGET WIRELESS NETWORK, WHICH THE MOBILE DEVICE ACCESSES BY USING THE IDENTIFIER.

FIG. 15

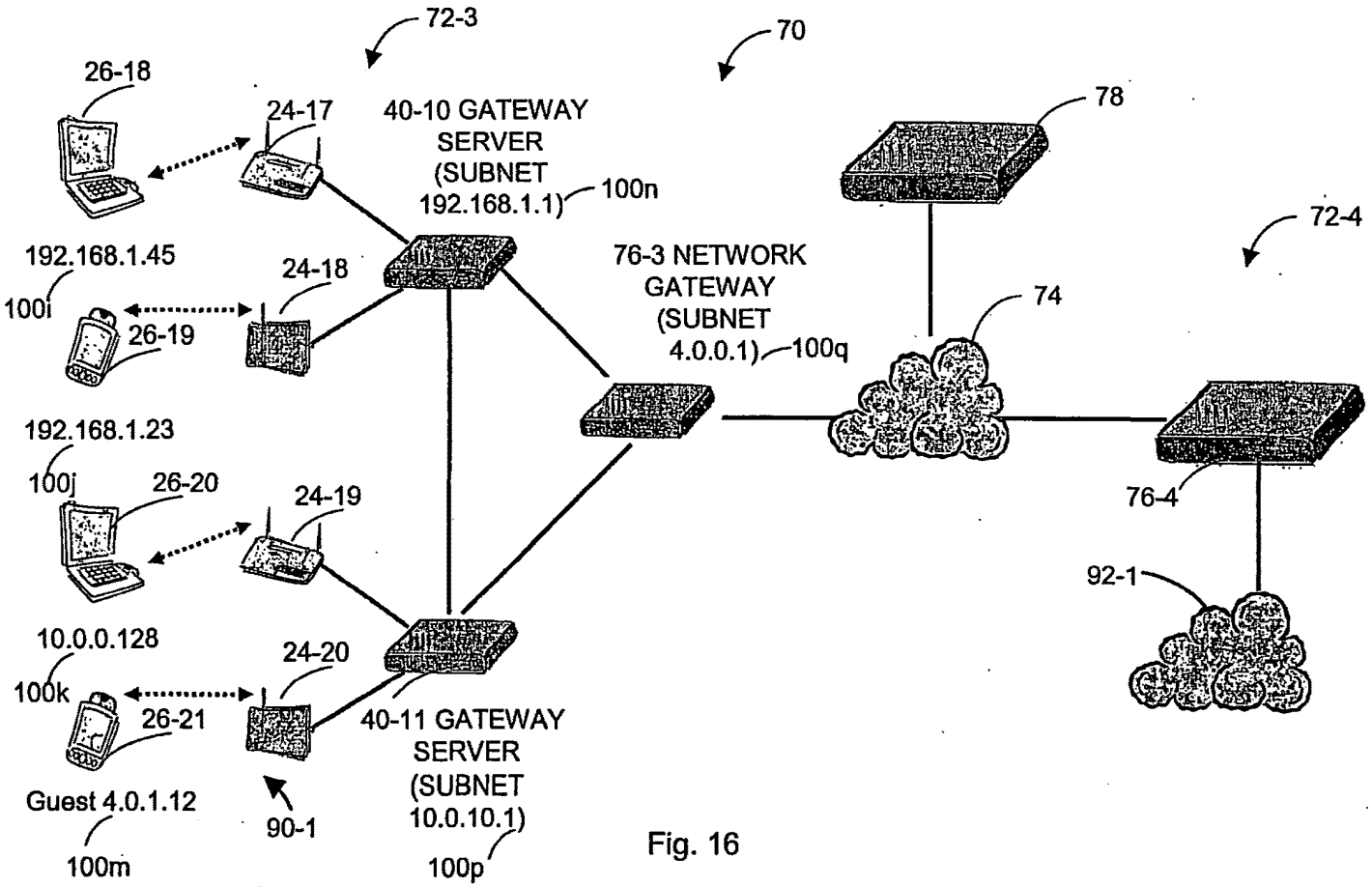

72-3
70
26-18
24-17
40-10 GATEWAY SERVER (SUBNET 192.168.1.1)
100n
78
72-4
192.168.1.45
100i
24-18
26-19
76-3 NETWORK GATEWAY (SUBNET 4.0.0.1)
100q
74
192.168.1.23
100j
26-20
24-19
76-4
92-1
10.0.0.128
100k
24-20
26-21
40-11 GATEWAY SERVER (SUBNET 10.0.10.1)
Guest 4.0.1.12
100m
90-1
100p

Fig. 16

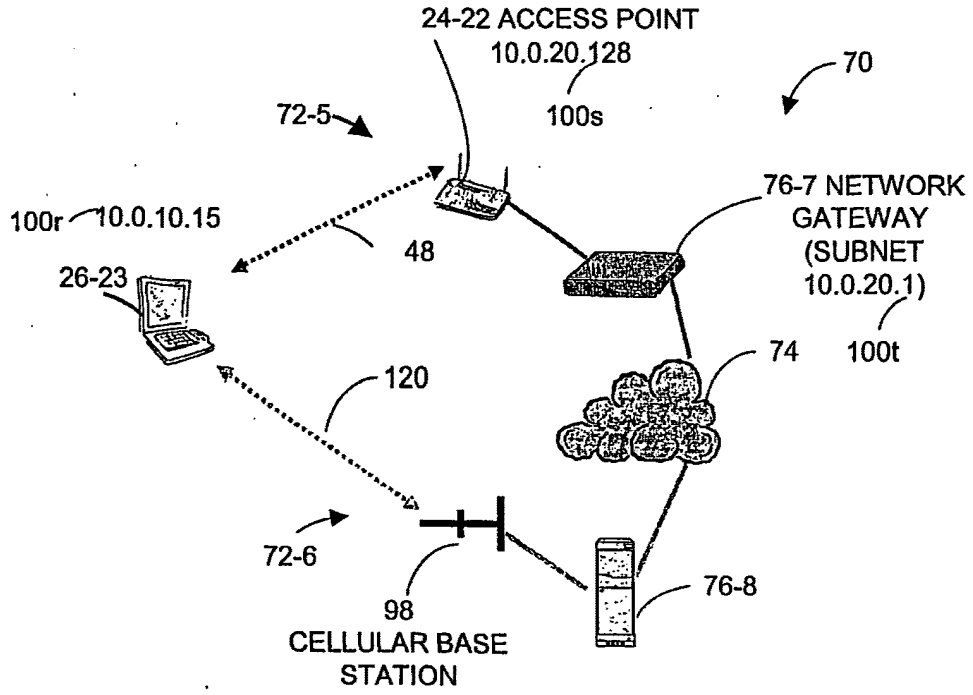

24-22 ACCESS POINT
10.0.20.128
100s
70
72-5
76-7 NETWORK
GATEWAY
(SUBNET
10.0.20.1)
100t
100r
10.0.10.15
48
26-23
74
120
72-6
98
CELLULAR BASE
STATION
76-8

Fig. 17

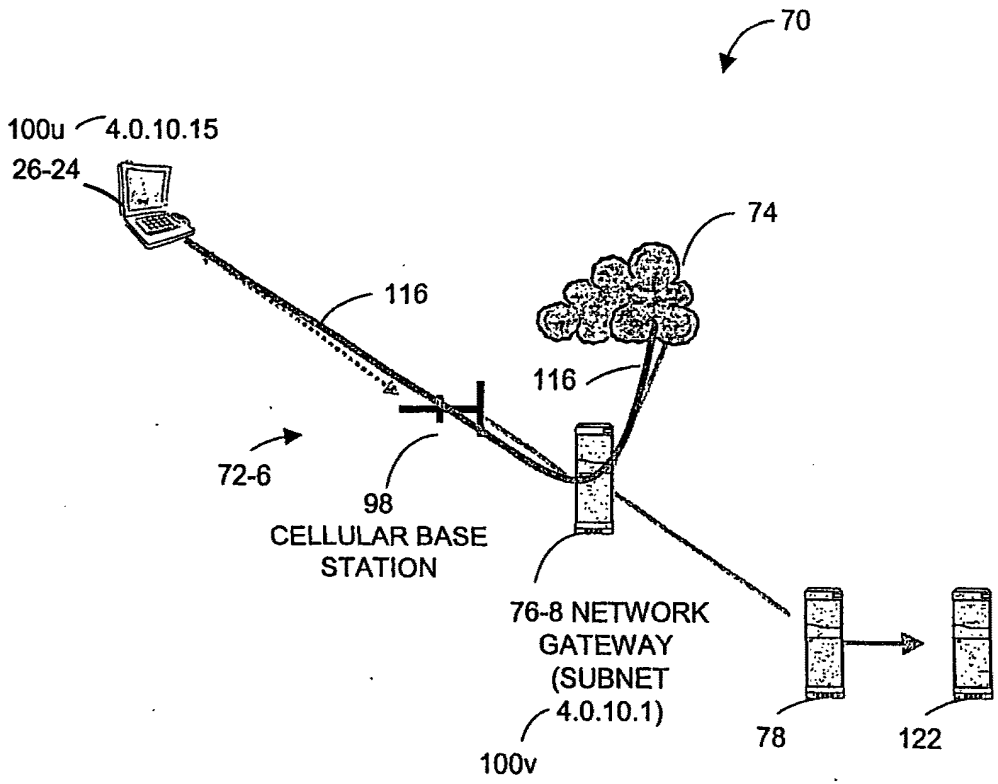

70
100u
4.0.10.15
26-24
74
116
116
72-6
98
CELLULAR BASE
STATION
76-8 NETWORK
GATEWAY
(SUBNET
4.0.10.1)
100v
78
122

Fig. 18

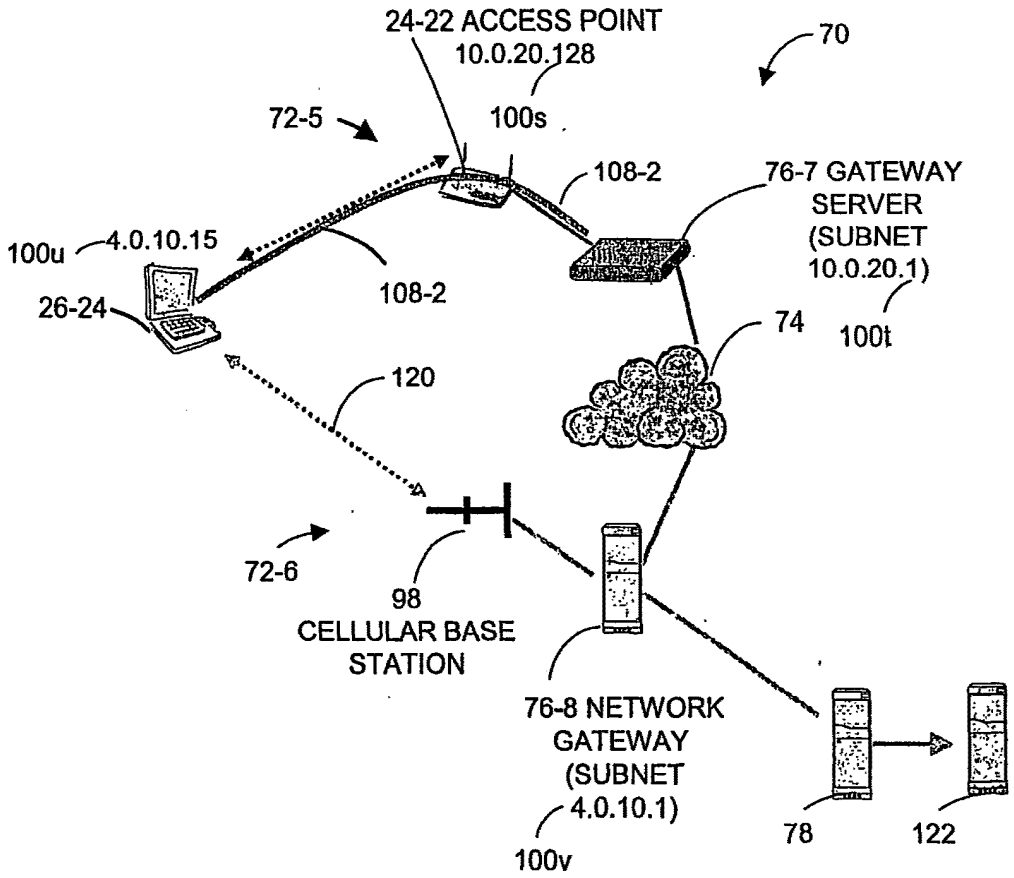

24-22 ACCESS POINT
10.0.20.128
70
72-5
100s
108-2
76-7 GATEWAY SERVER (SUBNET 10.0.20.1)
100u
4.0.10.15
108-2
26-24
100t
74
120
72-6
98
CELLULAR BASE STATION
76-8 NETWORK GATEWAY (SUBNET 4.0.10.1)
100v
78
122

Fig. 19

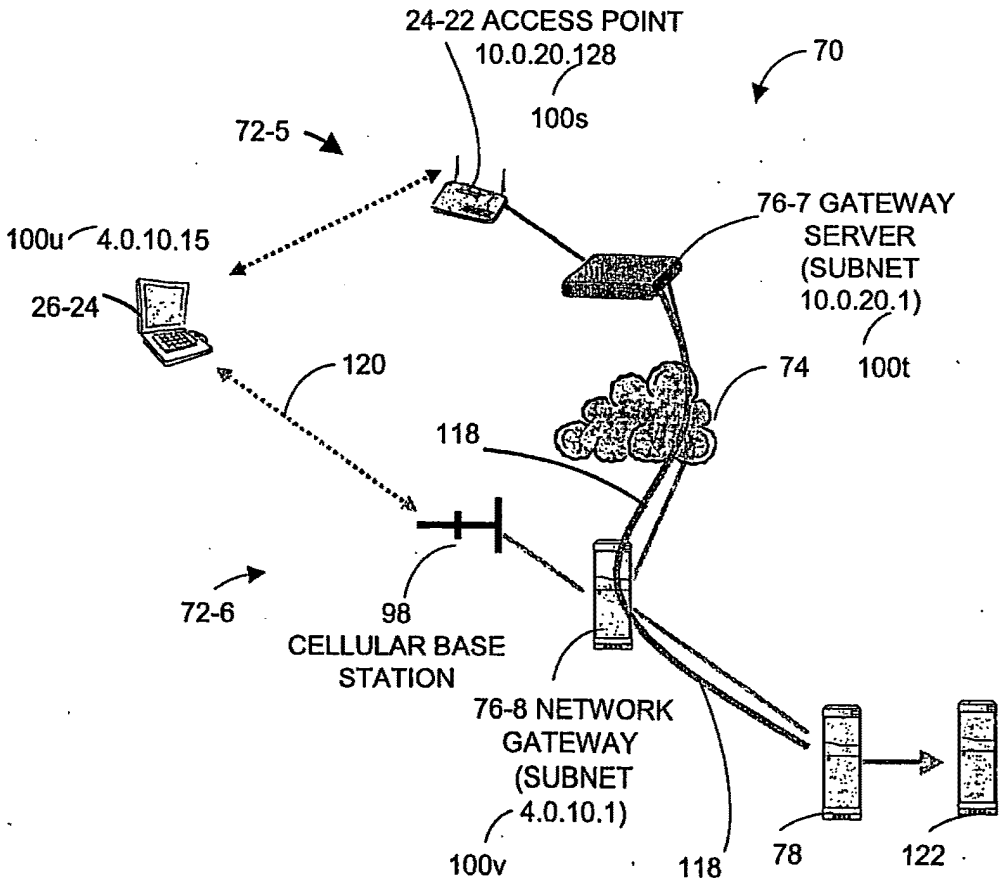

24-22 ACCESS POINT
10.0.20.128
100s
70
72-5
100u 4.0.10.15
26-24
76-7 GATEWAY SERVER (SUBNET 10.0.20.1)
100t
74
120
118
72-6
98
CELLULAR BASE STATION
76-8 NETWORK GATEWAY (SUBNET 4.0.10.1)
100v
118
78
122

Fig. 20

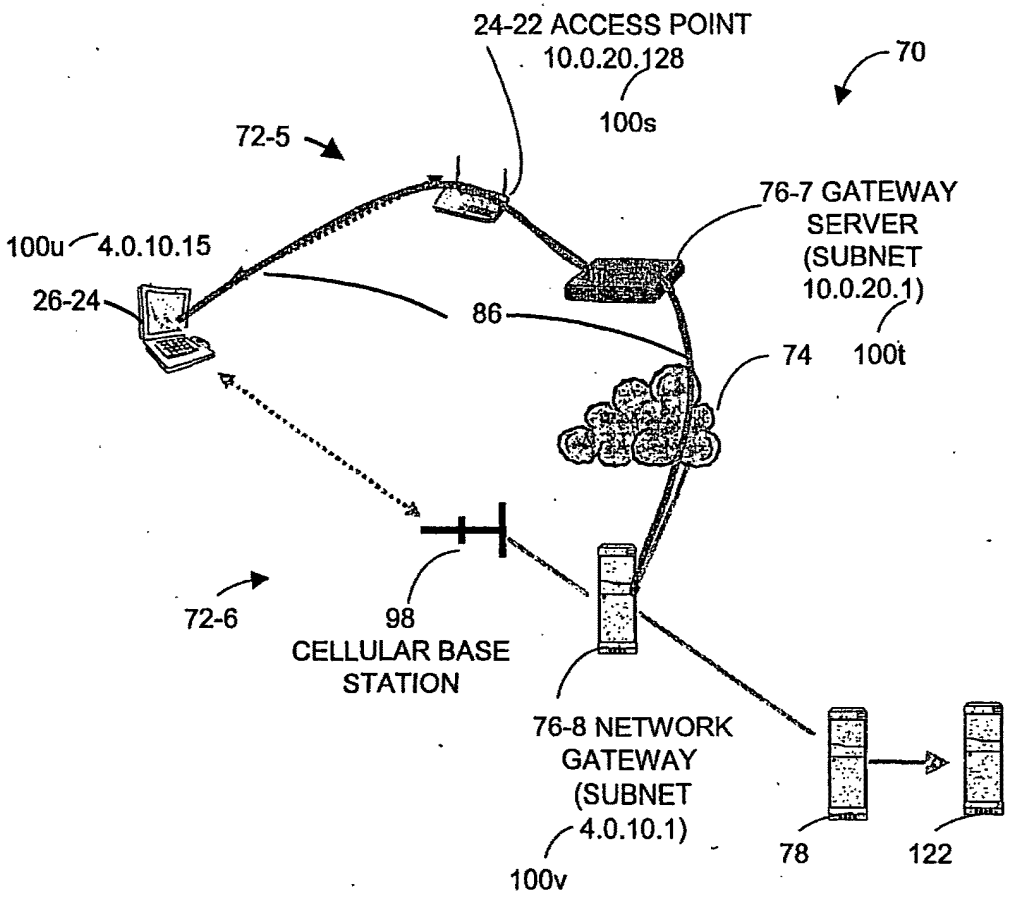

24-22 ACCESS POINT
10.0.20.128
100s
70
72-5
76-7 GATEWAY
SERVER
(SUBNET
10.0.20.1)
100u
4.0.10.15
26-24
86
74
100t
72-6
98
CELLULAR BASE
STATION
76-8 NETWORK
GATEWAY
(SUBNET
4.0.10.1)
100v
78
122

Fig. 21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/08986

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30; H04L 9/00
US CL : 713/200, 201, 160
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 160

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST- USPATFULL, JPO, EPO, DERWENT, IBMTBD, terms: roam, roaming, mobile, secure, comm$, connection, tunnel, class 713, 380.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/0066029 A1 (YI) 30 MAY 2002	1
A	US 2002/0066032 A1 (KURUMIDA) 30 May 2002	1
A	US 2002/0066036 A1 (MAKINENI ET AL.) 30 May 2002	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 01 JULY 2002	Date of mailing of the international search report 19 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harwood NORMAN M. WRIGHT Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★

B8

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2003 (27.11.2003)

PCT

(10) International Publication Number
WO 03/098461 A1

(51) International Patent Classification[7]: G06F 15/177, 13/00

(21) International Application Number: PCT/US03/13407

(22) International Filing Date: 14 May 2003 (14.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/379,757	14 May 2002 (14.05.2002)	US
60/426,341	15 November 2002 (15.11.2002)	US
10/321,722	18 December 2002 (18.12.2002)	US
60/436,996	31 December 2002 (31.12.2002)	US

(71) Applicants and
(72) Inventors: **POLCHA, Andrew, J.** [US/US]; 12462 Cabin Spring Lane, Lovettsville, VA 20180 (US). **POLCHA, Michael, P.** [US/US]; 12462 Cabin Spring Lane, Lovettsville, VA 20180 (US).

(74) Agents: **FLESHNER, Mark, L.** et al.; Fleshner & Kim, LLP, P.O. Box 221200, Chantilly, VA 20153-1200 (US).

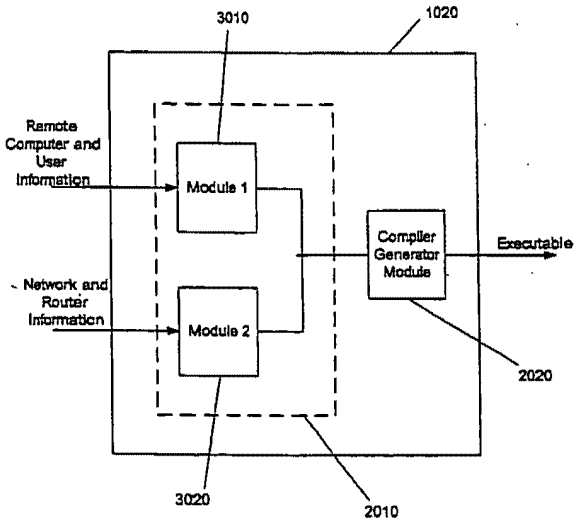
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AUTOMATICALLY CONFIGURING REMOTE COMPUTER



(57) Abstract: A system and method for automatically configuring a remote computer to establish a VPN connection with a network is disclosed. According to the system and method, a configuration generator (1020) determines information necessary for the remote computer to establish the VPN connection, and generate an executable file to be run the remote computer. When run on the remote computer, the executable file automatically updates the remote computer's configuration settings so as to enable it to establish the connection with the network. The information required by the configuration generator (1020) can either be extracted from a database automatically, or can be keyed in by a network administrator.

WO 03/098461 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR AUTOMATICALLY CONFIGURING REMOTE COMPUTER

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to remote computer configuration, and more particularly to a system and method for automatically configuring a remote computer for establishing a virtual private network (VPN).

Background of the Related Art

A Virtual Private Network (VPN) is a secure communication channel established between computers over a shared public network. In most instances, the VPN connects a remote user's computer (sometimes referred to as the caller) with a local host computer (sometimes referred to as the callee) over the Internet. Thus, for example, a user's home computer can be connected to a local area network (LAN) at the user's place of employment. Before such a connection can be established, however, the user's home computer and the LAN need to be properly configured for the remote connection.

Referring to Figure 1, a structure of a related art VPN is shown. Referring to Figure 1, a LAN includes at least one server 100 having various local user computers 100-1 ~ 100-N connected thereto. Additionally, the server 100 is coupled to a gateway/router 120 to access the Internet 130. The gateway/router 120 allows for two-way communication between the server 100 and the Internet 130. Additionally, the gateway/router 120 can also be coupled to an Internet service provider (ISP) 150.

At least one remote computer 140-1 is also coupled to the Internet 130. The remote user 140-1 can connect to the Internet 130 using its own ISP 160-1. When the remote user 140-1 and the gateway/router 120 are properly configured, the remote computer 140-1 can establish a secure connection through the Internet 130 to the gateway/router 120. The VPN connection is thus established. Once the VPN connection is established, the remote computer 140-1 is seen by the server 100 as another local user connected to the server 100. For example, the remote computer 140-1 would be present in the network neighborhood administered by the server 100. Any number of remote users could access the gateway/router 120 through the Internet 130, depending on the configuration of the gateway/router 120.

Before a VPN connection can be established between the remote computer 140-1 and the server 100, however, the remote computer 140-1 and the gateway/router 120 need to be properly configured. For example, the remote computer 140-1 needs to be given the proper network

address to the gateway/router 120, and needs to know how to access the server 100. For example, various client services must be installed and configured on the remote computer to access the server. The procedure for accessing the server 100 could include, for example, knowing proper user names and passwords.

A network administrator operating the LAN is typically required to configure both the gateway/router 120 and the remote computer 140-1. Because the gateway/router 120 is typically co-located with the LAN, and is also remotely accessible by using prescribed TELNET commands, the network administrator supporting the LAN can easily access the gateway/router 120 (being an Internet device) so as to properly configure it. However, most remote computers are, by definition, not co-located with the LAN 100. Therefore, these computers are most often not remotely accessible to be remotely configured.

Accordingly, a problem with a related art VPN is that a network administrator needs to individually configure each remote computer so that the user will be able to access the LAN. This may require that the network administrator physically visit the remote location where the remote computer is, or alternatively may require that a remote user bring the remote computer to the network administrator. This can be very inconvenient and cause delay in configuring the remote computer. Additionally, when establishing the connection between the remote computer 140-1 and the server 100, a remote user may be required to first access the remote user's Internet service provider, next access the gateway/router, and then access the LAN. Accordingly, there can be up to three levels of authentication that need to be traversed by the remote user to gain access to the LAN. This can be difficult for some users to properly navigate.

One solution to this problem is to provide an HTML wizard that can provide instructions for a user to follow to configure a computer for remote access. However, because of the complexity of properly configuring a remote computer for access, this method can prove ineffective. Additionally, even with the instructions, the process of configuring the remote computer can still be time-consuming. Finally, a user following the instructions of the wizard may still enter erroneous data, thus requiring a network administrator to first undo the mistake and then reconfigure the computer for remote access.

The above references are incorporated by reference herein where appropriate for appropriate teachings of additional or alternative details, features and/or technical background.

SUMMARY OF THE INVENTION

An object of the invention is to solve at least the above problems and/or disadvantages and to provide at least the advantages described hereinafter.

It is another object of the present invention to provide a system and method for configuring a remote computer for access to a VPN by generating an executable code to be run on the remote computer that configures the remote computer.

It is another object of the present invention to provide a system and method for automatically configuring a remote computer to access a VPN by e-mailing an executable program to the remote user which, when executed, properly sets the required parameters to establish the VPN connection.

It is another object of the present invention to provide a system and method for automatically configuring a remote computer to access a VPN by generating an executable program that configures a computer to access an ISP, access a gateway/router, and login to a LAN by selecting a single program icon.

It is another object of the present invention to provide a system and method for remotely configuring an operating system of a remote computer by generating an executable file that, when executed, manipulates registry entries of the remote computer according to requirements of the user of the remote computer.

According to the preferred embodiment, a compiler module is provided to generate an executable program that can be run on a remote computer to configure the remote computer to establish a VPN connection to the host computer. The compiler module uses various information regarding the local/host computer to generate the executable file that will configure the remote computer. For example, the compiler module uses information on the WAN profile of the network/LAN, the primary and secondary DNS of the local computer, and the primary and secondary WINS address of the local computer. Additionally, the compiler module uses the type of network configuration (client services), such as Microsoft or Novell, as well as the configuration of the server (for example, as domain controller or server). Next, the gateway address of the local computer is also provided to the compiler module.

In the preferred embodiment, no information regarding the remote computer is necessary to generate the executable file. Specifically, the executable file will first determine the necessary information regarding the remote computer when it is executed on the remote computer, and then will use that information to properly configure the remote computer. However, it would also be possible to provide the configuration module with information regarding the operating system that the remote user has installed on the remote computer. By doing this, it may be possible to streamline the executable file that will eventually be delivered to the remote computer. That is, the executable file will already be tailored for the remote computer.

It is to be understood that any method can be used to provide the necessary information to the compiler module. In one embodiment, a system information front end module is provided to prompt the network administrator to provide the necessary information. The system information module then saves this information in a prescribed format to be used by the compiler module. In another embodiment, the necessary information is extracted from a database into which the information has previously been stored.

Using the information, the compiler module generates an executable file including all of the parameters in a prescribed format. These parameters include client, adapter, protocol, and service. When run on a remote computer, the executable program configures the operating system with the settings necessary to establish a VPN connection to the local/host network. Thus, it loads the client, adapter, protocol, and service. According to the preferred embodiment, the protocol is TCP/IP and the services file and printer sharing, which is turned on. In the preferred embodiment, the RAS phonebook of the Windows operating system is configured. Alternatively, registry entries can be directly manipulated by this executable program. The executable file can either be e-mailed to the remote user or can be downloaded from a Web site. It should be understood that any method of providing this information to the remote user could be used, such as saving it to a disk that is sent to the remote user. To provide an additional layer of security, the executable file could be password protected such that the executable program would not run on the remote computer unless a prescribed password is provided upon executing the program. By doing this, if the executable program is intercepted by an unintended recipient, the unintended recipient cannot gain access to the network because the executable program will not run without the password.

Additional information regarding the user can also be provided depending on the level of service that is intended to be provided to the user. For example, an automatic dialing program can be implemented in the executable program using the user's login and password information. Moreover, automatic login information for the network can also be provided. When this additional user information is provided, after the executable configuration program is run on the remote computer, the remote user is given a single program to run (that is, a single icon to click), which will connect to and login to the host network. This single program is preferably a dialer program. Alternatively, the compiler module could generate both a configuration program and a separate dialer program.

Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objects

FORTINET EX1002 Page 319

and advantages of the invention may be realized and attained as particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in detail with reference to the following drawings in which like reference numerals refer to like elements wherein:

Figure 1 shows a related art network configuration.

Figure 2 illustrates a system for generating the executable remote configuration file according to the preferred embodiment.

Figure 3 illustrates a configuration program generator according to the preferred embodiment.

Figure 4 illustrates the information collection module according to a first embodiment.

Figure 5 illustrates additional details of the information collection module according to the first embodiment.

Figure 6 illustrates the user configuration tab of the information collection module according to the first embodiment.

Figure 7 illustrates a construction of the database that is preferably used with the second embodiment of the information collection module.

Figure 8 illustrates a method of providing information to the information collection module according to the first embodiment.

Figure 9 illustrates a method of providing WAN profile information to the information collection module according to the first embodiment.

Figure 10 illustrates a method of providing remote user information to the information collection module according to the first embodiment.

Figure 11 illustrates a USB storage device including the executable remote configuration file according to the preferred embodiment.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The system and method of automatically configuring a remote computer to establish a VPN connection to a local computer preferably collects information about the remote computer, collects information about the local area network (LAN) and its associated gateway/router, and collects information regarding login and authentication procedures for the LAN and/or gateway/router. Using this information, at least one executable file is preferably generated for execution on the remote computer. The executable file is designed to configure the remote computer to establish a

FORTINET EX1002 Page 320

VPN connection to the LAN through the gateway/router. In the preferred embodiment, the executable file manipulates the remote computer's registry information, such as the Remote Access Service (RAS). Additionally, and the preferred embodiment, the VPN connection is a client to gateway connection. That is, the remote computer is able to itself connect to the gateway of the local computer.

In order to collect the information needed to generate the executable file, the preferred embodiment uses a configuration program generator, which can be hardware, firmware, software, or any combination thereof. Preferably, the configuration program generator is made up of at least one or more software modules. Thus, referring to Figure 3, the configuration program generator preferably includes at least two modules. A first module collects information regarding the local computer (for example, the LAN server), the remote computer (for example, a PC), and user information for the operator of the remote computer. This module is referred to as the information collection module 2010.

A second module uses the information collected by the system information module to generate the executable file. This module is referred to as the compiler module 2020. The executable file is then preferably deployed by any manner, for example by e-mail, to the remote computer for execution.

As stated above, the configuration program generator is preferably software that would be run on a computer operated by the network administrator. This computer may be the server, or can be any other computer operated by the administrator. Additionally, the configuration program generator software could have any type of graphic user interface, or none at all. For example, in operation, the configuration program generator could be displayed as one or more dialog boxes. The dialog boxes could prompt the network administrator for information, or can be pre-populated with relevant information if the configuration program generator is associated with a database that has the necessary information for each potential remote user. Alternatively, if the configuration program generator is associated with such a database, it would be possible to implement the software with no graphical user interface.

Thus, in one embodiment, the network administrator could be provided with a great deal of control over the configuration program generator by having relevant information automatically retrieved from the database, and information input fields in various dialog boxes automatically populated with the retrieved information. The retrieved information would be information necessary to generate the executable file for any given remote user. In this case, one or more dialog boxes could be initially presented having blank/empty text fields corresponding to the various information necessary to establish the VPN connection. Upon receiving an instruction from the network

administrator, the relevant information could be retrieved from the database and directly inserted into the corresponding text boxes. The network administrator would thus have the opportunity to review and/or change the information in the text boxes prior to causing the configuration program generator to generate the executable file.

Alternatively, if there is no associated database, the configuration program generator could prompt an administrator to manually enter the required information into the corresponding text boxes. In this case, similar dialog boxes would be presented having blank text boxes. The network administrator would then enter the necessary information manually. In this embodiment, the configuration program generator could be further configured to provide the manually entered information to a database for later use, in addition to generating the executable file.

In the preferred embodiment, however, the information collection module of the configuration program generator would transparently retrieve the necessary information directly from the database and pass it to the compiler module, without first displaying the information. The compiler module would then uses information to generate the executable file. A network administrator may optionally be given the opportunity to confirm the information retrieved from the database prior to generating the executable file, or to modify the information.

Regardless of how the information is provided, there is certain network information that is necessary to establish the VPN connection. This network information includes, for example, a WAN number, one or two DNS numbers, one or two WINS numbers, and the gateway IP address.

Using the network information (either provided manually by the administrator or automatically extracted from the database), the configuration program generator preferably generates an executable program that can be run on the remote computer. The executable program, when run on the remote computer, would configure the remote computer so that it can establish a VPN connection with the local computer network. It is preferable that the executable configuration program would update the registry settings of the remote computer or update the Windows settings. Depending on the operating system employed, various aspects of the registry and/or operating system data would be updated. Additionally, in a preferred embodiment, the executable file is encrypted prior to being deployed to the remote computer. In order to execute the executable file, the user of the remote computer would need to know the key to unlock the program. This would prevent unauthorized users from executing the program, and provides a layer of security.

Referring to Figure 2, a conceptual view of the system for generating the executable remote configuration file is shown. The system preferably includes a computer/processor 1010 for executing commands to convert remote user information/network information into the executable

FORTINET EX1002 Page 322

file. The computer/processor 1010 preferably has loaded thereon the configuration program generator 1020, which is preferably a software module configured to receive the remote user information and/or network information and generate the executable remote configuration file.

The software may be written in standard programming language, compiled and linked into an executable program. For example, the software could be written in JavaScript, C++, PERL, and CGI. In the preferred embodiment, the software is one of an ActiveX or and OCX module, which can be linked to an application program such as Microsoft Access.

Additionally, it is possible to use scripting to cause the remote computer to execute certain procedures. If scripting is used, the script first passes to an interpreter of the remote computer. The interpreter, preferably Windows, executes the software script into a readable medium. It should be understood that any other interpreter could be used, including UNIX, LINUX, or HTML. Moreover, it should be understood that it is possible to write code to emulate certain mouse clicks and keystrokes. For example, to configure a remote computer having Windows 98, it may be beneficial to generate the executable file to emulate keystrokes and mouse clicks required to configure the system, instead of directly writing to the registry.

Additional details of how the executable file is generated will be described in a later section.

Referring to Figure 3, additional detail of the configuration program generator 1020 is shown. The configuration program generator 1020 preferably includes an information collection module 2010 and a compiler module 2020.

The information collection module 2010 can be any software used to collect information needed by the compiler module to generate the executable remote configuration file. For example, in a very basic configuration, the information collection module could be an ASCII text comma separated document. In that case, the compiler module 2020 would preferably parse the information in the ASCII document to retrieve the necessary information for generating the executable remote configuration file.

Alternatively, the information collection module 2010 could be a database with or without a filter. Preferably, using the filter, only relevant information for a prescribed user would be provided from the database to the compiler module 2020. Alternatively, information for several users could be provided to compiler module 2020, so as to allow the compiler module 2020 to generate a plurality of executable files for each of the respective users. In either case, a network administrator could additionally review the information extracted from the database prior to transferring it to the compiler module 2020. Moreover, the network administrator could make changes to the data at that time. It should be understood that any method of compiling the database can be used.

FORTINET EX1002 Page 323

Thus, in a first embodiment of the information collection module 2010, the network administrator enters the necessary information manually. Using this embodiment, no database is necessary. Rather, for each remote user for which a VPN connection will be configured, the relevant information is prided directly to the information collection module 2010 when the network administrator needs to generate the executable file. In a second embodiment, on the other hand, a database is required. The network administrator would preferably select an appropriate record from the database. The record would preferably includes all of the information necessary to generate the executable files. The network administrator would then simply run the compiler module directly from the database to generate the executable file based on the selected record. In this case, the information collection module 2010 could optionally include a verification module, displaying the information extracted from the database for the network administrator to verify prior to generating the executable file.

Regardless of the embodiment of the information collection module 2010, the compiler module 2020 uses the information collected to generate the executable program to be run on the remote computer. Additional details of the information collection module 2010 and the compiler module 2020 are provided hereinbelow.

Referring to Figure 4, additional detail of the information collection module 2010 according to the first embodiment is provided. As shown therein, the information collection module 2010 is preferably comprised of two sub-modules 3010, 3020. The first sub-module is a remote user information collection module 3010. The second sub-module is a network information collection module 3020. A network administrator would preferably manually enter information into each of these modules, according to one embodiment of the invention.

Each module of the information collection module 2010 is preferably displayed on a user interface screen (for example, a computer monitor) as a dialog box having prompts for the required information. The network administrator would preferably enter the required information into the associated text box, or select the appropriate radio buttons, and then apply the settings. Upon applying the settings, the information collection module 2010 would format the selected information so as to be usable by the compiler module 2020. It should be understood that the dialog box could be formatted in any manner, and could be partitioned into any number of sections and/or sub-screens. Each section would preferably be identified by an associated tab, which could be selected by the network administrator to access that section of the dialog box.

The remote user information collection module 3010 preferably collects information about the remote user and the remote user's computer. Specifically, it can preferably collect information concerning what operating system the remote user is running on the remote computer, as well as

password and logon information for the remote user. By way of example, the password/login information can be for either a dial-up adapter, the LAN to which the VPN will connect, or both.

The network information collection module 3020 preferably collects information about the local area network (LAN) to which the VPN connection will be established. This information is necessary for the remote user to negotiate to the router that is coupled to the LAN, as well as negotiate through the router and/or gateway to access the LAN. Additionally, further information regarding the names of the computers on the LAN should be provided, as well as the location of the domain name service (DNS).

In a second embodiment, the information collection module 2010 would extract data directly from a database. Consequently, a dialog box would not be necessary. However, it would be possible to provide some user interface to direct the network administrator as to how to extract the relevant information. Moreover, there could be informational screens allowing the network administrator to verify incorrect information prior to generating the executable file. Preferably, information collection module 2010 would identify particular fields of the database that are needed by the compiler module 2020 and extract only that information. Additionally, once the information is extracted, the information collection module 2010 would preferably display the information for the network administrator to verify. Upon his verification, the network administrator would preferably cause the information to be transferred to the compiler module 2020.

According to the second embodiment of the information collection module 2010, any database design can be used. Preferably, the database would include at least the same information described above with respect to the first embodiment. Specifically, the database would include the information necessary for the remote user to negotiate to the router/gateway and then onto the LAN. Additional detail concerning this information will be provided below.

In both the first and second embodiments of the information collection module 2010, information regarding the remote user's e-mail address and security code can also be provided. In this way, the compiler module, upon generating the executable file, could automatically transmit all generator programs (including the configuration program and a dialog program) to the remote user. Moreover, the executable file could be encrypted, using the security code as the decryption key. Alternatively, if the program will be provided to the remote user by a method other than e-mail, a storage address could be provided to the information collection module 2010, identifying where the executable files should be stored. For example, it could be stored in a directory on a computer or to a removable storage unit, such as a floppy disk or a compact disc.

Referring again to Figure 3, the compiler module 2020 is preferably software configured to generate an executable program using the data collected from the information collection module

FORTINET EX1002 Page 325

2010. The executable program, when run on the remote computer, preferably configures the remote computer to be able to establish the VPN connection with the local network. In essence, the executable file is configured to install the VPN configuration onto the remote user's computer. It should be understood that the executable file could be used to configure their remote computer in any fashion so as to customize it to a user's needs. For example, an executable program could be generated to allow a remote user to configure a program on the remote computer, such as Microsoft Outlook, to be set up in a certain way. Thus, if a user wanted both their work computer and their home computer to have identical settings for a particular program, a network administrator could generate an executable file to configure the home computer to have the same settings as the were computer. The executable file would then be run on the home computer to change the configuration settings.

In the example of setting up the VPN connection, the compiler module 2020 preferably uses the information collected through the information collection module 2010 to generate an executable file that can be used by the remote user to configure the remote computer for the VPN connection. In the preferred embodiment, the executable file is configured to edit the Remote Access Service (RAS) files of the remote computer's operating system. Specifically, the RAS phonebook is preferably manipulated. It should be understood that any method of modifying the registry entries of the remote computer's operating system could be used. This could include directly modifying .INI files and .INF files, or any other configuration files for the remote computer.

In the preferred embodiment, the data that is received from the information collection module 2010 is either embedded or attached to the executable file, such that upon execution of the executable file on the remote computer, the data is used to configure the remote computer. In the preferred embodiment, the Microsoft installer program is used as the executable file. Microsoft installer is a binary resource out of the OCX program module. Thus, the installer is the first program built. The binary resource includes the configuration data, and because it is the first program to be built, the configuration data is initially empty. That is, the installer program is built with blank data.

When the information collection module 2010 generates the configuration data file, the blank data on the installer is replaced with the configuration data file. The installer program is preferably configured to call the RAS API, and use the data configuration file to modify the RAS entries. It should be understood that the executable file to use any method to modify particular registry entries. Accordingly, the RAS entries for VPN that have been built are attached to the installer program, and the executable file for configuring the remote computer is created.

FORTINET EX1002 Page 326

Additionally, the compiler module 2020 could be configured to automatically e-mail the executable file to an intended recipient. Thus, part of the information collected by the information collection module 2010 would include the e-mail address of the intended user. Once the code is written by the compiler module 2020, it would automatically be inserted into an e-mail addressed to the intended recipient. This e-mail could either automatically be transmitted when the executable file is generated, or could await a user command prior to sending the e-mail. Thus, for example, the configuration program generator could be integrated with any type of e-mail program, such as Microsoft Outlook or Microsoft Outlook Express.

When integrated with an e-mail program, the executable file is preferably written to an e-mail manager, such as an outbox or a draft box of the e-mail program. That is, it is written to a path on the computer that corresponds to the outbox. Moreover, an outlook plug-in will interpret specific data within the database as an e-mail address. Accordingly, the e-mail is automatically generated with the executable file or files as an attachment. Additionally, the body of the e-mail can be configured to include instructions for running the executable file. These instructions can be either tailored to a particular operating system of the user, or all instructions can be included, allowing the user to pick the appropriate set of instructions.

It should be understood that information collection module 2010 and the compiler module 2020 could be formatted as a single dialog box, so that once the information is entered into the dialog box, a single click to accept the data would generate the executable file. Additionally, that single click could also be configured to automatically send the e-mail to the intended user. Moreover, it should be understood that the whole process could be transparent to the network administrator, and thus selecting a remote user from the database would automatically generate the executable file, and could also automatically e-mail the executable file to the remote user. Alternatively, the process could be partially transparent. That is, the network administrator would have an opportunity to review dated extracted from the database prior to generating the executable file. Moreover, the network administrator may be required to manually e-mail the program to the recipient.

It should be understood that the information collection module 2010 could be a stand-alone program, or could be a module within another application program. For example, information collection module could be an OCX module and part of a Microsoft Access database. Alternatively, the program could be written and compiled in any programming language, and configured to perform the same tasks. In the preferred embodiment, the information collection module is an OCX module.

FORTINET EX1002 Page 327

Referring to Figure 5, additional details of the first embodiment (manual data entry) of the information collection module 2010 of Figure 3 are provided. As shown in Figure 5, a dialog box 200 of the configuration program generator according to a preferred embodiment is shown. The dialog box preferably includes a plurality of tabs to distinguish between information screens. In the preferred embodiment, a WAN profile tab 205 and a user configuration tab 305 are provided. The WAN profile tab 205 corresponds to the network information collection module 3020 of Figure 4, and the user configuration tab 305 corresponds to the remote user information collection module 3010 of Figure 4. Figure 5 shows details of the dialog box with the WAN profile tab selected. Details of the user configuration tab 305 will be described blow with reference to Figure 6.

The WAN profile tab 205 provides a user interface for the system administrator to enter information relating to the network to which the remote user will connect. First, a WAN text box 215 is provided. It is preferably configured in a format to accept a WAN number. The WAN number describes the IP address for the router/gateway. This information is used by the remote computer to identify the router/gateway to which it will connect to establish the VPN connection. This number is preferably a static IP address that uniquely identifies the WAN to the outside world. Additionally, a gateway text box 230 is also provided. Within this text box, the administrator preferably enters the private gateway information. This address, also formatted as an IP address, cannot be seen by the outside world when they look at the router/gateway on the Internet. Again, this text box is preferably formatted as a standard IP address. Thus, the default dialog box is preset with all zeros, such as "0.0.0.0" In the preferred embodiment, when a prescribed number of digits is entered prior to any one of the dots, the cursor automatically moves to the next digit in the address.

Next, a text entry box is provided for the primary and secondary DNS addresses 235, 240. The DNS (domain name system) is the way that Internet domain names are located and translated into IP addresses. Various lists of domain names and IP addresses are distributed throughout the Internet in an hierarchical structure, rather than maintaining a central list of domain name-to-IP address translations.

Next, a text entry box is provided for the primary and secondary WINS addresses 255, 260. The WINS address points to location on the network where the Windows Internet Naming Service (WINS) resides. WINS is an operating system based service that manages the association of workstation names and locations with IP addresses. This is done without a user's or an administrator's input. WINS thus automatically creates a mapping entry in a table to map a computer name to an associated IP address. Each computer name is unique. If a computer is moved to another geographic location, the subnet part of the IP address will most likely change. WINS ensures that the new subnet information will be updated automatically in the WINS table.

FORTINET EX1002 Page 328

WINS works in conjunction with the Dynamic Host Configuration Protocol (DHCP), which negotiates an IP address for any computer when it is first defined to the network.

Figure 6 illustrates additional details of the first embodiment of the information collection module 2010 with the user configuration tab 305 selected. The user profile configuration box is preferably divided into two sections. The first section is the router/WAN section 5010, and the second section is the LAN section 5020. Within the LAN section 5020, there is a free formatted text box for the LAN IP address 5060. This text box is preferably presented with all "0" entered in each segment of the IP address. Additionally, the text box is preferably preformatted with dots between the initial zeros, for example having "0.0.0.0" as the initial address. Next, text boxes for login 5070 and password 5080 are presented. These are the login and password necessary for the user to access LAN. Finally, a drop-down box 5090 is provided to select the operating system of the remote computer. Any operating system could be selected from this drop-down box. Based on the selection of operating system, the executable file will be generated to configure particular aspects of the corresponding operating system. In the preferred embodiment, the LAN password is not needed. The LAN login is used to change the name of the computer. Thus the user will be prompted to give the password. Also the system can be configured to prompt for both the user name and password.

On the router/WAN side 5010, a text box is provided for each of login 5030 and password 5040. These represent the login/password combination necessary for the remote user to access the router. Additionally, there is a duplicate login check box 5050 provided to indicate whether the login/password combination for the router/WAN is the same as the login/password combination for the LAN. By checking this box 5050, the login/password combination entered on the router/WAN side 5010 is automatically entered on the LAN side 5020.

As with the WAN profile configuration dialog box, control buttons are provided for accepting or rejecting the information provided. These control buttons include an "OK" button 265, a "cancel" button 270, and an "apply" button 275.

According to the second embodiment, where a database is used to directly provide the information to the compiler module, the database would preferably have all the information described above with respect to Figures 40 and 50. Specifically, for each record of the database, fields for WAN information, WINS information, and DNS information would preferably be provided. Additionally, a user's login/password information would also be provided.

Referring to Figure 7, a construction of the database that is preferably used with the second embodiment is shown. It should be understood, however, that any method of storing and collecting data can be used, such as a spreadsheet, a text table, or comma separated values.

FORTINET EX1002 Page 329

Additionally, any layout of the database could be used. Preferably, the database will include modules for collecting and storing information needed to generate the executable program by the configuration program generator. For example, there may be a users module 6005, WAN settings 6010 module, ISP module 6015, and an operating system module 6020. The users module 6005 may require, for example, user identification information, user first name information, user last name information, user phone number information. Additionally, it may require user IP address information, user WAN login information, user WAN password information, user LAN login information, and user LAN password information. Additional user information that is not relevant to generating the executable file may also be stored in the database.

The WAN setting module 6010 is preferably configured to store information such as WAN settings identification information, company identification information, ISP identification information, hardware make information, hardware model information, hardware administrative password information, workgroup or domain, network type identification information, server type identification information, IP assignment type identification information, Gateway IP information, WAN IP information and, primary DNS information, secondary DNS information, primary WINS information, secondary WINS information, and WAN setting notes. At a minimum, however, the WAN setting module 6010 should include the information required by the configuration program generator to generate the executable file.

Next, the operating systems module 6020 is preferably configured to store information such as operating system identification information and operating system name. The ISP module 6015 is preferably configured to store information such as ISP identification information, ISP name information, ISP address information, ISP phone information, primary DNS IP information, and secondary DNS IP information.

Other information that may also be provided based on the particular need of the user may include information such as contact information 6025, billing information 6030, employee information 6035, company information 6040, calls information 6045, user calls information 6050, ISP calls information 6055, contact types 6060, and any other pertinent information.

Additionally, the database is preferably a Customer Management Program (CMP). As such, it preferably includes full support and fields for troubleshooting the database. Additionally, the database could include personal information regarding each user to validate the users. Such information could be mother's maiden name, place of birth, Social Security number, or any information that could authenticate a particular user.

Additionally, the database could be configured so that information common to all users would not have to be entered into the database each time a new users added. For example, if all

FORTINET EX1002 Page 330

users in the database will be establishing a VPN connection to the same network, information such as the DNS numbers and the WAN/Gateway address could automatically be inserted into the appropriate fields of the new record. Alternatively, if the database is used to manage a plurality of networks having different configuration settings, all users associated with any given network could be identified (for example by using a company name) as belonging to the same group. When that group identification is provided to the database for a new user, the proper information for that user could automatically be populated into the fields of the database.

Moreover, other information to be automatically inserted into other fields for each record. For example, if it is determined that the client is Microsoft, when the Microsoft client is selected for a new record in the database, the database will automatically insert all associated Microsoft features.

It should be understood that any database configuration or structure can be used, and the particular modules described above need not be present. Moreover, the database can be any type the database, such as SQL or Microsoft Access. Any method of storing some or all of the data necessary to generate the executable files by the configuration program generator of would be suitable. Moreover, in the preferred embodiment, the information from the database is provided directly to the configuration program generator to generate the executable file for any given remote user. This eliminates the need for the network administrator to manually enter the information.

Additionally, when the database is used to generate the e-mail, string tables for the mailer modules are provided. This information is interpreted as an e-mail address.

Next, a description of how a network administrator would manually use the above described system according to the first embodiment is provided. It should be understood that this process could be circumvented by associating the database with the configuration program generator, allowing the network administrator to simply select a user from the database and automatically generate the executable file according to the data in the database, in accordance with the second embodiment.

Referring to Figure 8, using the manual procedure of the first embodiment, a network administrator would first preferably open a dialog box of the configuration program generator, as shown in step 200. This dialog box represents the information collection module. The dialog box preferably includes a plurality of tabs to distinguish between various information screens. The network administrator would then select one of the tabs to determine which information screen would be displayed. Thus, the administrator could choose the WAN profile tab, as shown in step 205, or choose the user profile tab, as shown in step 210.

FORTINET EX1002 Page 331

Depending upon the selected tab, the network administrator would then enter the appropriate information for the information screen that is displayed. Thus, if the administrator had chosen the WAN profile tab in step 205, the administrator would then proceed to enter WAN profile information, as shown in step 215. Alternatively, if the administrator had chosen the user profile tab in step 210, then the administrator would proceed to enter user profile information, as shown in step 220.

In the preferred embodiment, both WAN profile information and user profile information need to be entered. Thus, upon entering information corresponding to one of the information screens, the administrator would next show the other information screen. When information for both information screens have been entered, the administrator would apply the settings to generate the binary data file, as shown in step 225. The binary data file is then used to generate the executable file to be deployed to the remote user.

Additional details for each of the selectable dialog box tabs will be provided next. Figure 9 illustrates the steps to be followed by the network administrator if the network administrator selects the WAN profile tab in step 205 of Figure 8, and Figure 10 illustrates the steps to be followed by the network administrator if the network administrator selects the user profile tab in step 210 of Figure 8. It should be understood that the steps need not necessarily be performed in the sequence shown. For instance, the network administrator can enter the information in any sequence, so long as all necessary information is provided. However, for sake of explanation, a particular sequence is outlined below.

Referring to Figure 9, the network administrator selects the WAN profile tab in the information collection module dialog box. In the preferred embodiment, the dialog box is displayed on a computer monitor, and includes text boxes in which to input various information. The text boxes are labeled with a description of the information to be provided in the associated text box. Additionally, for text boxes that require network addresses, the text boxes are preformatted as blank IP addresses, and with a field size limit for each number to be entered. Thus, it would be impossible to enter and incorrect number format for any given network address.

Next, as shown in step 310, the network administrator first enters a WAN profile number corresponding to the LAN/gateway/router. The WAN number preferably describes the IP address for the router/gateway. This information is used by the remote computer to identify the router/gateway to which it will connect to establish the VPN connection. This number is preferably a static IP address that uniquely identifies the WAN to the outside world.

Next, as shown in step 320, the administrator would identify the type of network configuration of the LAN. For example, the network type could be Novell, NetWare, or Microsoft. It

FORTINET EX1002 Page 332

should be understood that any kind of network environment could be used. For the purposes of example, it will be assumed that Microsoft is selected. By selecting the type, both the client and file/printer sharing our determined.

Next, the administrator would preferably enter the type of the LAN, as shown in step 325. For example, the LAN could be configured as a Server or as a Domain Controller. It should be understood that any LAN configuration can be implemented at this point. If the server type is selected as "Server," as shown in step 340, then the administrator next identifies the workgroup, as shown in step 345. The Workgroup information determines what group of users exchange access to resources on the network. The workgroup information is preferably maintained on the server. Alternatively, if the administrator selects "Domain Controller" as a server type, as shown in step 330, and administrator would be prompted to fill in the domain information, as shown in step 335. In this scenario, the administrator would enter the Domain Controller group name needed to access the network. The domain information is used to uniquely identify a particular user.

The network administrator would next provide the gateway address information for the router/gateway, as shown in step 350. The gateway address is the IP address of the LAN. It may be public, and on the outside world, but may also be private and not known to the outside world. This IP address is for the network to see out from the LAN. Thus, when a user logs on to the network using the VPN connection, that user will access the Internet through the network, as opposed to through his own Internet connection.

Next, as shown in step 355, the administrator would provide the primary and secondary DNS addresses. The DNS (domain name system) is the way that Internet domain names are located and translated into IP addresses. Various lists of domain names and IP addresses are distributed throughout the Internet in an hierarchical structure, rather than maintaining a central list of domain name-to-IP address translations. In the preferred embodiment the administrator would determine the DNS number by querying the ISP. However, an administrator may receive DNS information from any other source. The administrator would also preferably enter a second DNS number as received for the ISP. However, only one DNS number is necessary for the operation.

Next, as shown in step 360 the administrator preferably enters at least one WINS number, and optionally enters a second WINS number as well. The WINS address points to a network location where the Windows Internet Naming Service (WINS) resides. This is typically located on the server, although it could be located on any machine on the network. Additionally, the WINS information is preferably known by the administrator based on the network configuration, although this information can be obtained by the administrator from any other source.

FORTINET EX1002 Page 333

WINS is an operating system based service that manages the association of workstation names and locations with IP addresses. This is done without a user's or an administrator's input. WINS thus automatically creates a mapping entry in a table to map a computer name to an associated IP address. Each computer name on the network is unique. If a computer on the network is moved to another geographic location, the subnet part of the IP address will most likely change. WINS ensures that the new subnet information will be updated automatically in the WINS table. WINS typically works in conjunction with the Dynamic Host Configuration Protocol (DHCP), which negotiates an IP address for any computer when it is first defined to the network.

The administrator next optionally selects an IP assignment from a plurality of IP assignments, as shown in Step 370. The IP assignment to be one of public and private, as shown in steps 371 and 372. Moreover, as shown in steps 375a ~375c, the administrator may select a router option, a server option, and a static IP option.

The IP addresses the remote computer's IP address on the network. The assignment of the IP address can be set by the DHCP router or the DHCP server, or a static IP address can be given by the system administrator. If all zeros are initially used, this typically signals that the DHCP should be prompted to assign an address.

It should be understood that the WAN profile dialog box could prompt the network administrator for additional information. However, in the preferred embodiment, the above information is sufficient. Thus, if the user information has already been provided (under the "user" tab of this configuration dialog box), the network administrator would proceed to generate the user data binary file. However, if the user data information has not yet been provided, the network administrator would select the user information tab to display the user information portion of the information collection module dialog box.

Figure 10 illustrates a method of providing remote user information to the information collection module according to the first embodiment. Thus, referring to Figure 10, the network administrator selects the user profile tab in a dialog box. Once that is selected, a user interface module dialog box appears, which prompts the network administrator to enter user specific information. This information is used to enable the remote user to login to the router/WAN, as well as to login to the LAN. In the preferred embodiment, the information gathered from this dialog box is used to generate the automatic login portion of the executable file. It should be understood that, except for the remote computer's operating system, this information is not necessary to establish the VPN connection; rather, it is used to provide a method of automating the login process to make it easier for the remote user. Thus, if this information is provided, after the remote computer has been configured by running the configuration executable file, a "Dialer" program appears as an

executable file on the remote computer. The remote user can then simply select the dialer program to be automatically connected to the LAN.

In the absence of this information, after the computer is configured for the VPN connection, the user would be faced with several login/password dialog boxes before gaining access to the LAN. For some users, this becomes cumbersome. Consequently, in the preferred embodiment, the network administrator provides the login/password information for the user to the configuration program generator prior to generating the executable file. This information could be provided manually or could be extracted from the database. By providing the login/password information, the configuration program generator is adapted to generate a Dialer program that could be deployed on the remote computer. When the remote user executes the Dialer program on the remote computer, and if the remote computer has been properly configured for the VPN connection, a VPN connection between the remote computer and the local network is automatically established.

It should be understood that the Dialer program could be generated and deployed to the remote computer separately from the network settings executable file. For example, the dialer program could be sent to the remote computer by a separate e-mail, or any other file delivery method. Consequently, should the login/password combinations for the remote user change at any time, the network administrator could provide a new dialer program having the revised login/password information. Additional information regarding the Dialer is provided hereinbelow.

Referring again to Figure 10, the network administrator first enters the LAN IP address, as shown in step 410. This information preferably corresponds to the LAN that the remote user will access. Next, as shown in step 420, the administrator enters the remote user's login name and password for the router/WAN. Additionally, the network administrator enters the remote user's login name and password for the LAN, as shown in step 430. It should be understood that if this login/password combination is identical to the router/WAN login/password, the administrator can simply select a check box indicating "duplicate login." By doing this, the login/password information for the LAN is automatically copied from the router/WAN information.

Finally, in step 440, the administrator identifies the operating system that the remote computer is using. This is necessary for the executable configuration program to properly modify the operating system parameters to establish the VPN connection. In the preferred embodiment, Windows XP, Windows 2000, Windows ME, or Windows 98 appear in a drop-down menu box. However, it should be understood that any operating system could be selected, including UNIX or LINUX, or any successor to the Windows family of operating systems. Moreover, and the preferred embodiment, a single executable files will work with all supported offering systems.

FORTINET EX1002 Page 335

If the network information has already been provided (under the "WAN profile" tab of this configuration dialog box), the network administrator would proceed to generate the user data binary file. However, if the network information has not yet been provided, the network administrator would select the "WAN profile" tab to display the network information portion of the information collection module dialog box.

The user data binary file is then used when generating the executable file. This information is interpreted by the remote computer so as to configure the remote computer for establishing a secure Internet connection to the LAN. The secure Internet connection between the remote computer and the LAN is the Virtual Private Network (VPN). In a preferred embodiment, Point-to-Point Tunneling Protocol (PPTP) is used for establishing the VPN connection. PPTP is a Layer 2 tunneling protocol which allows the remote computer to use a public IP network to communicate securely with the local computer (for example, the LAN server). PPTP thus essentially tunnels the IP. A VPN "tunnel" between the LAN and the remote computer allows traffic to flow securely across the Internet. The PPTP tunnel is preferably established using the Dial-Up Networking functions of the Windows operating system. Remote users are preferably authenticated using MS-CHAP against a user/password list maintained. Other authentication schemes, however, could be used. PPTP is described in RFC 2637, "Point-to-Point Tunneling Protocol (PPTP)," which is incorporated herein by reference. Consequently, in the preferred embodiment, the Dial-Up Networking aspects of Windows are manipulated by the executable file. For example, the RAS phonebook entries could be modified or registry entries pertaining to Dial-Up Networking could be modified.

Alternatively, IPSec could be used instead of PPTP. IPSec includes a series of protocols to handle data integrity and confidentiality when transmitting secure data across the Internet. A first protocol, the Authentication Header (AH) protocol handles data integrity, and a second protocol, the Encapsulated Security Payload (ESP) protocol, resolves both data integrity and confidentiality issues.

Each VPN tunnel created with IPSec is preferably assigned a specific Security Parameter Index (SPI) to differentiate it from other VPN tunnels configured on router/gateway. An SPI is an arbitrary, 32-bit number that tells the receiving device which group of security protocols (such as algorithms, keys and their longevity) the remote user is using for communication.

IPSec is described in RFC 2401, "Security Architecture for the Internet Protocol," and RFC 2709, "Security Model with Tunnel-mode IPsec for NAT Domains," which are incorporated herein by reference. The same general theory would apply to IPsec as applies to PPTP with respect to configuring the remote computer to establish the VPN connection.

FORTINET EX1002 Page 336

Additionally, it should be understood that the configuration method described herein can be applied to any communication protocol. For example, in addition to PPTP and IPsec, L2TP could also be used, or any other protocol, especially any other tunneling protocol.

Additional information concerning the Dialer program is next provided.

The Dialer program is a application that functionally performs dialing functions using any operating system. According to the preferred embodiment, its calls dialing functions contained with Microsoft "Dial-up Networking" contained within Microsoft Windows versions 95/98/ME and "Network and Dial-up Connections" within Microsoft Windows versions 2000/XP. The Dialer preferably assist in the operation of the connection method described herein by providing navigation for the user, and it binds user announcements when activating a connection. For example, it provides a user with the ability to activate a VPN connection using a single "click" of a mouse.

Additionally, the dialer can assist in providing various be security parameters within a remote access solution. For example, when making a connection "active" a user must provide information that validates that user for security features. This provides protection of both the "Caller" (the remote user making a secure connection) and the "Callee" (the network topology with this remote access feature). Every secure VPN or network connection requires some form of verification. The Dialer provides a module for both user verification, as well as connection activation.

The Dialer preferably makes user navigation easier. When the user initiates and starts a connection to get to a destination network, at least one, and typically several connections need to occur to access the network.

For example, a user may first need to access the Internet. After the Internet connection is established, the user or the VPN might possibly need to initiate a connection "directly" to the device that holds the parameters of how that user is going to "talk" (i.e. communicate) to the network topology. This includes encapsulation and authentication, i.e. the WAN Profile of the Callee. The third connection is necessary to access the network structure, for example to join the "Network Neighborhood," from the remote location. This is performed by the internal validation (user accounts and privileges) within the network topology, and preferably occurs within a network server or appliance when a new connection is established or sensed by the network server or appliance.

Pending on the number of network servers or appliances and security parameters within a network topology, each server can require a different validation of the same server. The Dialer eliminates the second of the stated connections because when the user has some or any

FORTINET EX1002 Page 337

connection to the Internet, the Dialer brings the "Caller" through the Internet to the "Callee" using a single "click."

To perform these functions, the Dialer preferably contains all the required announcements and authentications the user needs to both start and complete a secure connection to the network. Thus, the dialer contains programming code configured to select and initiate a specific dialing function. For example, the dialer can be configured to select and initiate a specific "RAS phonebook entry" that has been created using the above described configuration process.

Additionally, the Dialer replaces the "default" announcement program that is bound to any connection profile built in the operating system's dialing functions. For example the dialer would replace the connection profile contained in the "Dial-up Networking" contained within Microsoft Windows versions 95/98/ME, and would replace the "Network and Dial-up Connections" within Microsoft Windows versions 2000/XP.

By using the Dialer, user does not need to know the user's particular login and password combination to access the WAN of the network. Additionally, the Dialer will not work on any RAS phonebook entry that is not a match to the corresponding label. In doing this the dialer can direct both security and how the user connects because without the Dialer no connection can or would be made.

In the preferred embodiment, the Dialer is built from the user settings index within the database. Additionally, it is specific to the WAN Login and WAN password for a particular user. At both input fields the remote access engineer can configure and design a custom Dialer that is very complex containing a series of numbers, letters and characters, completely random" and unknown to the user. However, because this information is known to the dialer, access will be granted to the network.

Thus, when the remote computer executable configuration file is generated to establish the VPN connection, the network administrator preferably deploys the executable file to the remote user. This can be done by any method of transferring data, including attaching the program to an e-mail or providing on a computer readable medium. Additionally, if a Dialer executable program has been generated, it can be deployed simultaneously with the configuration executable file. It should be understood, however, that each of these executable files can be deployed separate and apart from the other executable file. For example, if a user is required to change a login/password combination according to a prescribed time schedule, the network administrator could deploy the dialer executable program to the remote user with the updated login/password combination at the appropriate time. When the remote user executes this updated program, the login/password settings on the remote computer are updated. Additionally, according to the preferred embodiment,

the executable configuration file is self deleting. That is, upon execution on the remote computer, after the remote computer is fully configured the executable file is automatically deleted from the remote computer. Alternatively, the dialer program could be set up to search for the configuration program the first time the dialer program is executed. If the configuration program is found, than the dialer program could be configured to automatically delete the configuration program.

Moreover, and order to enhance security, the configuration and dialer programs to be deployed to the user can stored within a removable USB key-type memory device that is provided to the user. Referring to Figure 11, the USB key-type memory device 8010 is a small portable single piece device that plugs into a USB port of a computer using the USB interface connector 8020. The USB key-type memory device 8010 preferably includes an electronically erasable read-only memory (EEPROM) 8030. The USB key also preferably includes a flash RAM 8040. The EEPROM 8030 is preferably a locked EEPROM section, which prevents users from accessing information stored therein. The flash RAM 8040 is a general storage area, which emulates a disk/hard drive. The EEPROM 8030 can be write protected all the flash RAM 8040 is for storing general data. The USB key-type memory device 8010 further includes a USB controller 8050 to control the device.

Because the EEPROM 8030 is inaccessible to users, the can be used to store verification and/or encryption information. According to the preferred embodiment, before the configuration program or the dialer program can be run, whether from a hard drive, a remote disk, or the flash RAM 8040, the program would first query the EEPROM to authenticate the user. Thus, if the USB key-type memory device 8010 is not coupled to the USB port of the computer, neither the configuration program or the dialer program will work.

Thus, the dialer program and configuration program could initially be stored to the file structure section of the removable key. These programs could be run directly from the key, or could be copied to a hard drive and run from there. However, without the USB key being inserted into the USB drive, the programs would not operate.

Specifically, as part of the configuration program and the dialer program, a special code could be incorporated that requires the program to access the EEPROM 8030 of the USB key 8010. Within that EEPROM 8030, a password could be stored that would authenticate the dialer program and/or the configuration program.

To generate the USB key 8010, the administrator would first access the EEPROM 8030 of the USB key 8010 to program a password that would be used by another program. Accordingly, it would not be necessary for the remote user to even know the password; rather the programs to be executed in automatically query for the password. The executable program, in order to run, would

FORTINET EX1002 Page 339

need to verify the existence and authenticity of the password on the EEPROM 8030 of the USB key 8010.

The executable programs, for example the dialer program or the configuration program, can be stored in the flash RAM 8040 of the USB key 8010. When the dialer program is run, it would first query the EEPROM 8030 to determine if the password stored in the EEPROM 8030 is identical to that which is required by the dialer program. If the password matches, than the program will run. Otherwise, no connection can be made to the VPN. Even if the dialer program is copied to the hard drive, a would still require the authentications through the USB key. Thus, if the dialer program is copied to a hard drive other than the USB key 8010, it will not operate unless the USB key 8010 is installed on the system.

Moreover, and order to protect the key for being stolen, a further layer of security could be used that requires the user to enter a password to authenticate the user prior to authenticating the key. Moreover, the dialer program could be encrypted, when the decryption key being stored in the EEPROM 8030 of the USB key 8010. Thus, would be very difficult, if not impossible, for someone to modify the dialer program to run without use of the USB key 8010. It should be understood that the configuration generator program can also be so encrypted. Additionally, the information on the EEPROM 8030 could also be encrypted.

Additionally, because the installer program is intended to be run once while the dialer program is intended to be run every time a VPN connection is desired, each of the two programs could have a unique password stored on the EEPROM 8030. When the installer program is run, it would call for the associated password stored on the EEPROM 8030. After installation, it would preferably erase that password. Consequently any further attempt to run the installer program would fail for lack of authentication. Meanwhile, the dialer program would have a different password associated with it on the EEPROM 8030. Accordingly, when the dialer program is run it would first query the associated password on the EEPROM to determine the authenticity of the key. If the password were found, then the dialer program would proceed to establish a connection to the server.

The system and method for automatically configuring a remote computer according to the preferred embodiment has various advantages. For example, it allows a network administrator to easily configure remote computers by generating a single executable file that can be provided to the remote user for execution. By doing this, the network administrator can save much time and can more actively manage the network. Additionally, any portion of a remote user's computer can be remotely configured by using an application program designed to manipulate the registry of the remote computer. Consequently, anyone with the need to remotely modify the configuration

settings of a computer can generate an executable file to be run on the remote computer to accomplish the configuration update. Additionally, by having a conduit from a database to the program modules, it becomes easy to generate a large number of such executable files in a short period of time. This allows for efficient management of remote users.

Moreover, according to the preferred embodiment, the remote user's computer is seen as a gateway in establishing the VPN connection to the host/local computer. Accordingly, because a VPN connection is typically established between gateways, it is possible to automatically establishing VPN connection between the local computer's gateway and the remote computer directly. Thus the remote computer essentially becomes a router.

The foregoing embodiments and advantages are merely exemplary and are not to be construed as limiting the present invention. The present teaching can be readily applied to other types of apparatuses. The description of the present invention is intended to be illustrative, and not to limit the scope of the claims. Many alternatives, modifications, and variations will be apparent to those skilled in the art. In the claims, means-plus-function clauses are intended to cover the structures described herein as performing the recited function and not only structural equivalents but also equivalent structures.

FORTINET EX1002 Page 341

WHAT IS CLAIMED IS:

1. A method of configuring a remote computer to access a network of computers, comprising:

initiating an installer program having an empty binary file, the installer program being configured to generate an executable installation program using the binary file;

generating a user data binary file including data necessary to configure the remote computer to access the network;

replacing the empty binary file with the user data binary file and generating the executable installation program using the user data binary file; and

executing the executable installation program on the remote computer to modify configuration settings of the remote computer such that the remote computer is configured to access the network.

2. The method of claim 1, wherein the executable installation program is e-mailed to the remote computer to be executed on the remote computer.

3. The method of claim 1, further comprising storing the executable file on a computer readable medium prior to execution of the executable file to provide the executable file to the remote computer for execution.

4. The method of claim 3, wherein the computer readable medium comprises a universal serial bus (USB) data storage peripheral having first and second storage areas, the first area being an electronically erasable read-only memory (EEPROM) storage area and the second storage area being a flash RAM storage area.

5. The method of claim 4, wherein the first storage area is a secure storage area which is an accessible to a user of the USB data storage peripheral, and wherein the second storage area comprises a general storage area, which emulates a disk/hard drive, wherein the executable file is stored in the second storage area.

6. The method of claim 5, wherein an encryption key is stored in the first storage area, and wherein the executable file searches the first storage area for a prescribed authentication key before it can be executed by a user.

FORTINET EX1002 Page 342

7. The method of claim 6, wherein the modified configuration settings of the remote computer comprise a setting that requires the remote computer to access the first storage area of the USB data storage peripheral prior to accessing the network.

8. The method of claim 6, wherein the remote computer cannot access the network if the encryption key within the first storage area cannot be accessed by the remote computer.

9. The method of claim 1, wherein the user data binary file comprises an IP address of a router coupled to the network of computers, a gateway address of the router, at least one DNS address, and at least one WINS address.

10. The method of claim 9, wherein the user data binary file further comprises and identification of an operating system used by the remote computer and an identification of an operating system of the network of computers.

11. The method of claim 10, wherein the user data binary file further comprises at least one login and password necessary for the remote computer to access the network of computers.

12. The method of claim 1, wherein the user data binary file is generated by an user data application that receives network information needed by the remote computer to gain access to the network.

13. The method of claim 12, wherein the user data application prompts an operator of the network for the network information, and generates the user data binary file upon a command of the operator.

14. The method of claim 12, wherein the user data application extracts the network information from a database containing relevant configuration information for the remote computer.

15. The method of claim 12, wherein the user data application is one of an OCX and ActiveX application.

FORTINET EX1002 Page 343

16. The method of claim 15, wherein the user data application is configured to run with at least one of a commercial database application, a commercial spreadsheet application, and a commercial word processor application.

17. The method of claim 15, wherein the prescribed RAS settings configure the remote computer to establish a VPN connection with the network.

18. The method of claim 1, wherein the executable installation program installs prescribed Remote Access Service (RAS) settings on the remote computer, and wherein the prescribed RAS settings are adapted to allow the remote computer to access the network.

19. A method of configuring a remote computer to access a network of computers, comprising:

accessing a database having networking information necessary for at least one remote computer to access the network of computers, including a WAN profile for the network of computers, at least one DNS address for the network of computers, and at least one WINS address for the network of computers;

executing a software module from within the database, the software module configured extract the networking information for a selected one of the at least one remote computer;

converting the extracted networking information to a binary code representing configuration settings for the selected one of the at least one remote computer;

generating an executable program having the binary code embedded therein, the executable program being configured to modify a current configuration of the selected one of the at least one remote computer when executed by the remote computer; and

providing the executable program to the selected one of the at least one remote computer for execution.

20. The method of claim 19, wherein providing the executable program comprises at least one of e-mailing the executable program to the remote computer, transferring the executable program to a magnetic storage device, transferring the executable program to an optical disc, and loading the executable program onto a web site for download by the remote computer.

FORTINET EX1002 Page 344

21. The method of claim 20, wherein the magnetic storage device comprises a universal serial bus (USB) data storage peripheral having first and second storage areas, the first area being an electronically erasable read-only memory (EEPROM) storage area and the second storage area being a flash RAM storage area.

22. The method of claim 21, wherein the first storage area is a secure storage area which is an accessible to a user of the USB data storage peripheral, and wherein the second storage area comprises a general storage area, which emulates a disk/hard drive, wherein the executable file is stored in the second storage area.

23. The method of claim 22, wherein an encryption key is stored in the first storage area, and wherein the executable file searches the first storage area for a prescribed authentication key before it can be executed by a user.

24. The method of claim 23, wherein the modified configuration settings of the remote computer comprise a setting that requires the remote computer to access the first storage area of the USB data storage peripheral prior to accessing the network.

25. The method of claim 22, wherein the remote computer cannot access the network if the encryption key within the first storage area cannot be accessed by the remote computer.

26. The method of claim 19, wherein the networking information further comprises a login and password combination necessary for the selected one of the at least one remote computer to access the network of computers and an IP address for the network of computers.

27. The method of claim 26, wherein the networking information further comprises a login and password combination necessary for the selected one of the at least one remote computer to access a router/gateway that couples the network of computers to the Internet.

28. The method of claim 27, wherein the networking information further comprises an identification of an operating system used by the selected one of the at least one remote computer.

29. The method of claim 19, wherein the executable file is configured to modify a registry of the selected one of the at least one remote computer to insert the information necessary for the remote computer to access the network of computers.

30. The method of claim 29, wherein the executable file is configured to modify RAS phonebook entries of the remote computer for establishing a virtual private network (VPN) with the network of computers.

31. The method of claim 29, wherein the executable file is configured to modify dial-up networking settings of an operating system of the remote computer necessary to establish a secure Internet connection between the remote computer and the network of computers.

32. A method of configuring a remote computer, comprising:

accessing a database having configuration information necessary to configure at least one remote computer according to a user's preferences;

executing a software module associated with the database, the software module configured extract the configuration information from the database for a selected one of the at least one remote computer;

converting the extracted networking information to a binary code representing configuration settings for the selected one of the at least one remote computer;

generating an executable program having the binary code embedded therein that will modify a current configuration of the selected one of the at least one remote computer when executed by the remote computer; and

providing the executable program to the selected one of the at least one remote computer for execution.

33. The method of claim 32, wherein providing the executable program to the selected one of the at least one remote computer comprises e-mailing the executable program to the remote computer, transferring the executable program to a computer readable magnetic medium, transferring the executable program to a computer readable optical medium, and loading the executable program onto a web site for download by the remote controller.

34. The method of claim 32, wherein the configuration information comprises an identification of an operating system of the selected one of the at least one remote computer.

FORTINET EX1002 Page 346

35. The method of claim 32, wherein the configuration information comprises application program settings, and wherein the executable program is configured to modify a registry of the remote computer.

36. A method of modifying configuration settings of a remote computer; comprising:

determining configuration settings necessary for a remote computer to perform a prescribed operation;

generating a binary file representing the configuration settings for the remote computer;

generating an executable program having the binary code embedded therein that will modify a current configuration of the remote computer when executed by the remote computer; and

deploying the executable program to the remote computer for execution.

37. The method of claim 36, wherein the executable file is configured to modify a registry settings of the remote computer to effect the configuration modification.

38. A method of configuring a remote computer to access a network of computers, comprising:

executing a software module that is configured to prompt a system administrator for configuration settings of the remote computer to access the network of computers;

receiving the configuration setting provided by the system administrator through the software module;

converting the configuration settings received through the software module to a binary code representing the configuration settings;

generating an executable program that will modify a current configuration of the remote computer when executed by the remote computer, the executable program having the binary code embedded therein; and

providing the executable program to the remote computer for execution.

FORTINET EX1002 Page 347

39. A computer readable medium having stored thereon a sequence of instructions which, when executed by a processor, cause the processor to perform a sequence of steps, comprising:

initiating an installer application having an empty binary file, the installer application being configured to generate an executable installation program using the binary file;

generating a user data binary file including data necessary to configure the remote computer to access the network;

replacing the empty binary file with the user data binary file and generating the executable installation program using the user data binary file; and

storing the executable installation program on a storage medium to be run by the remote computer to modify configuration settings of the remote computer such that the remote computer is configured to access the network.

40. A method of configuring a remote computer to establish a secure connection to a local computer, comprising:

determining configuration settings required by a remote computer to access a local computer;

converting the configuration settings required by the remote computer to a binary code representing the configuration settings; and

generating an executable program that will modify a current configuration of the remote computer when executed by the remote computer, the executable program having the binary code embedded therein.

41. The method of claim 40, further comprising providing the executable program to the remote computer for execution.

42. The method of claim 40, wherein the configuration settings are determined by a network system operator and manually keyed into a conversion application, the conversion application being configured to convert the configuration settings to the binary code representing the configuration settings.

43. The method of claim 42, wherein the conversion application comprises a software module configured to be integrated with at least one of a database application software and a spreadsheet application software.

FORTINET EX1002 Page 348

44. The method of claim 42, wherein the executable program is further configured to establish an auto-dialer feature that automatically establishes a connection with the ISP and automatically provides a user name and password to provide an automatic login to the network.

45. The method of claim 40, wherein the current configuration to be modified by the executable program comprises at least one of RAS entries, a windows registry and Windows Phone Book files.

46. The method of claim 40, wherein the executable program is automatically deleted from the remote computer upon its execution by the remote computer.

47. The method of claim 40, wherein the configuration settings required by the remote computer comprise at least one DNS number, at least one WINS address, and a WAN profile of a gateway coupled to the local computer.

48. The method of claim 40, wherein the local computer comprises a gateway/router and a local area network (LAN).

FORTINET EX1002 Page 349

Figure 1

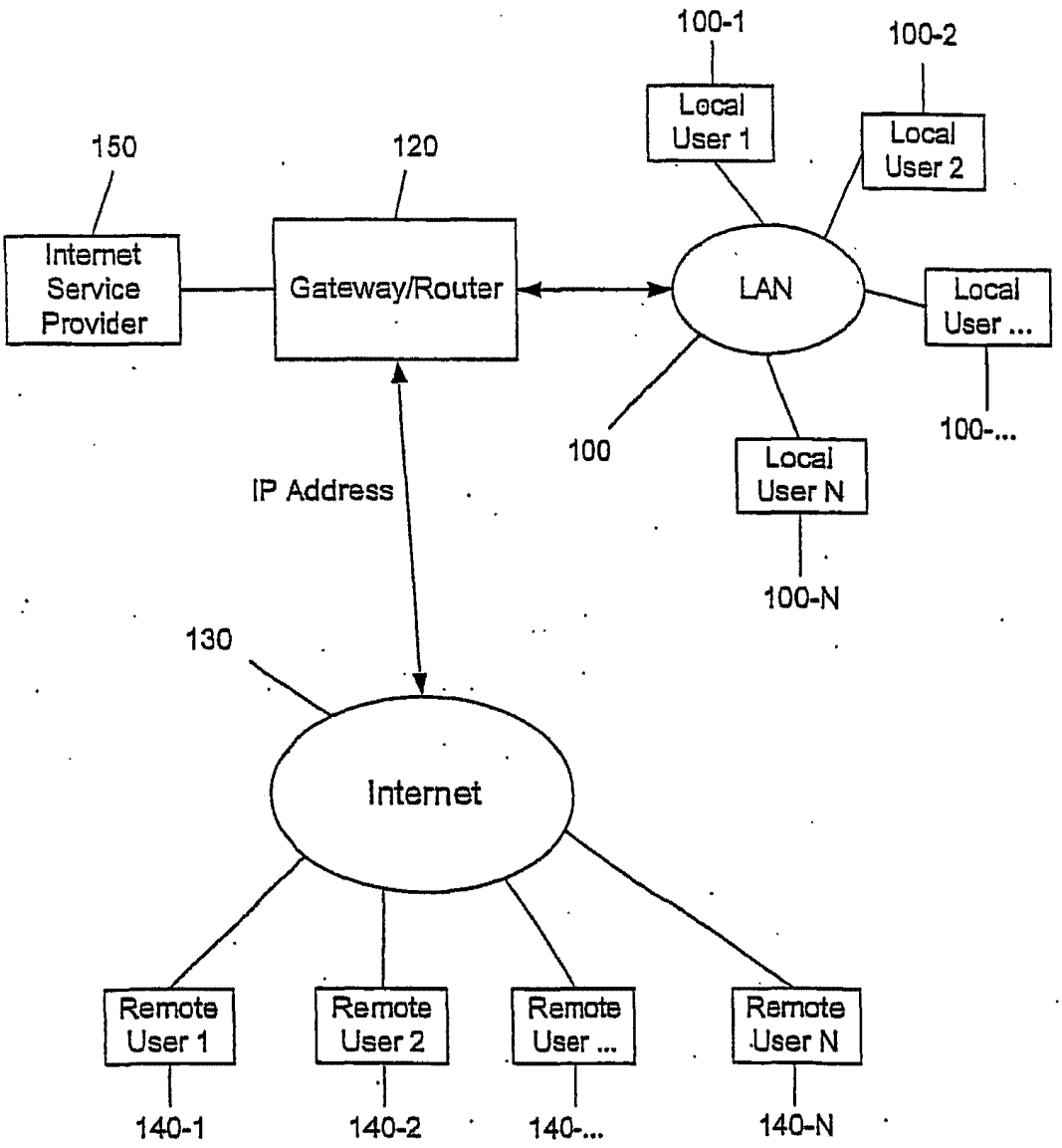

100-1
100-2
Local User 1
Local User 2
150
120
Internet Service Provider
Gateway/Router
LAN
Local User ...
100
100-...
Local User N
IP Address
100-N
130
Internet
Remote User 1
Remote User 2
Remote User ...
Remote User N
140-1
140-2
140-...
140-N

Figure 2

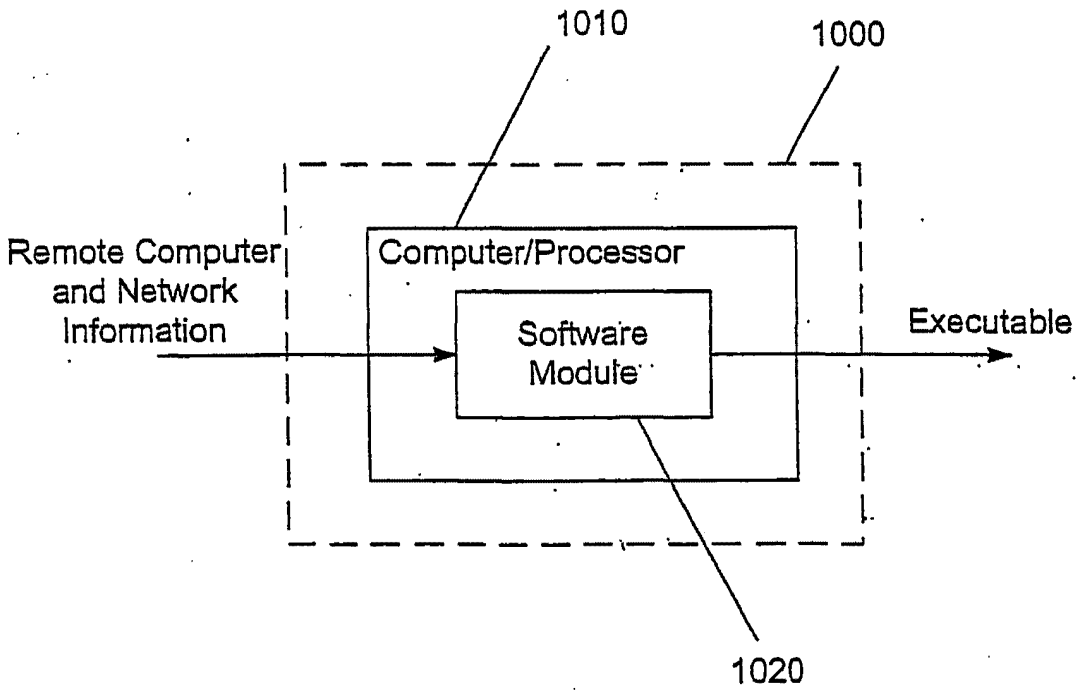

1010
1000
Remote Computer and Network Information
Computer/Processor
Software Module
Executable
1020

Figure 3

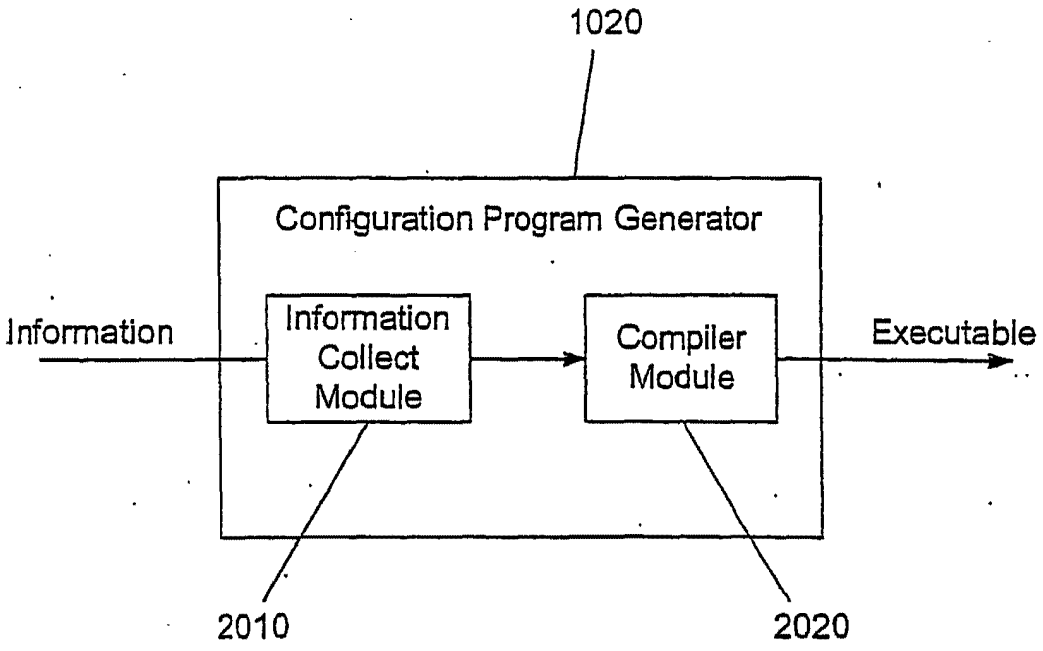
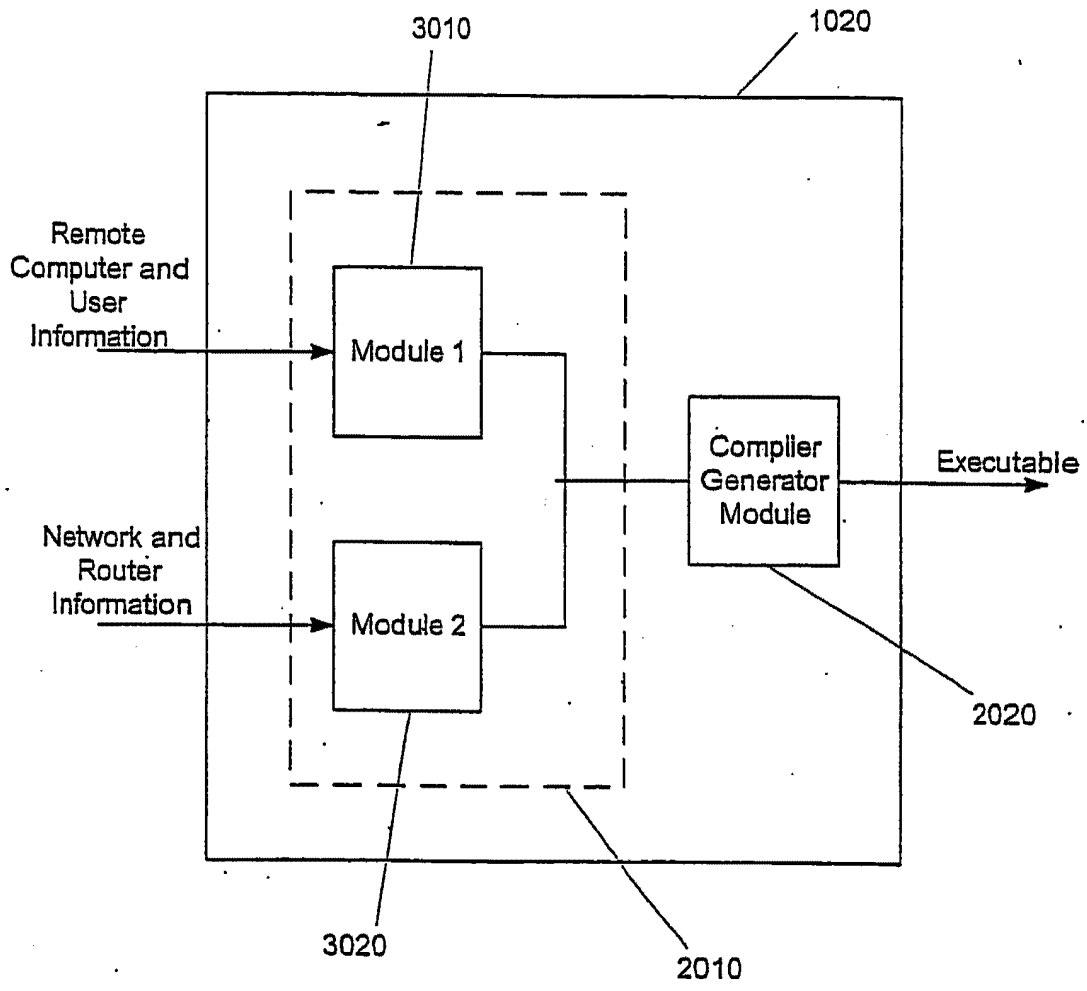

1020
Configuration Program Generator
Information
Information Collect Module
Compiler Module
Executable
2010
2020

Figure 4


3010
1020
Remote Computer and User Information
Module 1
Compiler Generator Module
Executable
Network and Router Information
Module 2
2020
3020
2010

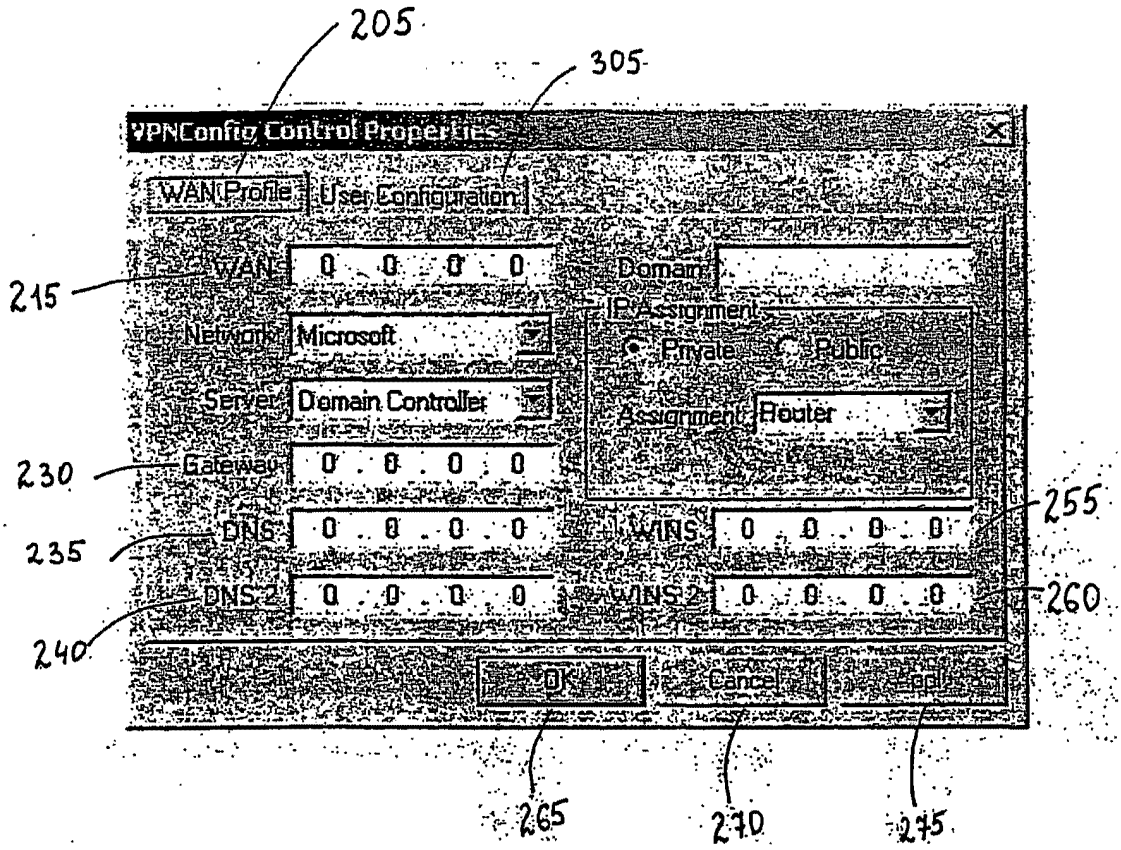

205
305
VPNConfig Control Properties
WAN Profile
User Configuration
WAN
0 0 0 0
Domain
215
IP Assignment
Network
Microsoft
Private
Public
Server
Domain Controller
Assignment
Router
230
Gateway
0 0 0 0
255
235
DNS
0 0 0 0
WINS
0 0 0 0
DNS 2
0 0 0 0
WINS 2
0 0 0 0
260
240
OK
Cancel
Apply
265
270
275

Figure 5

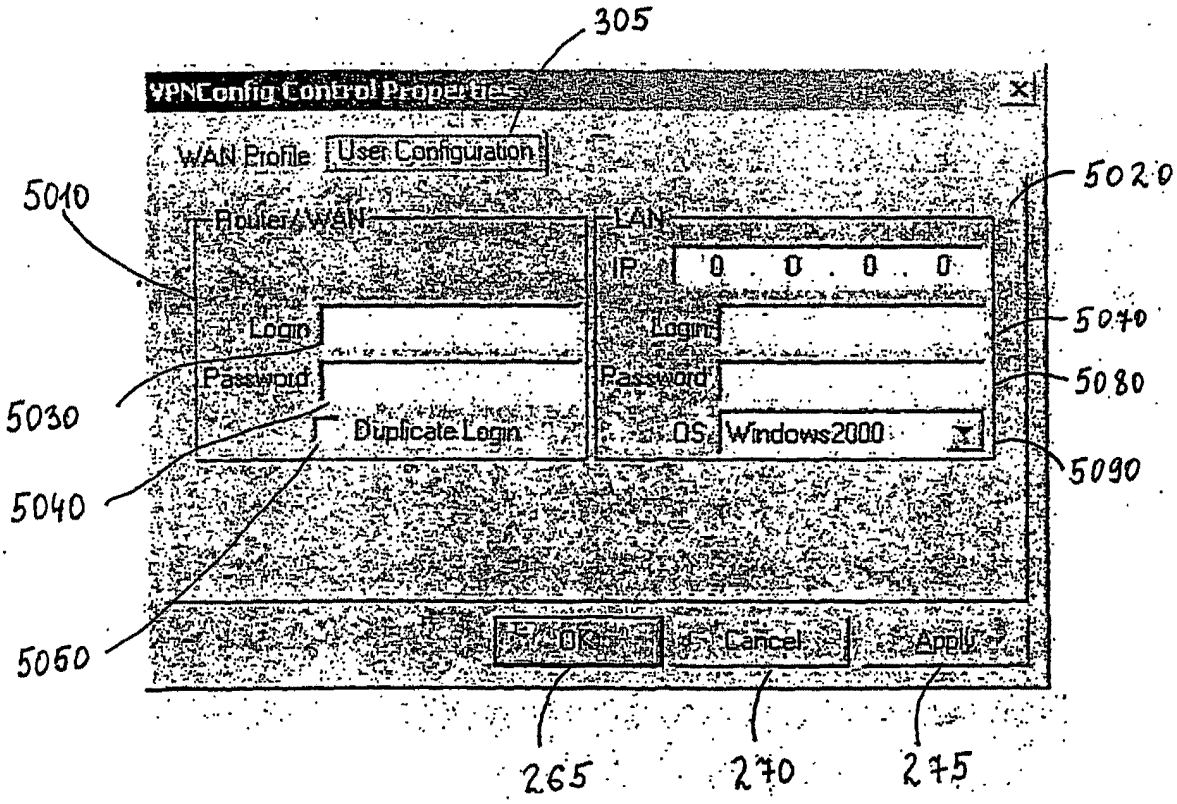

305
VPNConfig Control Properties
WAN Profile
User Configuration
5010
Router/WAN
Login
Password
Duplicate Login
5030
5040
5060
LAN
IP
0 . 0 . 0 . 0
Login
Password
OS
Windows2000
5020
5070
5080
5090
OK
Cancel
Apply
265
270
275

Figure 6

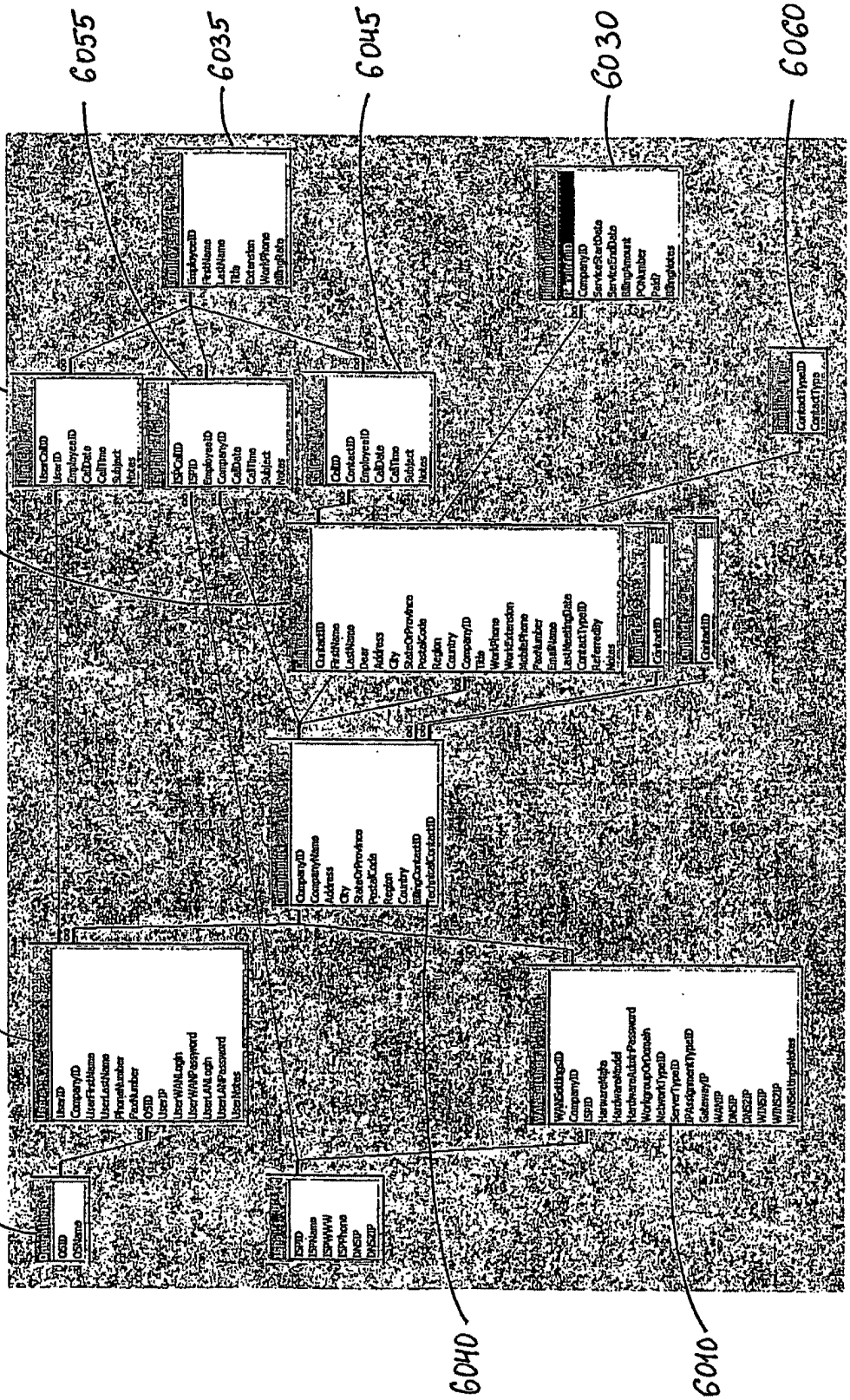


Figure 1

Figure 8

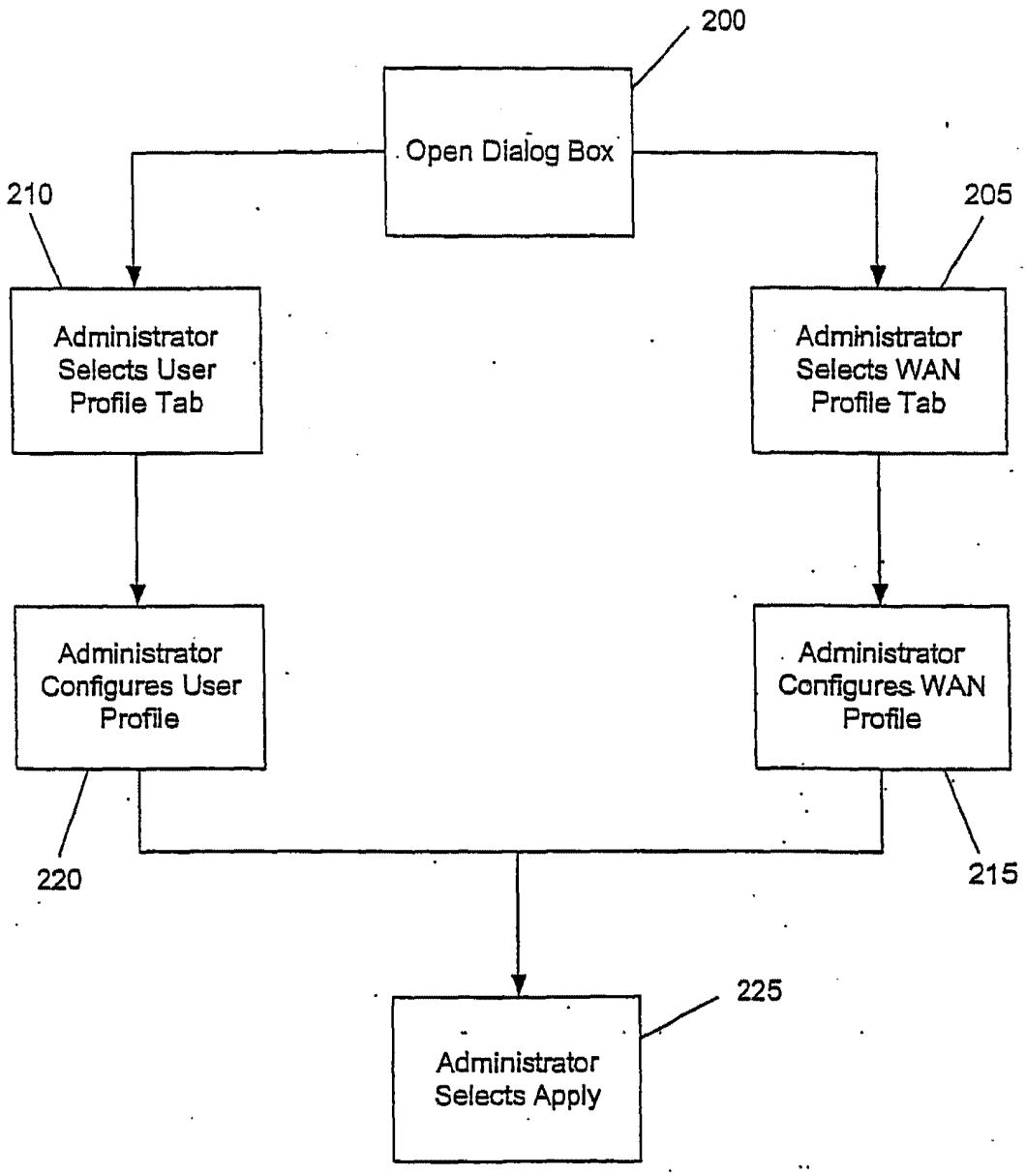

200
Open Dialog Box
210
205
Administrator Selects User Profile Tab
Administrator Selects WAN Profile Tab
Administrator Configures User Profile
Administrator Configures WAN Profile
220
215
225
Administrator Selects Apply

Figure 9

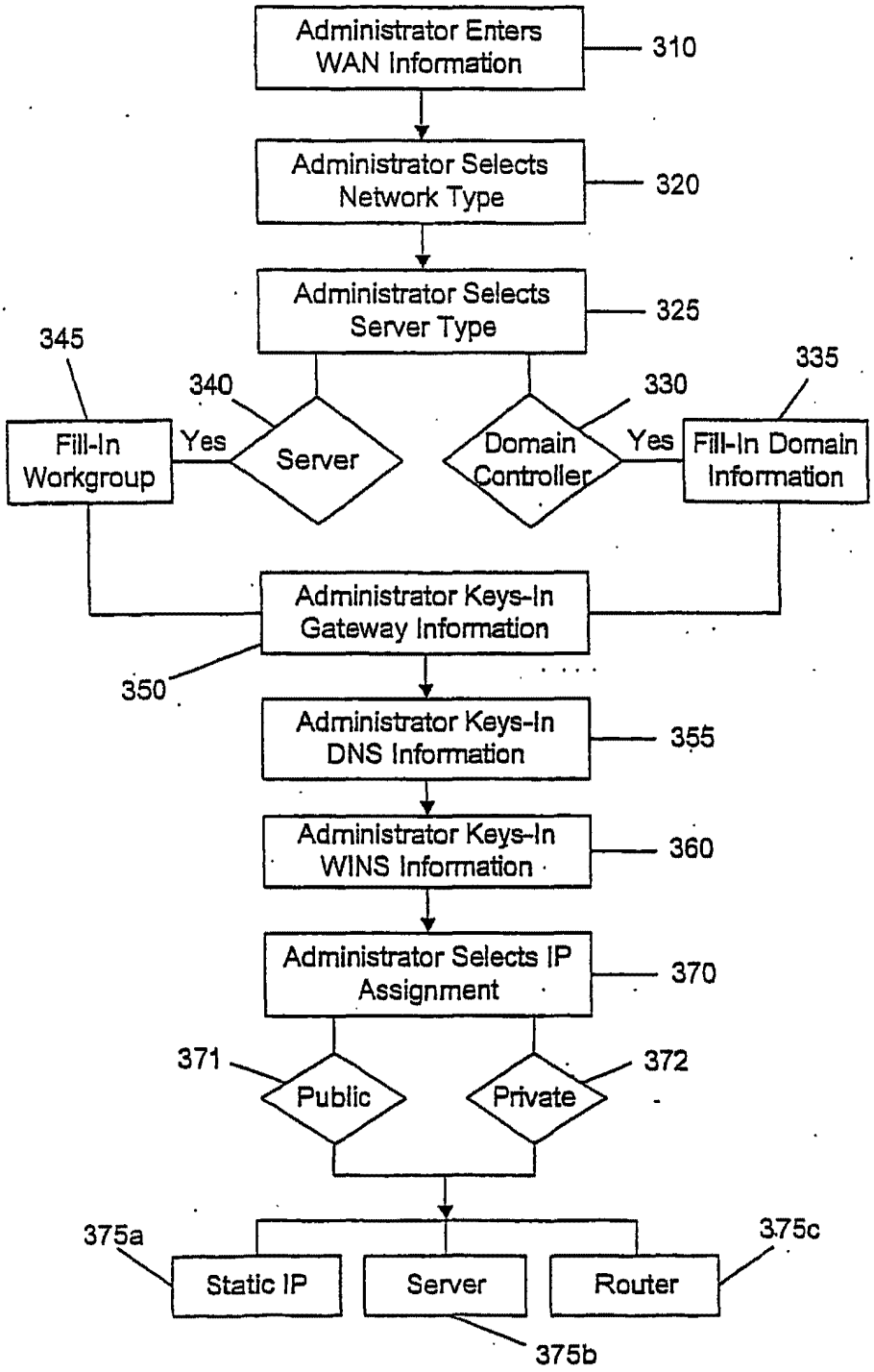
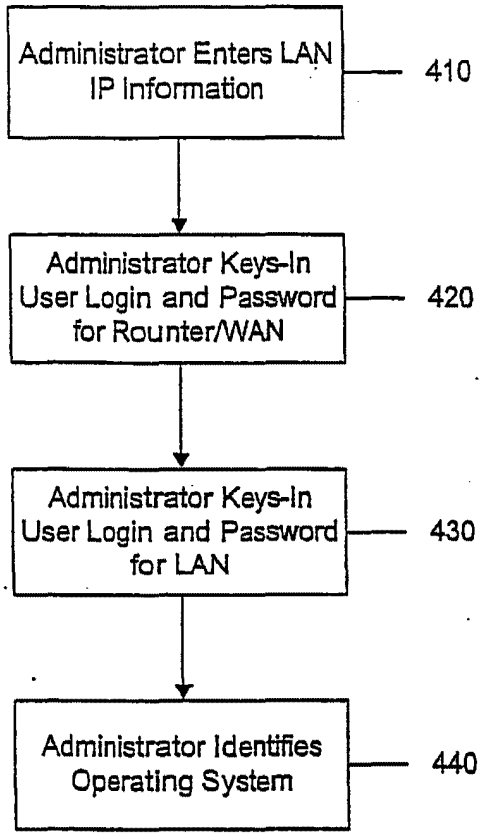

Administrator Enters WAN Information
310
Administrator Selects Network Type
320
Administrator Selects Server Type
325
345
340
330
335
Fill-In Workgroup
Yes
Server
Domain Controller
Yes
Fill-In Domain Information
Administrator Keys-In Gateway Information
350
Administrator Keys-In DNS Information
355
Administrator Keys-In WINS Information
360
Administrator Selects IP Assignment
370
371
372
Public
Private
375a
375c
Static IP
Server
Router
375b

Figure 10


Administrator Enters LAN IP Information
410
Administrator Keys-In User Login and Password for Rounter/WAN
420
Administrator Keys-In User Login and Password for LAN
430
Administrator Identifies Operating System
440

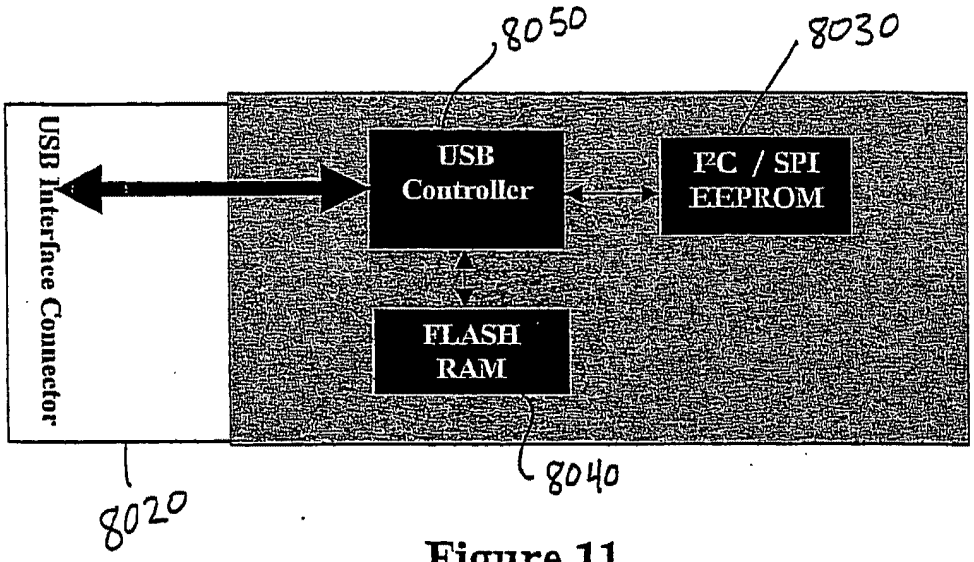


Figure 11

8010

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/13407

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 15/177, 13/00
US CL :709/222; 710/104
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/202, 220, 221, 222; 710/8, 104; 713/200, 201, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,108,420 A (LAROSE et al.) 22 AUGUST 2000 ABSTRACT, Column 3, Lines 5-56, Column 5, Lines 33-60, Column 6, Lines 55-67	1-48
Y	US 6,295,556 B1 (FALCON et al.) 25 SEPTEMBER 2001 ABSTRACT, Column 1, Line 50 THROUGH Column 2, Line 24, Column 3, Line 18 through Column 7, Line 67	1-48
A, P	US 6,493,751 B1 (TATE et al) 10 DECEMBER 2002 Entire document	1-48
A	US 6,324,690 B1 (LUU) 27 NOVEMBER 2001 Entire document	1-48

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
08 AUGUST 2003	26 AUG 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer for MARC THOMPSON James R. Matthews Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/13407

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

EAST USPAT/EPO text serach; IEEE, ACM non-patent literature text search
Terms: installation/configuration program, VPN configuration, netowkr computer configuration, WINS, RAS, USB, WAN profile, gateway

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2004 (22.04.2004)

PCT

(10) International Publication Number
WO 2004/034229 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/032268

(22) International Filing Date: 10 October 2003 (10.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/417,674 10 October 2002 (10.10.2002) US

(71) Applicant *(for all designated States except US)*: **ROCKSTEADY NETWORKS, INC.** [US/US]; 3410 Far West Blvd., Suite 210, Austin, TX 78731 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MACKINNON, Richard** [US/US]; 4201 Speedway, Austin, TX 78751 (US). **LOONEY, Kelly** [US/US]; 10737 Chestnut Ridge, Austin, TX 78726 (US). **WHITE, Eric** [US/US]; 1717 Bartoncliff Drive, Austin, TX 78704 (US).

(74) Agent: **ADAIR, John, L.**; Gray Cary Ware & Freidenrich, LLP, 1221 South MoPac Expressway, Suite 400, Austin, TX 78746 (US).

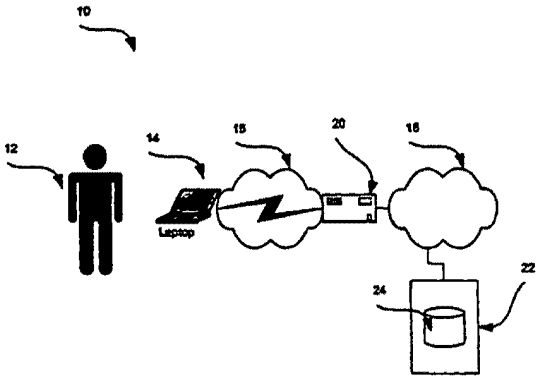
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL



(57) Abstract: More particularly, one embodiment of the present invention provides a system of providing network access comprising a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media, executable by the processor. In one embodiment of the present invention, the computer instructions can be executable to receive a network communication over the first network interface from a user using a user device and determine if the network communication is associated with an authenticated user. If the network communication is not associated with an authenticated user, the computer instructions can be executable to direct the user to an authentication interface. The computer instructions can be further executable to receive credentials from the user and authenticate the user based on the credentials. Another embodiment of the present invention can include a system for providing access to a network that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media. The computer instructions can be executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

WO 2004/034229 A2

DESCRIPTION

SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL

TECHNICAL FIELD

Embodiments of the present invention relate to network access. More particularly, embodiments of the present invention relate to providing access control for a shared network.

BACKGROUND

The communication of data over networks has become an important, if not essential, way for many organizations and individuals to communicate. The Internet is a global network connecting millions of computers using a client-server architecture in which any computer connected to the Internet can potentially receive data from and send data to any other computer connected to the Internet. The Internet provides a variety methods in which to communicate data, one of the most ubiquitous of which is the World Wide Web. Other methods for communicating data over the Internet include e-mail, usenet newsgroups, telnet and FTP.

Users typically access the Internet either through a computer connected to an Internet Service Provider ("ISP") or computer connected to a local area network ("LAN") provided by an organization, which is in turn, connected to the ISP. The ISP provides a point of presence to interface with the Internet backbone. Routers and switches in the backbone direct data traffic between the various ISPs.

To access a LAN and, in turn, the Internet, many prior art access control systems require a user to connect his or her computer to a wired network (e.g., through an Ethernet port) and enter a user name and password. If the user name and password match a user name and password in an authentication database, the user will be provided access to the network. These systems typically assume that a user is tied to a particular physical port, such as a port in the user's office. Based on this assumption, provisioning of bandwidth to the user occurs by physically provisioning the port to which the user is connected. If the user moves to a different port, the user will typically be provided with the bandwidth provisioned to the new port. Thus, provisioning of bandwidth is done on a per port rather than a per user basis.

General internet access provided via broadband technology (e.g., Digital Subscriber Line, DOCSIS or analog cable modem, or similar technologies) are capable of provisioning bandwidth to a computer premise equipment (CPE) device. CPE provisioning can be dynamic and remotely administered. However, broadband technology adoption is not a single-user and, hence, is not user-specific provisioning.

An increasing number of organizations (e.g., businesses, governmental organizations) wish to provide access to LANs and the Internet to various classes of users (internal users, contractors, customers, visitors). For example, many cafés have public wireless networks to allow patrons to access the Internet, receive email and perform other network activities. While users may be asked to authenticate to use the network, bandwidth is provisioned to the wireless routers, not the individual users. This means that one user connected to a particular router can consume a majority of the bandwidth (e.g., downloading pictures from the Internet), slowing down the wireless network for other users connected to that router.

An additional problem with many current networks, particularly wireless networks, is roaming between subnets. A subnet is a portion of a LAN that has a common address component. One subnet, for example, can cover a particular floor of a building, while another subnet covers another floor. Each subnet can potentially have its own set of internet protocol ("IP") addresses that may or may not overlap with the IP addresses of other subnets. When a user moves from one subnet to another, even if both subnets are part of the same LAN, the user must typically reauthenticate with the network. This can make physically roaming between subnets frustrating because open network sessions will often be dropped.

DISCLOSURE OF THE INVENTION

Embodiments of the present invention provide a system and method of providing network access that eliminates, or at least substantially reduces, the shortcomings of prior art network access systems and methods. More particularly, one embodiment of the present invention provides a system of providing network access comprising a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media, executable by the processor. In one embodiment of the present invention, the computer instructions can be executable to receive a network communication over the first network interface from a user using a user device and determine if the network

communication is associated with an authenticated user. If the network communication is not associated with an authenticated user, the computer instructions can be executable to direct the user to an authentication interface. The computer instructions can be further executable to receive credentials from the user and authenticate the user based on the credentials. If the user is authenticated, the computer instructions can receive a user profile.

Another embodiment of the present invention can include a system for providing access to a network that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media. The computer instructions can be executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

Another embodiment of the present invention includes a set of computer instructions stored on a storage media, executable by a processor to receive a network communication over a first network interface from a user using a user device, determine if the network communication is associated with an authenticated user, if the network communication is not associated with an authenticated user, direct the user to an authentication interface, receive credentials from the user, authenticate the user based on the credentials. If the user is authenticated, the computer instructions can be executed to receive a user profile.

Yet another embodiment of the present invention includes a set of computer instructions stored on the storage media, executable by the processor to receive a user profile and provision a user with access to a network based on the user profile.

Another embodiment of the present invention includes a method comprising receiving a user profile and provisioning a user with access to a network based on the user profile.

Another embodiment of the present invention includes a method comprising receiving a network communication over a first network interface from a user using a user device, determining if the network communication is associated with an authenticated user, if the network communication is not associated with an authenticated user, directing the user to an authentication interface, receiving credentials from the user, authenticating the user based on the credentials, and receiving a user profile if the user is authenticated.

Embodiments of the present invention provide an advantage over current systems and methods of providing access to a network by being able to authenticate a user sending network communications in any number of protocols.

Embodiments of the present invention provide another advantage over current systems and methods of providing access to a network by not requiring propriety client software to authenticate.

Embodiments of the present invention provide yet another advantage over current systems and methods of providing network access by provisioning network access on a per user rather than per port basis.

Embodiments of the present invention provide yet another advantage over current systems and methods of providing network access by supporting the ability of a user to physically roam without requiring reauthentication on different subnets.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

FIGURE 1 is a diagrammatic representation of a system for providing network access according to one embodiment of the present invention;

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing network access control;

FIGURE 3 is a flow chart illustrating one embodiment of provisioning user access to a network;

FIGURE 4 is a diagrammatic representation of a software architecture for providing authentication, according to one embodiment of the present invention;

FIGURE 5 is a diagrammatic representation of one embodiment of a software system for controlling access to a network for an authenticated user;

FIGURE 6 is a diagrammatic representation of traffic conditioning module, according to one embodiment of the present invention;

FIGURE 7 is a diagrammatic representation of roaming according to one embodiment of the present invention; and

FIGURE 8 is a diagrammatic representation of an example embodiment of a control device.

DETAILED DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are illustrated in the FIGURES, like numerals being used to refer to like and corresponding parts of the various drawings.

Embodiments of the present invention provide a system and method of network access control. According to one embodiment of the present invention, a control device can sit between a network (e.g., an Internet, a LAN or other network known in the art) and users. The users themselves may be located on a network or subnet or may connect directly to the control device. When a particular user attempts to access the network behind the control device (i.e., the controlled network), the control device can determine if the user has already been authenticated to use the controlled network. If the user has not been authenticated, the control device can direct the user to an authentication interface, such as a web page, and receive a set of credentials from the user. If the user is authorized to use the controlled network, based on the credentials, the control device can provision the user with access to the controlled network based on user specific settings.

FIGURE 1 is a diagrammatic representation of a system 10 for providing network access according to one embodiment of the present invention. In system 10, a user 12, using a user device 14 on network 16, can send a network communication that is destined for a device on controlled network 18. Network 16 and controlled network 18 can be any networks known in the art including, but not limited to, LANs, WANs, the Internet, global communications networks, wireless networks and/or any other communications network known in the art. For the sake of example, network 16 can be a wireless network, such as public wireless network provided to café patrons, and controlled network 18 can be the Internet. An access control device 20 ("control device 20") can receive the network communication and determine if user 12 is authorized to access network 18 and the extent of the user's access. Control device

20 can contact an authentication system 22 to authenticate user 12 against a set of authorized users stored, for example, in authentication database 24. If user 12 is authenticated, access control device 20 can receive a user profile that includes one or more attributes that govern the user's access to controlled network 18.

According to one embodiment of the present invention, user device 14 can comprise any computing device known in the art (e.g., desktop, laptop, PDA, mobile phone or any other device capable of network communication) and can be connected to control device 20 in any manner known in the art (e.g., by LAN, wireless network, direct connection or other manner known in the art). In the example of FIGURE 1, user 12 is using a laptop 14 on a public wireless network 16 (e.g., a wireless LAN) to access Internet 18.

User 12 can send the network communication using a network application running on user device 14 destined for a device on network 18. The network application can be any publicly available network application (e.g., a web browser, email program, etc.) or proprietary application. For example, user 12 can use an internet browser, such as Netscape Navigator or Microsoft Internet Explorer, to send a request for a web page available over Internet 18. As would be understood by those of ordinary skill in the art, the web page request is transmitted as an HTTP request in one or more internet protocol ("IP") packets.

Control device 20 can monitor network 16 for network communications originating on network 16 (e.g., for example for IP packets originating on LAN 16) using any network monitoring technique known in the art. Control device 20 can read the IP packet headers to extract information on the originating user device. As an example, control device 20 can read the packet headers corresponding to the web page request to determine the IP address and MAC address associated with laptop 14.

Based on the MAC address, IP address or other information that can be extracted from the network communication, control device 20 can determine if user 12 has been authenticated. This can be done, for example, by comparing the MAC address and IP address of user device 14 to MAC addresses and IP addresses for users that have been authenticated. If the user has not authenticated, control device 20 can direct user 12 to an authentication interface by, for example, redirecting the HTTP request to a login web page that requests user credentials, such as user name and password.

Control device 20 can receive the user credentials and send the credentials to authentication system 22. Authentication system 22 can compare the credentials to credentials in authentication database 24 to determine if user 12 is permitted access to network 18 and the extent of the user's access. If the credentials are authenticated, authentication system 22 can pass a user profile associated with user 12 to control device 20.

The user profile can include parameters that determine the extent of a user's access to network 18 and/or services available to that user. For example, the user profile can indicate that a user is permitted certain upload and download data transfer rates, that the user is not permitted to visit particular web sites, or that the user qualifies for virus scanning. In one embodiment of the present invention, the constraints indicated in the user profile can be implemented through one or more applications at control device 20.

When control device 20 receives a user profile from authentication system 22 (or self authenticates the user), control device 20 can establish a control session for the user, indicating that the user is currently active. Additionally, control device 20 can establish provisioning rules based on the user profile. The provisioning rules can include, for example, firewall rules and traffic constraints that govern the user's access to network 18. In one embodiment of the present invention, the sessions and provisioning rules can be indexed to a particular user. This can be done, for example, by associating the control session and rules to a key based on the MAC address and/or IP address of laptop and/or user credentials. The use of user credentials as part of an indexing key allows multiple sessions by the same user using different devices (e.g., a user accessing network 18 through a laptop and PDA) to be tied together for, for example, billing purposes.

It should be noted that FIGURE 1 is provided by way of example only. In other embodiments of the present invention, control device 20 can control access to multiple networks. For example, if a user requests a web page over a cafés publicly available wireless connection, the user may need to access both additional portions of the café's internal LAN (e.g., routers, switches or other network devices) and the Internet. Additionally, it should be noted that authentication, in one embodiment of the present invention, can be performed at control device 20 or be carried out by a separate authentication system.

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing network access control at, for example, a control device (e.g., control device 20 of FIGURE 1). At

step 30, the control device can monitor a connection, such as a LAN, across protocol layers (e.g., IP, UPD/IP, TCP/IP and other protocol layers known in the art) for a network communication originating at a user device and, at step 32, receive a network communication. The network communication can be, for example, an HTTP request, an email message, an FTP request, a telnet request, an instant message, an ICMP message, a SNMP message, a UDP message or other network communication known in the art.

The control device can determine, at step 34, if a user associated with the network communication has been authenticated. In one embodiment of the present invention, this can be done by comparing an identifier(s) with identifiers previously associated with authenticated users. Any identifier or combination of identifiers known in the art can be used to identify the origins of a network communication. By way of example, but not limitation, the control device can read the headers of IP packets carrying the network communication to extract an originating MAC address and/or an originating IP address associated with the originating user device. The control device can compare the identifier(s) extracted from the IP packet to identifiers for previously authenticated users. If the extracted identifier matches an authenticated user, the control device can control the user's network access as described in conjunction with the example of FIGURE 5. Otherwise, control can pass to step 36.

If a user has not authenticated, the control device, at step 36, can capture the user's network application session until the user authenticates. For applications that are latency or session sensitive, such as HTTP or HTTPS communications, the session may be cached or suspended in a manner that does cause the destination application (e.g., web page) to drop the session. For example, if the user enters into a stateful network application session, the control device can detect this, based on information in the IP packets, and maintain the session on behalf of the user until the user has authenticated.

At step 38, the control device can redirect the user to an authentication interface. By way of example but not limitation, if the network communication is an HTTP request, control device 20 can redirect the HTTP request to an authentication web page hosted by the control device using any HTTP redirection technique known in the art. If the network communication is in another form, such as an email message, the control device can detect, from the IP packets, the protocol (e.g., POP, SMTP or other protocol known in the art) used by the network application (e.g., a mail user agent) and send a message back to the network

application with, for example, an embedded link to the authentication interface. In other embodiments of the present invention, the control device can send a protocol-specific message, such as an error message, indicating the authentication state and providing information about further actions necessary on part of the user to authenticate. As an example, if an unauthenticated user initiates a telnet session, the control device can return a telnet error indicating a failed authentication and providing directions to the application interface. Thus, the control device, rather than simply returning "Connect Failed" could return "Connect Failed: Authenticate at http://www.Rocksteady1.com/login//." In this case, http://www.Rocksteady1.com/login// can be hosted by the control device.

In response to the authentication interface, the user can provide credentials and, at step 40, the control device can receive them. The credentials can be any credentials known in the art including, but not limited to, user name, password, biometric data (e.g., fingerprint, retina pattern or other biometric information known in the art), smart card credentials, certificates and/or other user or hardware based credentials. In one embodiment of the present invention, the credentials can be received by HTTP Post from a web page based form.

At step 42, the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users. This can be done at the control device, or the control device can authenticate the user by sending the credentials to a backend authentication system (e.g., using HTTP Post). The credentials, in one embodiment of the present invention, can be compared against an authentication database of authorized users to determine if the credentials match credentials in the authentication database. Example authentication technologies include LDAP, RADIUS, Microsoft Active Directory Service, Tivoli Access Manager, and Cisco TACACS/TACACS+.

If the credentials are not authenticated, control can pass to step 52. If, on the other hand, the credentials are authenticated, the control device, at step 44, can receive a user profile from the authentication system or internal data storage (e.g., a database, file or other data storage format known in the art) that contains attributes that govern provisioning of user access to the network. For example, the user profile can contain indicators of the upload and download bandwidth to which the user is entitled, session time limit, whether the control device will perform virus scanning for the user of incoming and/or outgoing IP packets, or other services known in the art. The user profile can also point to additional information that can be used to

control network access. For example, the user profile can point to a list of web sites that the particular user is not permitted to visit. In one embodiment of the present invention, the user profile can be received in a canonical format as an HTTP Post from the authentication system to the control device.

According to one embodiment of the present invention, each user profile can have a predefined set of attributes. In some cases, the backend authentication system may not provide values for each of these attributes. Therefore, the control device can determine, at step 46, if the received user profile is complete, and, if it is not complete can, at step 48, fill in the missing attribute values with default values, which can be part of the control device's local configuration or may be retrieved by the control device during, for example, its initialization or startup phase. At step 50, the control device can initiate a control session for the authenticated user. The control session can have a specified time limit, a time out limit and/or other session features known in the art. While the control session is active, the control device can govern a user's access to a network according to the user profile associated with that user and defaults. The control session can be tracked by credentials, IP address, MAC address and/or other identifier. In one embodiment of the present invention, the control session can be tracked based on a combination of user device MAC address and IP address and user provided credentials.

Thus, the control device can determine if the user seeking to use a network is authorized to use the network (step 42). According to one embodiment of the present invention, if the user is authenticated, the control device receives a user profile (step 44), fills in any missing parameters in the user profile with defaults (steps 46 and 48) and initiates a control session for the user (step 50).

If, however, at step 42, the user is not authenticated, the control device, at step 52, can direct the user to a setup interface, such as an account setup web page. At the setup interface, the user can specify credentials, network access and levels of service, payment options and/or other account information. Based on this information, a user profile can be generated and stored in the authentication database. Profiles can also be entered into the authentication database by a systems administrator or in any other manner known in the art.

The control device can, thus, authenticate a user based on a network communication from a network application such as a web browser, ftp client, telnet client, mail user agent or other

publicly available or proprietary network application. By supporting publicly available network applications, such as web browsers, embodiments of the present invention allow authentication without requiring that a user install a proprietary network application on the user's user device. If a user can authenticate, the control device can control a user's access to a controlled network based on a user profile and/or default values. If the user can not authenticate, the user can be given an opportunity to establish a user profile. According to one embodiment of the present invention, steps 30-54 can be optionally repeated (step 54) for each new network communication or IP packet detected.

FIGURE 3 is a flow chart illustrating one embodiment of provisioning user access to a network at a control device (e.g., control device 20 of FIGURE 1). At step 56, global rules can be established. Global rules can include rules, such as firewall rules and bandwidth allocations. A firewall rule can include any firewall rule known in the art, such as, for example, that all packets destined for a particular web site will be blocked. A traffic rule can include any globally applicable traffic rule; for example, that the total used bandwidth of control device 20 must not exceed a particular amount. Additionally global rules can include rules such as that every packet is scanned for viruses or subject to some other arbitrarily defined process. At step 58, interface specific rules can be established. Interface specific rules can specify and arbitrary traffic rule or condition on a per interface basis. For example, an interface specific firewall rule can specify that streaming content will not be permitted over a wireless interface. Global and interface specific rules can be established in any manner, as would be understood by those of ordinary skill in the art.

At step 60, the control device can establish user specific rules and conditions based on attributes in the user profile. According to one embodiment of the present invention, the control device can map the attributes to any arbitrary rule or traffic condition. By way of example, but not limitation, a user profile can contain attributes to specify upload and download bandwidth allocations for a user, firewall settings, whether the user can use transient VPNs, whether the user can use streaming services or voice over IP services, whether the user should be permitted to perform video teleconferencing, whether the control device should perform virus scanning or worm detection for the user, whether the user can utilize print services, surcharges for services or other settings.

In one embodiment of the present invention, rules can be represented in an IP table. As would be understood by those of ordinary skill in the art, IP tables are essentially tables of rules that can be accessed by applications, such as a firewall, to execute the rules. Rules in the IP table can be associated to a user through any arbitrary identifier. Using the example of FIGURE 1, the IP table rule(s) for user 12 can be bound to user 12 based on the MAC address and IP address of user device 14 and the credentials provided by user 12 for the particular control session.

An IP table rule can reference other rules or parameters for providing user specific provisioning. As an example, the IP table rule can reference websites that a user is not permitted to visit. A firewall application can access the rule to prevent the user from visiting these sites. As another example, the IP table rule for user 12 can reference a traffic rule that dictates that the bandwidth allocated to user 12 is 128kbps up and 512kbps down. A traffic control application, such as the Linux based Traffic Control module, can access the traffic control rule through the IP table and enforce the bandwidth allocation.

It should be noted that a user specific rule in an IP table can reference rules or parameters usable by any number of applications or process, such as firewalls, traffic control modules, virus scan applications or other applications known in the art. For example, a virus scan application can access the IP table rule for a particular user and us parameters referenced by the rule to provide user specific virus scanning. It should be further noted that the use of IP tables to establish user specific rules for user specific provisioning of bandwidth and access control is provided by way of example only, and user specific rules can be implemented in any suitable manner, as would be understood by those of ordinary skill in the art

FIGURE 4 is a diagrammatic representation of a software architecture for providing authentication, according to one embodiment of the present invention. The software architecture can be implemented, for example, at control device 20. According to one embodiment of the present invention, an authentication module 62 of an authentication and control program 61 can monitor a connection, such a network connection for communications from user devices. Control device 20 can receive a network communication in the form of, for example, one or more IP packets 63, which can represent a network communication from a web browser, a telnet client, a mail user agent or other communication from a network application. In one embodiment of the present invention, the network

communication can be directed to control device 20 to access authentication page 70 or to another destination, such as a web server on the Internet.

Authentication module 62 can read the header 64 of IP packet 63 to determine an identifier for the originating user device such as, for example, an originating MAC address and/or IP address. For the sake of example, the MAC address is 08:00:69:02:01:FF and the IP address is 100.100.100. Authentication module 62 can then determine if the IP packet originated at a user device for which a control session is active by comparing information extracted from the header to a list 66 of active control sessions. The active control sessions can be indexed by, for example, MAC address, IP address, a combination of addresses or other identifier(s) associated with the originating user device or user. If a control session is active for the originating user device, the IP packet and header information can be passed to provisioning module 68. If the IP packet originated at a user device not associated with an active control session, control device 20 can authenticate the user.

According to one embodiment of the present invention, to authenticate the user, control device 20 can redirect the user to an authentication interface, such as authentication web page 70, by sending a redirect message 72. Redirect message 72 can be a web page redirect, an error message, an email message with an embedded link to web page 70 or other indication that a user should access the authentication interface.

A user can provide credentials 74 to control device 20 and control device 20 can pass the credentials 74 to an authentication system as, for example, an HTTP Post. If the credentials are authenticated by the authentication system, authentication module 62 can receive a user profile 76 that contains attributes that can govern provisioning of access control for the user. In one embodiment of the present invention, if the user profile is incomplete, authentication module 62 can add default attributes to the profile. Furthermore, if the user is authenticated by the authentication system, session monitor 78 can initiate a new control session if the credentials are authenticated and update the list 66 of active control sessions. It should be noted that in another embodiment of the present invention, authentication can occur internally to control device 20.

FIGURE 5 is a diagrammatic representation of one embodiment of a software system for controlling access to a network for an authenticated user. According to one embodiment of the present invention, an authentication and control program 61 running at control device 20

can receive an IP packet 80 originating from a user device. Authentication module 62 can determine if IP packet 80 is associated with a user that has authenticated, as described in conjunction with FIGURE 4. Continuing with the previous example, and assuming that the user associated with MAC address 08:00:69:02:01:FF and the IP address 100.100.100 authenticated, IP packet 80 can be processed by provisioning module 68, which can provide user specific provisioning. In the example of FIGURE 5, user specific provisioning can include provisioning of firewall services (e.g., by firewall module 82), user specific allocation of bandwidth (e.g., by traffic conditioning module 84). It should be understood, however, that user specific provisioning can include provisioning of additional services known in the art. In one embodiment of the present invention firewall module 82 can be a LINUX based firewall and traffic conditioning module 84 can be the LINUX based Traffic Controller program.

According to one embodiment of the present invention, provisioning module 68 can build a set of IP tables to govern provisioning by firewall module 82 and traffic conditioning module 84. In the example of FIGURE 5, provisioning module 68 can have IP table 86 for interface specific rules, IP table 88 for global rules and IP table 90 for user specific rules. IP table 90 can contain user specific rules associated with particular users. For example, IP table 90 can contain user rule 92 indexed to MAC address 08:00:69:02:01:FF and the IP address 100.100.100 (i.e., indexed to user 12 on laptop 14).

Each rule can optionally point to additional rules and parameters. For example user specific rule 92 can point to traffic control rule 94 to govern bandwidth provisioning, firewall parameters 96 to govern firewall settings and file 98 that contains web sites that user 12 is not permitted to access. User specific rule 92 and the associated rules and parameters can be based on user profile 76. As an example, user profile 76 can specify that user 12 is entitled to 128kbps up and 512kbps down. Provisioning module 68 can establish traffic control rule 94, accessible by traffic conditioning module 84, that contains these limitations. Similarly, provisioning module 68 can establish firewall parameters 96 and file 98 based on attributes in user profile 76.

In the example of FIGURE 5, provisioning module 68 can provide firewall and traffic conditioning services for IP packet 80. Firewall module 82, in one embodiment of the present invention, can process IP packet 80 according to several stages. At interface specific

stage 98, firewall module 82 can access interface specific IP table 86 to access rules to be applied to packet 80 based on the type of interface over which packet 80 is received (e.g., wireless, Ethernet, or other interface known in the art). At global stage 100, firewall module 82 can apply global firewall rules to packet 80 from global IP table 88. In general, firewall module 82 can apply global firewall rules to every IP packet that firewall module 82 processes.

At client discrimination stage 102, firewall module 82 can read the packet header of packet 80 to extract information to associate packet 80 with a user. Continuing with the previous example, if firewall module 82 extracts MAC address 08:00:69:02:01:FF and the IP address 100.100.100, firewall module 82 can associate packet 80 with user specific rule 92. At user specific rule stage 104, firewall module 82 can access user specific rule 92 based, for example, on the extracted MAC address and IP address. Based on user specific rule 92, firewall module 82 can access firewall parameters 94 and restricted web site list 96 and can process packet 80 accordingly. It should be noted that firewall parameters 94 can include any arbitrary set of parameters that can be used by a firewall to control traffic flow. For example, firewall parameters 94 can specify whether the associated user (e.g., user 12 of FIGURE 1) can use voice over IP applications, video conferencing services, transient VPN applications or other applications. Finally, at interface specific stage 106, firewall module 82 can access interface specific IP table 86 and enforce rules corresponding to the interface over which packet 80 will be communicated (e.g., wireless connection, Ethernet connection, or other computer interface known in the art).

In one embodiment of the present invention, traffic conditioning module 84 can also access user specific IP table 90 and locate user specific rule 92, based for example, on the originating MAC address and IP address. From user specific rule 92, traffic conditioning module 84 can locate traffic control rule 94 that specifies a maximum upload bandwidth of 128kbps. If the user exceeds this bandwidth limitation, traffic conditioning module 84 can queue or drop packet 80.

Packet flow in the reverse direction can be processed in an analogous manner. For example, a packet arriving from the Internet destined for a user device (e.g., laptop 14 of FIGURE 1) can be examined for IP address and MAC address. Based on these identifiers, user specific traffic control rules and firewall rules can be applied to the packet as governed by user

specific rule 92 in IP table 90. Firewall module 82 can apply global rules based on IP table 88 and interface specific rules based on IP table 86 for both the controlled network and user side interfaces.

In addition to authentication and provisioning, authentication and control program 61 can provide session monitoring. Session monitoring can be performed in any manner known in the art. Session monitor 78 can monitor a control session for session characteristics such as session time, time out, bandwidth utilization and other session characteristics known in the art. In one embodiment of the present invention, session monitor 78 can determine if a user's session is still active by for example, performing port scans and ARP pings, as would be understood by those of skill in the art. If session monitor 78 determines that a control session is timed out (e.g., has been inactive for a predetermined period of time), session monitor can remove the control session from the list of active sessions, returning the user to an unauthenticated state, and delete the user specific rules for the associated user from IP table 90. Session monitor 78 can also generate records, such as accounting records and session records that can optionally be transmitted to other systems for further processing.

As would understood by those of ordinary skill in the art, authentication and control program 61 can also provide any arbitrary services known in the art, including, but not limited to, web server functions, DHCP client for negotiation with ISPs, DHCP server to assign IP addresses to user computers, kernel based packet filtering and stateful inspection, IP sharing, NATplus, port redirection, information and attack logging, automatic updating, VPN masquerade, remote support an configuration, name server configuration and/or web content filtering.

FIGURE 6 is a diagrammatic representation of traffic conditioning module 84, according to one embodiment of the present invention. Conditioning module 84 can include interface master queue 108, user discriminator 110 and user specific conditioner 112. User discriminator 110 can read a packet header to determine the appropriate user specific conditioner to which to send the packet based on for example, the IP address and MAC address of the packet. Bandwidth limits can be enforced based on user specific traffic control rules. According to one embodiment of the present invention, conditioning module 84 can locate the user specific traffic control rule based from user specific IP table 90. For example, for a packet having the originating MAC address 08:00:69:02:01:FF and the IP address 100.100.100, traffic conditioning module 84 can access user specific rule 92 and, from user

specific rule 92, user specific traffic control rule 94. The user specific traffic control rule can be enforced at the corresponding user specific conditioner.

Interface master queue 108 can control the flow of network traffic over a particular interface. It can be configured to send out data at whatever rate is appropriate for the corresponding network connection. Interface master queue 108 can be feed data by user specific conditioners 112, each of which can have its own queue to hold packets the conditioner has accepted, but interface master queue 108 is not ready to accept.

For a particular network interface, each user can have an inward (i.e., download) and outward (i.e., upload) bandwidth allowance, based on attributes in the user's user profile. A bandwidth limit is the maximum rate at which a user is permitted to transmit or receive network traffic over a particular interface. User specific traffic conditioners 112 ensure that, if a user exceeds his or her bandwidth allowance, further network traffic in that direction on the network will be queued or dropped until the average data rate fall back within the bandwidth allowance. Thus, traffic conditioning module 84 can regulate bandwidth on a per user basis. In one embodiment, the control device can also dynamically control bandwidth on a per user basis.

It should be noted that the architectures of FIGURE 4, FIGURE 5 and FIGURE 6 are provided by way of example only and authentication, session monitoring and provisioning can be implemented using any suitable programming language and/or structure known in the art. In the example of FIGURE 5, provisioning module 68 provides firewall and traffic conditioning based on a set of IP tables. It should be noted, however, that provisioning module 68 can provide additional services on a per user basis, such as virus scanning, worm detection or any other service known in the art. Each of these additional services can access rules and parameters based, for example, on IP table 90. Moreover, the use of IP tables to index and provide access to rules and parameters for particular services is also provided by way of example. In other embodiments of the present invention, a user profile can be mapped to rules and parameters for various applications in any suitable programming manner known in the art.

Embodiments of the present invention provide advantages over prior art systems and methods of providing access control. One advantage is that embodiments of the control device can detect network communications across a variety of protocols and direct a user to an

authentication interface. Another advantage provided by embodiments of the present invention is that provisioning can be done based on a user profile rather than based on a particular port. In other words provisioning of bandwidth and services can be done on a per user rather than per port basis. Additionally, as will be described in conjunction with FIGURE 7, embodiments of the present invention can provide advantages with respect to physical roaming.

FIGURE 7 is a diagrammatic representation of roaming according to one embodiment of the present invention. In the example of FIGURE 7, a LAN can have multiple subnets, in this case two, subnet 122 and subnet 124. For the sake of example, each subnet can be a wireless subnet. Each subnet could represent for example subnets on different floors of an office building or subnets in different buildings, etc. Each subnet can be connected to network 126 via control device 128 and control device 130, respectively. Network 126 can be any network known in the art including a LAN, the Internet, a wireless network a global communications network or any other network known in the art. According to one embodiment of the present invention, control device 128 and control device 130 can be in federation 132. This means that control device 128 and control device 132 have at least enough information about each other that they can send messages to each other over the LAN and/or over network 126 to exchange session information.

In operation, user 134 using user device 135 (e.g., a laptop or other computing device known in the art) can authenticate with control device 130 at point 136 in subnet 124. Because user 134 is in subnet 124 at point 136, user device 135 can be assigned a first IP address, for example 100.100.100. For the sake example, user device can also be associated with MAC address 08:00:69:02:01:FF. The user's active session can be indexed based on the first IP address, the MAC address and the user's credentials. User 134 can then roam outside of subnet 124, by for example, leaving the range of the wireless routers of subnet 124. Control device 130 can determine if user 134 is still active on subnet 124 by, for example, ARP pining and/or performing port scans on user device 135 at predetermined intervals.

If control device 130 can not locate user device on subnet 124, control device 130 can begin a time out timer. If the time out timer reaches a predetermined limit, control device 130 can close the control session, returning user 134 to his or her preauthenticated state. If, however, user 134 returns to subnet 124, as, for example, determined by the ARP pings and/or port

scans, within the time limit, control device 130 can reset the time out timer and keep the control session open. Assume, for the sake of example, that user 134 returns to point 138 in subnet 124 before the session is timed out, so his or her control session remains open. Thus, control device 130 can maintain user 134 in an authenticated state even though user 134 roamed outside of subnet 124.

User 134 can then roam from point 138 to point 140 with laptop 135. When user 134 leaves subnet 124, control device 130 can begin a time out timer for the user's control session. When user 134 enters subnet 122, laptop 135 can be assigned a new IP address for that subnet, say 101.100.100. If user 134 initiates a network communication destined for network 126 (e.g., a web page request), control device 128 can receive the communication and determine if IP address 101.100.100 and MAC address 08:00:69:02:01:FF correspond to an active control session. In this case, because user 134 authenticated with control device 130, IP address 101.100.100 and MAC address 08:00:69:02:01:FF will not correspond to an active session on control device 128. In one embodiment of the present invention, control device 128 can simply initiate a new authentication process.

In another embodiment of the present invention, control device 128 can query other control devices with which it is federated to determine if a user has an active control session. For example, because control device 128 and control device 130 are in federation 132, control device 128 can query control device 130 to determine if user 134 has an active session. This can be done based, for example, on the MAC address of laptop 135 as laptop 135 will typically retain the same MAC address across subnets.

According to one embodiment of the present invention, control device 128 can send an SNMP message to control device 130 to determine if there is an active session corresponding to the MAC address 08:00:69:02:01:FF. In this case, if the user's control session at control device 130 has not yet timed out, control device 130 can reply to control device 128 with session information and the user profile for user 134. Control device 128 can establish user based provisioning based on the user profile as if user 134 had authenticated at control device 128. Thus, user 134 can communicate to network 126 through control device 128 without reauthenticating.

In other embodiments of the present invention, active session information for each control device can be maintained at a centralized system. Control device 128 can, in this

embodiment of the present invention, query the centralized system as to whether there are any active session corresponding to MAC address 08:00:69:02:01:FF. In yet another embodiment of the present invention, control device 128 can receive the user profile for user 134 from an authentication system rather than from another control device.

Thus, embodiments of the present invention allow a user to physically roam, either in a wired or wireless environment, by, for example permitting mobile, transient behavior through the use of network access timeouts; and/or coordinating authentications between control devices.

As can be understood from the foregoing, physically moving from one location to another can cause a user device to become disconnected from the network or subnet (e.g., subnet 122 or subnet 124) for a short period of time. The length of the time the user is not connected can be a function of physically moving from one location to another. Embodiments of the present invention permit a configurable timeout period that allows an authenticated user to become disconnected from a network and then reappear without losing the user's authentication status. In one embodiment of the present invention, this timeout period can be part of the policy of the network service provider (e.g., the entity controlling subnet 122 and subnet 124) and, as such, is a configurable item in the control devices. The control devices can monitor user network device connection states actively, employing ARP ping techniques and non-obtrusive polling of network application ports to check the connection status of all authenticated users' devices.

A second aspect of physical roaming is when a user not only becomes disconnected from the network, but leaves a subnet arbitrated or monitored by a control device. In this case, once the user attempts any network access by way of a network access port (wired or wireless) at another control device, that control device can solicit feedback from any federation of control devices with which it has joined to determine if this particular user has an active session and should be granted a new session, without the requirement to authenticate. In some embodiments of the present invention, the new control device can dynamically remap the network connections and configuration of a roaming user's user device, in the event that the new control device is configured differently or controls a different subnet. For example, the new control device can remap the IP address of the user device according any IP mapping scheme known in the art.

Control devices can participate in federations, in one embodiment of the present invention, via loosely-coupled SNMP dialogs. In this embodiment of the present invention there is no permanent federation configuration and, instead, control devices can broadcast their authorization status requests dynamically.

Another aspect of roaming can be service roaming. Service roaming can be a function of negotiated usage agreements between internet service providers, resulting in cross-indexed user authentication database and, potentially, resulting surcharges for accessing network resources via service providers other than the primary service provider associated with a user; i.e., assuming network service is funded by an individual, there may be surcharges to access network services via control devices not owned by that service provider.

FIGURE 8 is a diagrammatic representation of one embodiment of a control device 141 that can provide access control and authentication. For the purposes of example, control device 141 can comprise a main bus 142, a main processor 144, a primary storage medium 146, a secondary storage controller 148, a storage media 150, a user side network interface 152 and a controlled network network interface 154. The network interfaces can include Ethernet interfaces, fibre channel interfaces, T1 interfaces, wireless interfaces or other network interfaces known in the art. Other devices may be connected to or be part of such a control device include, by way of example, but not limitation, controllers, a display, a mouse, a keyboard, and so forth. Additionally, control device 140 can include additional interfaces to communicate to additional networks using various protocols and can include interfaces for administrative functions.

The main processor 144 communicates with the other components by way of the main bus 142. This main processor 144 can be a general purpose processor, a limited processor such as an ASIC or microcontroller, or any other instruction execution machine. The primary storage 146 can provide transient memory or storage space for use by programs executing on the main processor 144. The main processor 144 communicates with the primary storage in any manner known in the art.

The secondary storage controller 148 connects a storage media 150 such as a hard drive, CD-ROM, floppy, tape drive, optical storage medium, memory or other storage device to the main processor 144 by way of the main bus 142. The main processor 144 communicates with the secondary storage controller 148 by way of the main bus 142, and the secondary storage

controller 148 is used to read and /or write the storage media 150 on behalf of the main processor 144.

Control device 141 may communicate with other computing devices (e.g., user devices, network servers, etc.) by way of networks using network interfaces (e.g., user side network interface 152 and controlled network network interface 154 or other network interface). Computer instructions running on the main processor may then access other computers across the network in any of the conventional ways, e.g. by executing "protocols" which affect the transmission and reception of protocol data units, packages, etc. over the data transmission network.

In one embodiment of the present invention, storage media 150 can store a set of computer instructions 156 that are executable by processor 144. During execution, portions of computer instructions 156 and data can be stored in primary storage 146, as would be understood by those of ordinary skill in the art. Processor 144 can execute computer instructions 156 to authenticate users and/or provide provisioning to users on a per user basis. Computer instructions 156 may be implemented in any programming language known in the art and can be implemented using any suitable architecture.

Additionally, in one embodiment of the present invention, storage media 150 can include a database of user profiles an authentication credentials. In this embodiment of the present invention, instructions 156 can be executable to authenticate the user at control device 141 and receive the user profile from storage media 150.

Although shown as a standalone device in FIGURE 8, control device 141 may be integrated with and share components with other devices such as routers, servers, hubs or other devices known in the art. Additionally, computer instructions 156 can be distributed across multiple storage media and can be executed by multiple processors. One example of an exemplary control device is the Rock Box or the Rocksteady NSA Server, from Rocksteady Networks, Inc. of Austin, Texas.

While the present invention has been described with reference to particular embodiments, it should be understood that the embodiments are illustrative and that the scope of the invention is not limited to these embodiments. Many variations, modifications, additions and improvements to the embodiments described above are possible. It is contemplated that these

variations, modifications, additions and improvements fall within the scope of the invention as detailed in the following claims.

5

CLAIMS

1. A system of providing network access comprising:

a processor;

a first network interface coupled to the processor;

a second network interface coupled to the processor;

a storage media accessible by the processor;

a set of computer instructions stored on the storage media, executable by the processor to:

receive a network communication over the first network interface from a user device associated with a user;

determine if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, direct the user to an authentication interface;

receive credentials from the user;

authenticate the user based on the credentials,

receive a user profile if the user is authenticated.

2. The system of Claim 1, wherein the computer instructions are further operable to monitor a network connected to the first network interface for the network communication.

3. The system of Claim 2, wherein the computer instructions are further operable to monitor the network across multiple protocols.

4. The system of Claim 1, wherein the network communication comprises an HTTP request and wherein the computer instructions are further executable to:

receive the HTTP request;

send a redirect request to the user device to redirect a web browser to the authentication interface.

5. The system of Claim 1, wherein the network communication comprises an email and wherein the computer instructions are further executable to:

receive the email;

determine a protocol for the email;

send a reply email message to the user device directing the user to the authentication interface.

6. The system of Claim 1, wherein the computer instructions are further executable to:

determine a network protocol for the network communication;

send a reply to the user device according to the network protocol directing the user to the authentication interface.

7. The system of Claim 6, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

8. The system of Claim 1, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

9. The system of Claim 8, wherein the identifier comprises an IP address for the user device.

10. The system of Claim 8, wherein the identifier comprises a MAC address for the user device.

11. The system of Claim 1, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by contacting a federated device.

12. The system of Claim 1, wherein the computer instructions are further executable to receive the user profile from an internal source.

13. The system of Claim 1, wherein the computer instructions are further executable to:

transmit the credentials to an authentication system; and

receive the user profile from the authentication system if the user is authenticated.

14. The system of Claim 1, wherein the computer instructions are further executable to:

provision the user with access to a network connected to the second network interface based on the user profile.

15. The system of Claim 14, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

16. The system of Claim 15, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

17. The system of Claim 16, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

18. The system of Claim 17, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

19. The system of Claim 18, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

20. The system of Claim 14 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

21. The system of Claim 1, wherein the computer instructions are executable to monitor a control session for the user to determine if the user times out.

22. The system of Claim 21, wherein the computer instructions are further executable to close the control session if the user times out.

23. A system of providing network access comprising:

a processor;

a first network interface coupled to the processor;

a second network interface coupled to the processor;

a storage media accessible by the processor;

a set of computer instructions stored on the storage media, executable by the processor to:

receive a user profile; and

provision a user on a first network connected to the first network interface with access to a second network connected to the second network interface based on the user profile.

24. The system of Claim 23, wherein the computer instructions are further executable to provision the user with access to the second network by provisioning user specific bandwidth to the user based on the user profile.

25. The system of Claim 24, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

26. The system of Claim 25, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

27. The system of Claim 26, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

28. The system of Claim 27, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

29. The system of Claim 23 wherein the computer instructions are further executable to provision the user with access to the second network by establishing user specific firewall rules and enforcing the user specific firewall rules.

30. The system of Claim 23, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the second network.

31. The system of Claim 23, wherein the computer instructions are further executable to authenticate the user.

32. A system of providing network access comprising

a set of computer instructions stored on a storage media, executable by a processor to:

receive a network communication over a first network interface from a user device associated with a user;

determine if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, direct the user to an authentication interface;

receive credentials from the user;

authenticate the user based on the credentials,

receive a user profile if the user is authenticated.

33. The system of Claim 32, wherein the computer instructions are further operable to monitor a network for the network communication.

34. The system of Claim 33, wherein the computer instructions are further operable to monitor the network across multiple protocols.

35. The system of Claim 32, wherein the network communication comprises an HTTP request and wherein the computer instructions are further executable to:

receive the HTTP request;

send a redirect request to the user device to redirect a web browser to the authentication interface.

36. The system of Claim 32, wherein the network communication comprises an email and wherein the computer instructions are further executable to:

receive the email;

determine a protocol for the email;

send a reply email message to the user device directing the user to the authentication interface.

37. The system of Claim 32, wherein the computer instructions are further executable to:

determine a network protocol for the network communication;

send a reply to the user device according to the network protocol directing the user to the authentication interface.

38. The system of Claim 37, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

39. The system of Claim 32, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

40. The system of Claim 39, wherein the identifier comprises an IP address for the user device.

41. The system of Claim 39, wherein the identifier comprises a MAC address for the user device.

42. The system of Claim 32, wherein the computer instructions are executable to determine if the network communication is associated with an authenticated user by contacting a federated device.

43. The system of Claim 32, wherein the computer instructions are further executable to receive the user profile from an internal source.

44. The system of Claim 32, wherein the computer instructions are further executable to:

transmit the credentials to an authentication system; and

receive the user profile from the authentication system if the user is authenticated.

45. The system of Claim 32, wherein the computer instructions are further executable to:

provision the user with access to a network based on the user profile.

46. The system of Claim 45, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

47. The system of Claim 46, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

48. The system of Claim 47, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

49. The system of Claim 48, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

50. The system of Claim 49, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

51. The system of Claim 45 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

52. The system of Claim 32, wherein the computer instructions are executable to monitor a control session for the user to determine if the user times out.

53. The system of Claim 52, wherein the computer instructions are further executable to close the control session if the user times out.

54. A system of providing network access comprising:

a set of computer instructions stored on the storage media, executable by the processor to:

receive a user profile;

provision a user with access to a network based on the user profile.

55. The system of Claim 54, wherein the computer instructions are further executable to provision the user with access to the network by provisioning user specific bandwidth based on the user profile.

56. The system of Claim 55, wherein the computer instructions are further executable to provision user specific bandwidth by establishing a traffic control rule based on the user profile.

57. The system of Claim 56, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

58. The system of Claim 57, wherein the computer instructions are executable to:

receive a packet;

determine that the traffic control rule applies to the packet based on an identifier extracted from the packet;

apply the traffic control rule to the packet.

59. The system of Claim 58, wherein the computer instructions are further executable to drop the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

60. The system of Claim 54 wherein the computer instructions are further executable to provision the user with access to the network by establishing user specific firewall rules and enforcing the user specific firewall rules.

61. The system of Claim 54, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the network.

62. The system of Claim 54, wherein the computer instructions are further executable to authenticate the user.

63. A method of providing network access comprising

receiving a network communication over a first network interface from a user using a user device;

determining if the network communication is associated with an authenticated user;

if the network communication is not associated with an authenticated user, directing the user to an authentication interface;

receiving credentials from the user;

authenticating the user based on the credentials,

receiving a user profile if the user is authenticated.

64. The method of Claim 63, further comprising:

determining a network protocol for the network communication;

sending a reply to the user device according to the network protocol directing the user to the authentication interface.

65. The method of Claim 64, wherein the network protocol is one of HTTP, SMTP, POP, telnet, UDP or FTP.

66. The method of Claim 63, further comprising determining if a network communication is associated with an authenticated user by comparing an identifier associated with the network communication to identifiers associated with authenticated users.

67. The method of Claim 63, further comprising determining if a network communication is associated with an authenticated user by contacting a federated control device.

68. The method of Claim 63, further comprising:

transmitting the credentials to an authentication system;

receiving the user profile from the authentication system.

69. A method of providing network access comprising:

receiving a user profile;

provisioning a user with access to a network based on the user profile.

70. The method of Claim 69, further comprising establishing a traffic control rule based on the user profile.

71. The method of Claim 70, wherein the traffic control rule specifies a maximum upload bandwidth and maximum download bandwidth.

72. The method of Claim 70, further comprising:

receiving a packet;

determining that the traffic control rule applies to the packet based on an identifier extracted from the packet;

applying the traffic control rule to the packet.

73. The method of Claim 72, further comprising dropping the packet if the packet causes the maximum upload or download bandwidth limits to be exceeded.

74. The method of Claim 69, further comprising establishing user specific firewall rules based on the user profile and enforcing the user specific firewall rules.

75. The method of Claim 69, wherein the user profile comprises one or more attributes that govern the provisioning of user's access to the network.

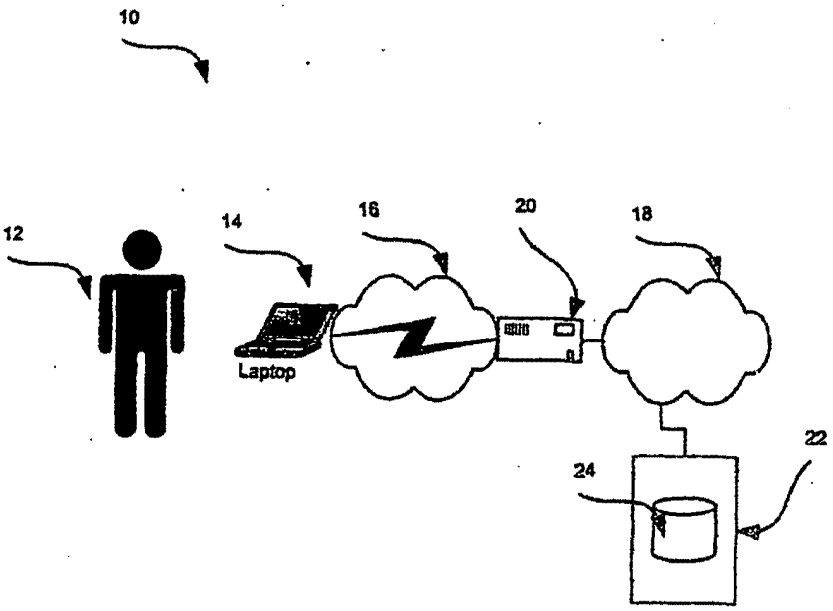


FIG. 1

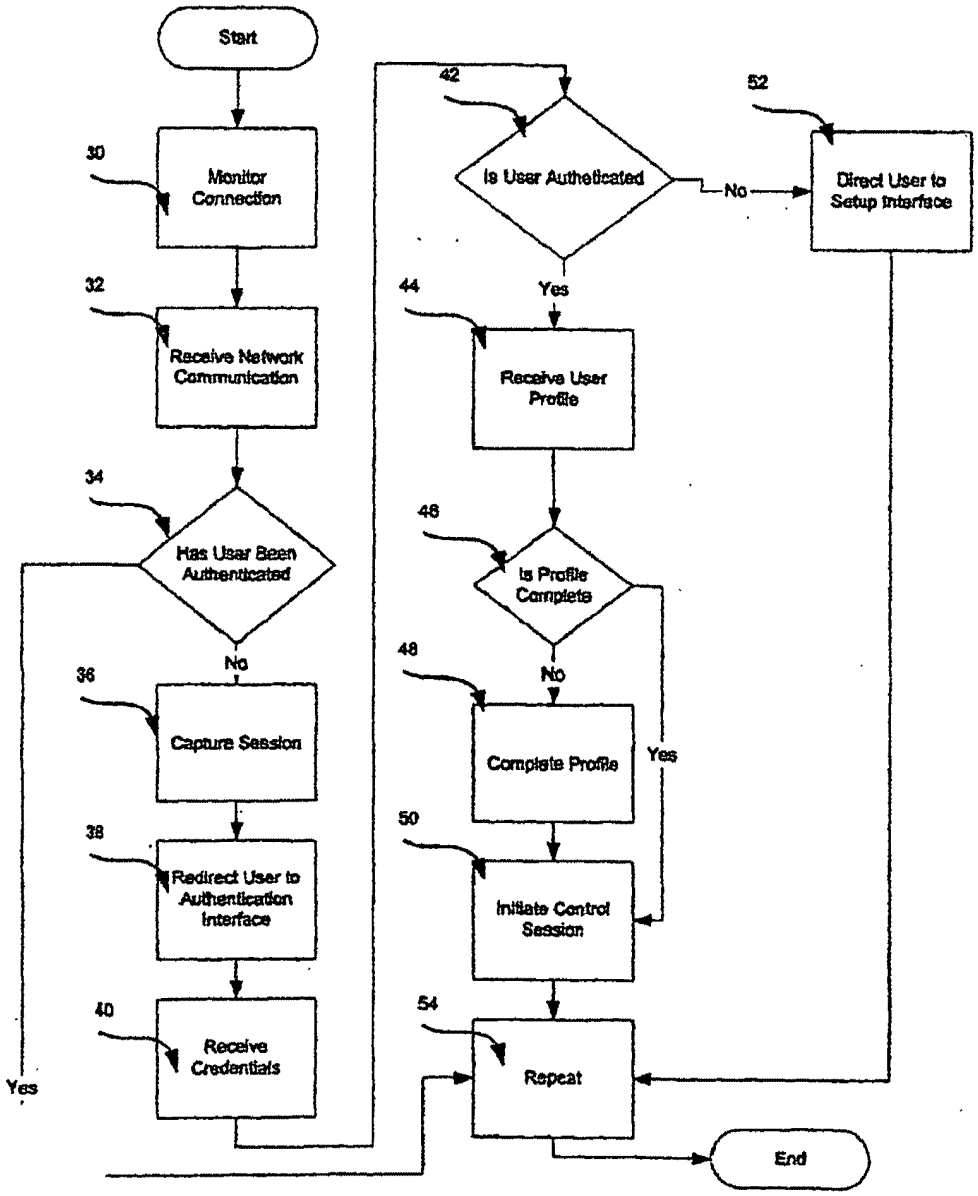

Start
30
Monitor Connection
32
Receive Network Communication
34
Has User Been Authenticated
No
Yes
36
Capture Session
38
Redirect User to Authentication Interface
40
Receive Credentials
42
Is User Authenticated
No
Yes
52
Direct User to Setup Interface
44
Receive User Profile
46
Is Profile Complete
No
Yes
48
Complete Profile
50
Initiate Control Session
54
Repeat
End

FIGURE 2

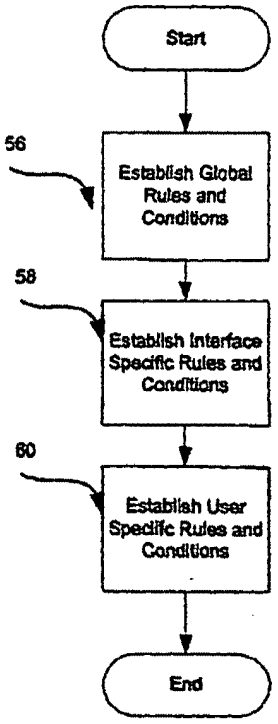

Start
56
Establish Global Rules and Conditions
58
Establish Interface Specific Rules and Conditions
60
Establish User Specific Rules and Conditions
End

FIGURE 3

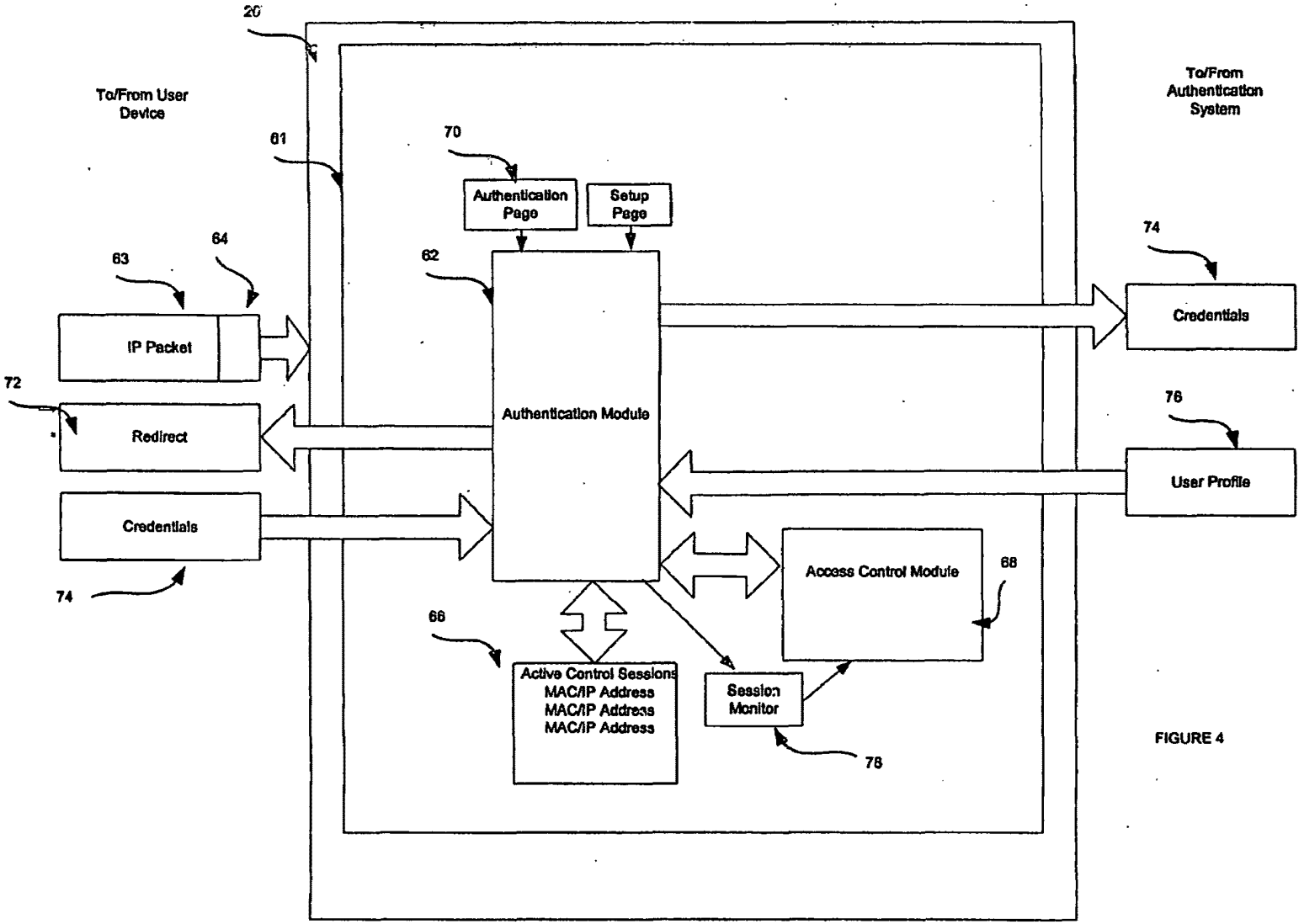

20
To/From User Device
61
70
Authentication Page
Setup Page
63
64
62
74
Credentials
IP Packet
72
Redirect
Authentication Module
76
User Profile
Credentials
74
Access Control Module
68
66
Active Control Sessions
MAC/IP Address
MAC/IP Address
MAC/IP Address
Session Monitor
78
To/From Authentication System

FIGURE 4

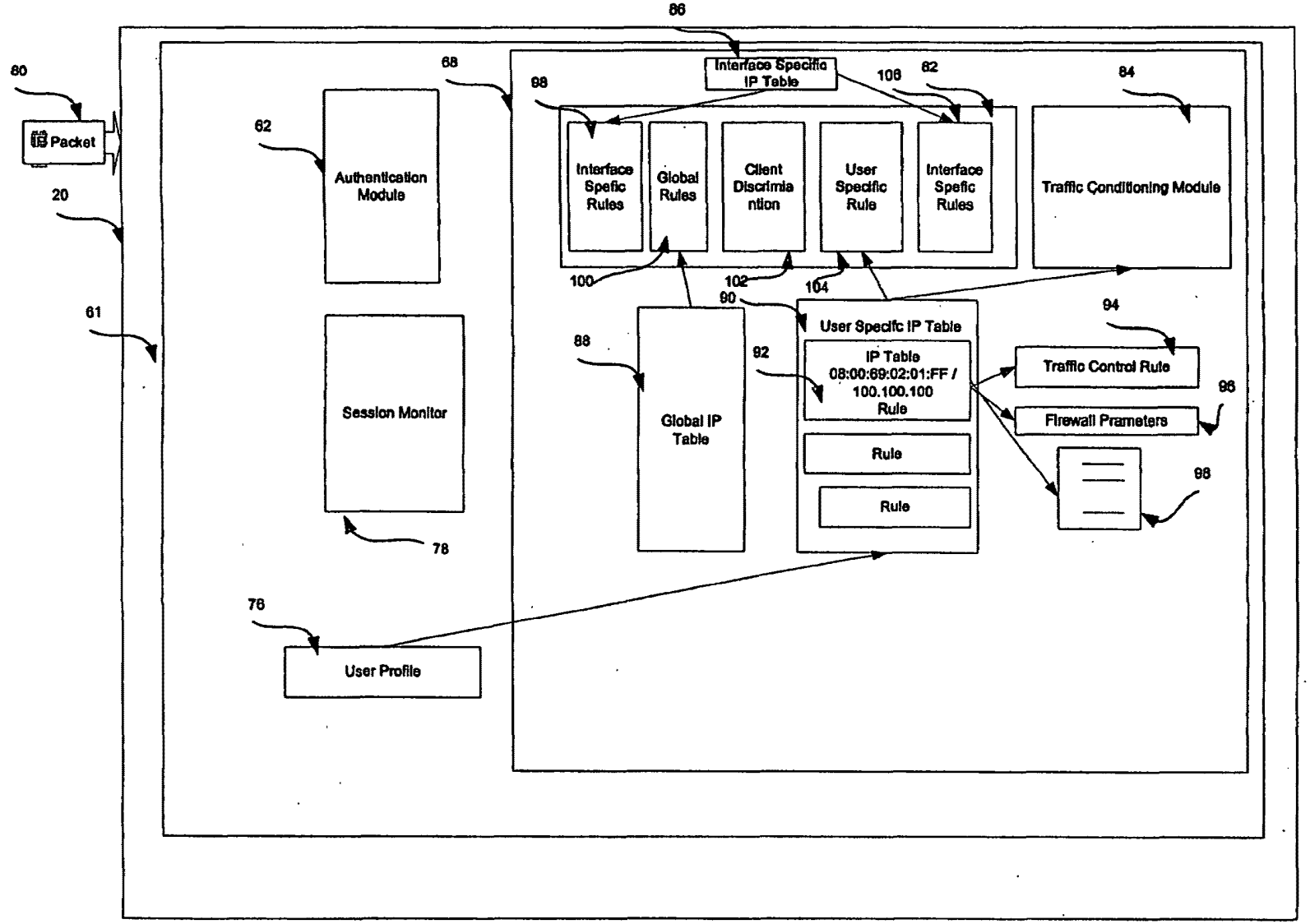

86
80
Packet
20
61
68
62
Authentication Module
Session Monitor
78
76
User Profile
98
Interface Specific IP Table
106
82
84
Interface Spefic Rules
Global Rules
Client Discrimination
User Specific Rule
Interface Spefic Rules
Traffic Conditioning Module
100
102
104
90
User Specific IP Table
88
Global IP Table
92
IP Table 08:00:69:02:01:FF / 100.100.100 Rule
Rule
Rule
94
Traffic Control Rule
Firewall Prameters
96
98

FIGURE 5

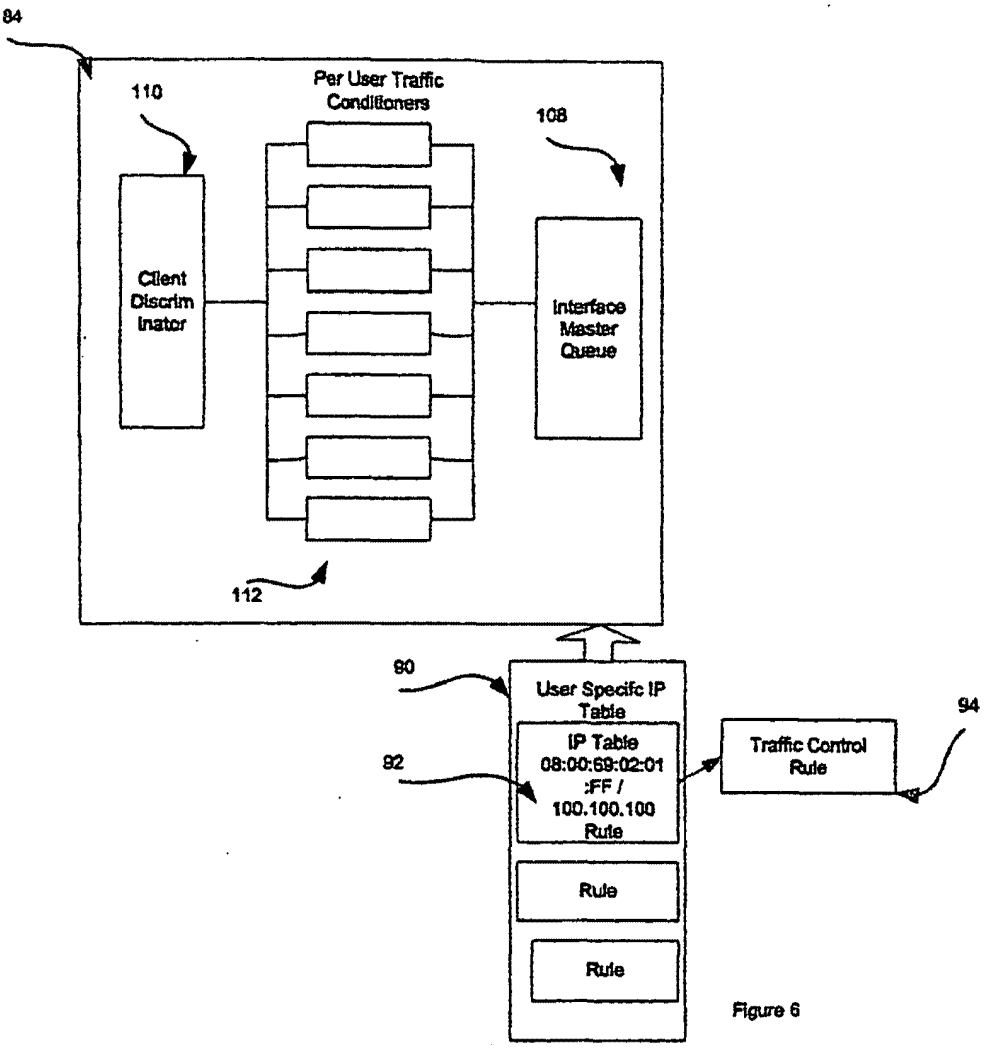

84
110
Per User Traffic Conditioners
108
Client Discrim inator
Interface Master Queue
112
90
User Specifc IP Table
IP Table 08:00:69:02:01 :FF / 100.100.100 Rule
92
Traffic Control Rule
94
Rule
Rule

Figure 6

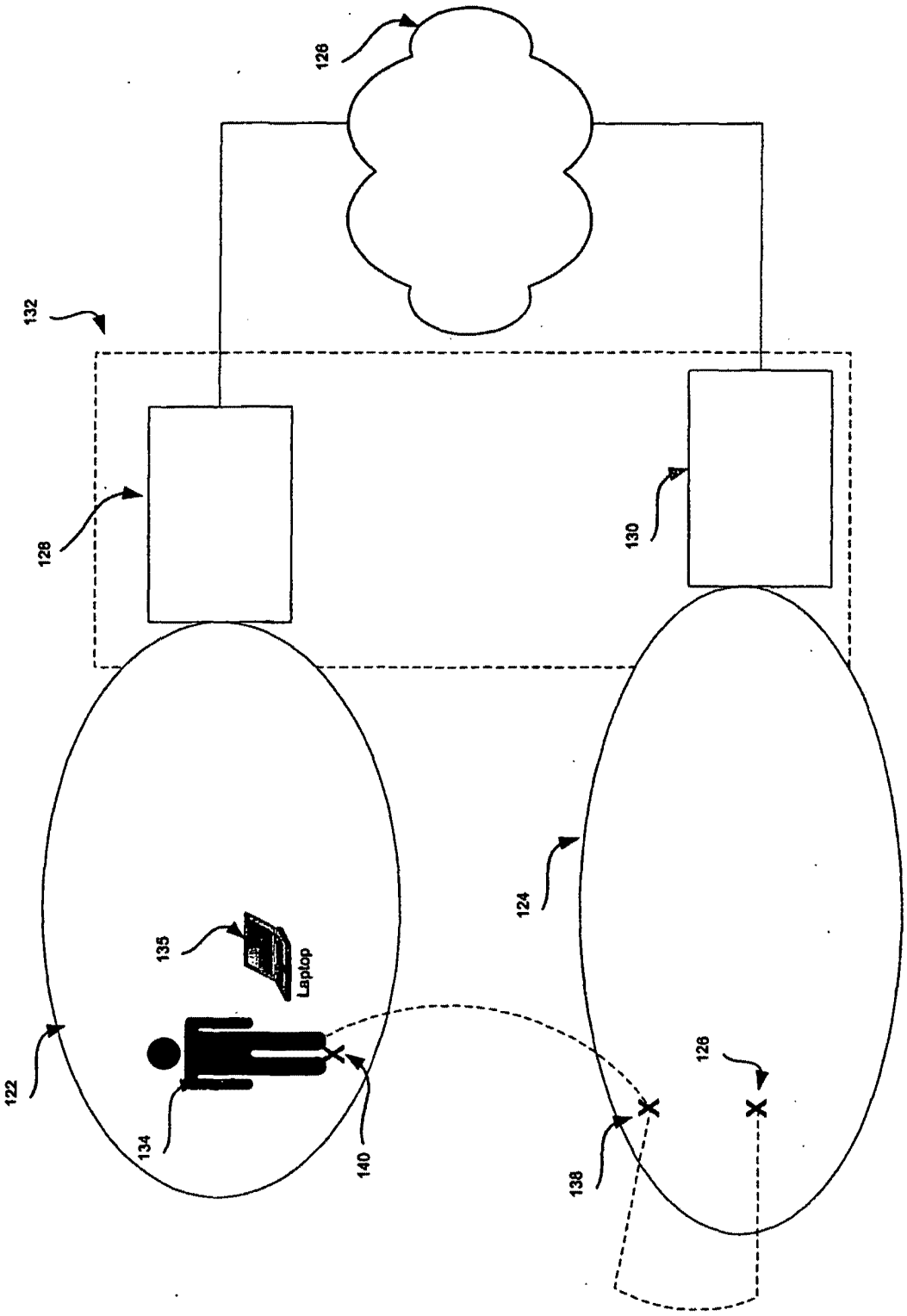
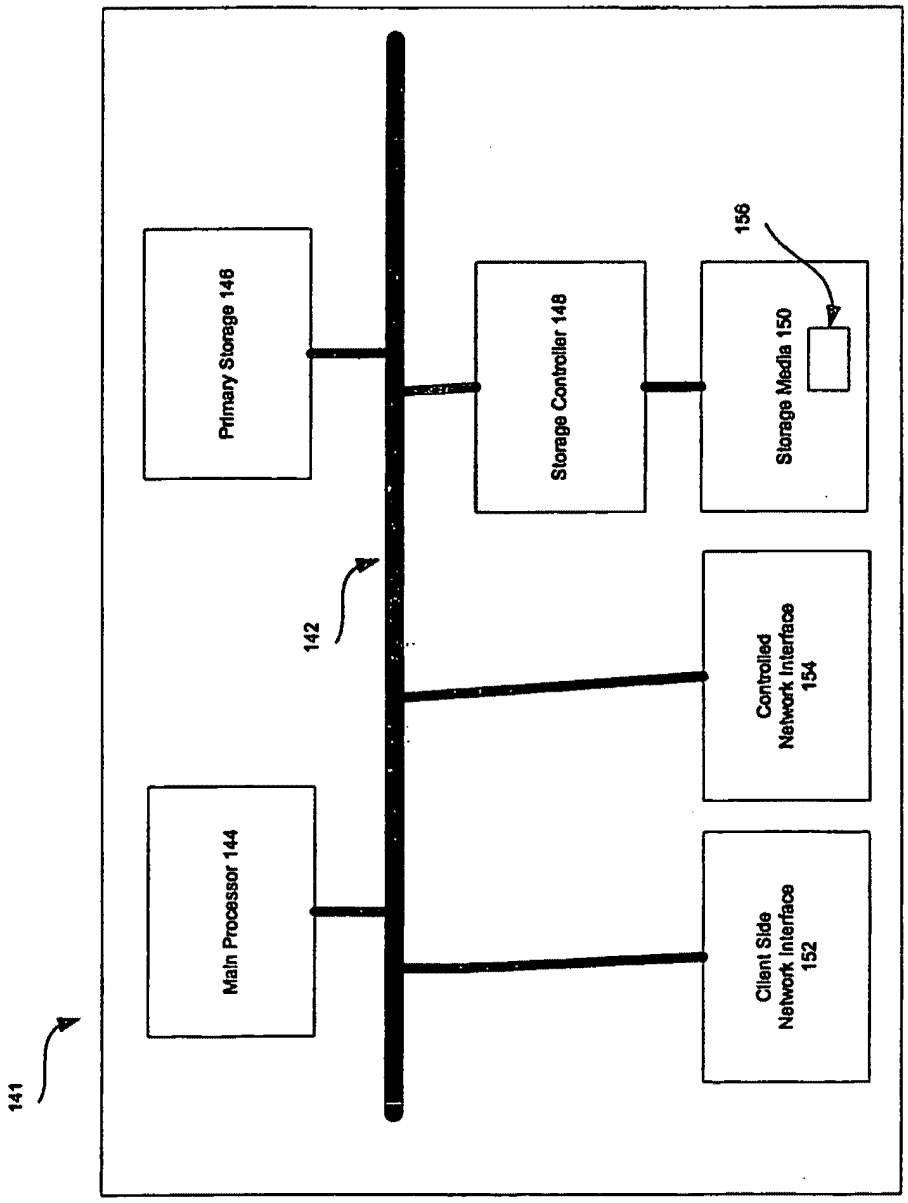

126
132
128
130
124
135
Laptop
122
134
140
138
126

FIGURE 8


141
142
Main Processor 144
Primary Storage 146
Storage Controller 148
156
Storage Media 150
Controlled Network Interface 154
Client Side Network Interface 152

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 April 2004 (29.04.2004)

PCT

(10) International Publication Number
WO 2004/036371 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/032912

(22) International Filing Date: 16 October 2003 (16.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/418,968	16 October 2002 (16.10.2002)	US
10/687,002	16 October 2003 (16.10.2003)	US

(71) Applicant *(for all designated States except US)*: **ROCKSTEADY NETWORKS, INC.** [US/US]; 3410 Far West Boulevard, Suite 210, Austin, TX 78731 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TA, Tuan** [US/US]; 10050 Great Hills Trail #103, Austin, TX 78759 (US). **TURLEY, Patrick** [US/US]; 5118 Saddleridge Cove, Austin, TX 78759 (US). **CLENDINNING, Kerry** [US/US]; 12504 Glacier Parke Cove, Austin, TX 78726 (US). **LOONEY, Kelly** [US/US]; 10737 Chestnut Ridge, Austin, TX 78726 (US).

(74) Agent: **ADAIR, John, L.**; Gray Cary Ware & Freidenrich, LLP, 1221 South MoPac Expressway, Suite 400, Austin, TX 78746-6875 (US).

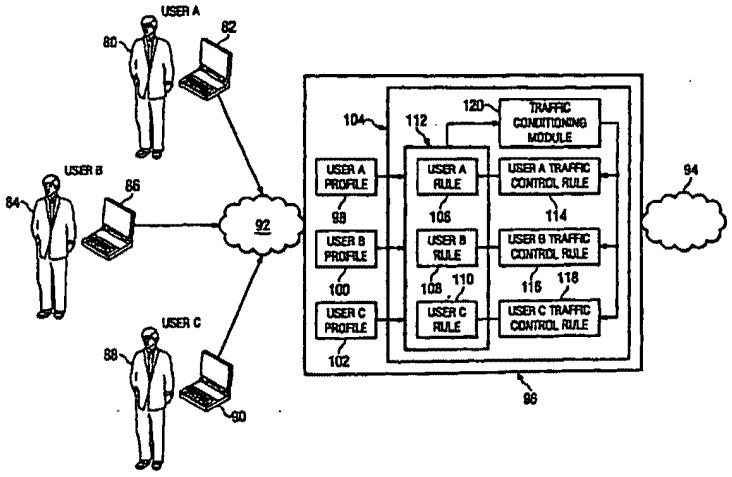
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR DYNAMIC BANDWIDTH PROVISIONING



(57) Abstract: One embodiment of the present invention provides a device for allocating bandwidth on a per user basis. The device can be a computing device that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, and a storage medium accessible by the processor that contains a set of computer instructions. The computer instructions can be executable by the processor to retrieve a set of user profiles. Based on the user profile for each user, the computer instructions can be executable to establish at least one bandwidth limit for each user. For each user, the computer instructions can be further executable to regulate bandwidth usage associated with that user based on the at least one bandwidth limit established for that user. The computer instructions can also be executable to update the at least one bandwidth limit.

WO 2004/036371 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DESCRIPTION

SYSTEM AND METHOD FOR DYNAMIC BANDWIDTH PROVISIONING

FIELD OF THE INVENTION

Embodiments of the present invention relate to providing network access. More particularly, embodiments of the present invention relate to provisioning bandwidth to users accessing a network. Even more particularly, embodiments of the present invention relate to dynamically provisioning bandwidth on a per user basis.

BACKGROUND OF THE INVENTION

The communication of data over networks has become an important, if not essential, way for many organizations and individuals to communicate. The Internet is a global network connecting millions of computers using a client-server architecture in which any computer connected to the Internet can potentially receive data from and send data to any other computer connected to the Internet. The Internet provides a variety methods in which to communicate data, one of the most ubiquitous of which is the World Wide Web. Other methods for communicating data over the Internet include e-mail, usenet newsgroups, telnet and FTP.

Users typically access the Internet either through a computer connected to an Internet Service Provider ("ISP") or computer connected to a local area network ("LAN") provided by an organization, which is in turn, connected to the ISP. The ISP provides a point of presence to interface with the Internet backbone. Routers and switches in the backbone direct data traffic between the various ISPs.

To access a LAN and, in turn, the Internet, many prior art access control systems require a user to connect his or her computer to a wired network (e.g., through an Ethernet port) and enter a user name and password. If the user name and password match a user name and password in an authentication database, the user will be provided access to the network. These systems typically assume that a user is tied to a particular physical port, such as a port in the user's office. Based on this assumption, provisioning of bandwidth to the user occurs by physically provisioning the port to which the user is connected. If the user moves to a different port, the user will typically be provided with the bandwidth provisioned to the new port. Thus, provisioning of bandwidth is done on a per port rather than a per user basis.

An increasing number of organizations (e.g., businesses, governmental organizations) wish to provide access to LANs and the Internet to various classes of users (internal users, contractors, customers, visitors). For example, many cafés have public wireless networks to allow patrons to access the Internet, receive email and perform other network activities. While users may be asked to authenticate to use the network, bandwidth is provisioned to the wireless routers, not the individual users. This means that one user connected to a particular router can consume a majority of the bandwidth (e.g., downloading pictures from the Internet), slowing down the wireless network for other users connected to that router.

Because bandwidth is provisioned on a per port rather than per user basis, current systems can not reprovision bandwidth to particular users as more users are added to the same port (e.g., as more users connect to the same wireless router). Continuing with the previous example of a public wireless LAN at a café, current systems can not reprovision bandwidth to individual users as more café patrons connect to the LAN. This can cause LAN performance to suffer for all users.

DISCLOSURE OF THE INVENTION

Embodiments of the present invention provide a system and method of providing bandwidth allocation that eliminates, or at least substantially reduces, the shortcomings of prior art bandwidth provisioning systems and methods. More particularly, one embodiment of the present invention provides a device for allocating bandwidth on a per user basis. The device can be a computing device that comprises a processor, a first network interface (e.g., an Ethernet interface, T1 interface, wireless interface or any other network interface known in the art) coupled to the processor, a second network interface (e.g., an Ethernet interface, T1 interface, wireless interface or any other network interface known in the art) coupled to the processor, and a storage medium (e.g., hard disk drive, RAM, ROM, optical storage and or any other storage medium known in the art). The storage medium can be accessible by the processor and can contain a set of computer instructions.

The computer instructions, according to one embodiment of the present invention, can be executable by the processor to retrieve a set of user profiles, wherein each user profile corresponds to a specific user in a set of users. Each user profile can contain an arbitrary number of attributes that can specify bandwidth limitations for the corresponding user. Based on the user profile for each user, the computer instructions can be executable to establish at least one bandwidth limit for each user and control bandwidth usage by that user accordingly. The computer instructions can also be executable to update the at least one bandwidth limit for one or more users.

Another embodiment of the present invention can include computer instructions stored on a computer readable medium (e.g., RAM, ROM, hard disk drive, magnetic storage device, optical storage device or other computer readable medium known in the art). The computer instructions can be executable by a processor to retrieve a set of user profiles, wherein each user profile corresponds to a specific user in a set of users. Each user profile can contain an arbitrary number of attributes that can specify bandwidth limitations for the corresponding user. Based on the user profile for each user, the computer instructions can be executable to establish at least one bandwidth limit for each user. For each user in the set of users, the computer instructions can be further executable to regulate bandwidth usage associated with that user based on the at least one bandwidth limit established for that user. The computer instructions can also be executable to update the at least one bandwidth limit for one or more of the users.

Yet another embodiment of the present invention can include a method comprising retrieving a set of user profiles, wherein each user profile corresponds to a specific user in a set of users; establishing at least one bandwidth limit for each user in the set of users based on the corresponding user profile for that user; for each user in the set of users, regulating bandwidth usage associated with that user based on the at least one bandwidth limit established for that user; and updating the at least one bandwidth limit for at least one user from the set of users.

Yet another embodiment of the present invention comprises computer instructions stored on a computer readable medium (e.g., RAM, ROM, hard disk drive, magnetic storage device, optical storage device or other computer readable medium known in the art). The computer instructions can be executable by a processor to establish a bandwidth limit for a user based on a user profile for the user; receive a first network communication; determine if the first network communication causes the bandwidth limit to be exceeded; if the first network communication causes the bandwidth limit to be exceeded, drop the network communication; and update the bandwidth limit for the user.

Embodiments of the present invention provide an advantage over prior art bandwidth allocation systems and methods by allowing bandwidth to be provisioned and dynamically updated on per user basis.

Embodiments of the present invention provide another advantage over prior art bandwidth allocation systems and methods by allowing bandwidth usage to be metered on a per user basis.

Embodiments of the present invention provide another advantage by allowing users to be allocated a predefined amount of bandwidth on wired and wireless networks.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention and the advantages thereof may be acquired by referring to the following description, taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

FIGURE 1 is a diagrammatic representation of a system for providing bandwidth allocation according to one embodiment of the present invention;

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing per user bandwidth allocation;

FIGURE 3 is a diagrammatic representation of one embodiment of a software system for providing per user bandwidth allocation;

FIGURE 4 is a diagrammatic representation of traffic conditioning module, according to one embodiment of the present invention;

FIGURE 5 is a diagrammatic representation of a system for dynamically allocating bandwidth to users on a per user basis, according to one embodiment of the present invention;

FIGURES 6A-6D illustrate various embodiments of bandwidth shaping; and

FIGURE 7 is a diagrammatic representation of one embodiment of a control device that can provide user based provisioning of bandwidth.

DETAILED DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are illustrated in the FIGURES, like numerals being used to refer to like and corresponding parts of the various drawings.

Embodiments of the present invention provide a system and method for providing bandwidth shaping on a per user basis. For purposes of this application, "bandwidth shaping" refers to the process of determining bandwidth allocations. According to one embodiment of the present invention, a control device can be located between a network (e.g., the Internet, a LAN or other network known in the art) and users. The users themselves may be located on a network or subnet or may connect directly to the control device. When a particular user attempts to access the network behind the control device (i.e., the controlled network), the control device can assign a bandwidth to the user based on a user profile. As more users attempt to access the controlled network through the control device, the

control device can dynamically alter the bandwidth allocations among users. Additionally, the control device can reallocate bandwidth on a per user basis to account for various factors, such as time of day, burstiness or other such factors known in the art.

By way of example, but not limitation, a control device can be coupled to a public wired or wireless LAN and the Internet to provide users with access to the Internet. When a user attempts to access the Internet over the public LAN, the control device can retrieve a user profile for the user and assign a bandwidth to the user. As additional users attempt to access the Internet, the control device can reassign bandwidths to the user.

Embodiments of the present invention provide an advantage over prior art bandwidth shaping systems and methods by allocating bandwidth on a per user basis. Additionally, embodiments of the present invention provide an advantage by allowing the bandwidth allocations to be dynamically altered to account for, for example, changes in network state, user activity or number of users. Embodiments of the present invention can allocate and dynamically shape bandwidth for both wired and/or wireless networks.

FIGURE 1 is a diagrammatic representation of a system 10 for providing bandwidth allocation according to one embodiment of the present invention. In system 10, a user 12, using a user device 14 on network 16, can send a network communication that is destined for a device on a controlled network 18. It should be noted that a user can be a human user, a programmatic user, or other user. User device 14 can comprise a desktop, a laptop, a PDA, a cell phone, a desktop computer or any other computing device capable of network communications. Network 16 and network 18 can be any networks known in the art including, but not limited to, LANs, WANs, the Internet, global communications networks, wireless networks and/or any other communications networks known in the art. For the sake of example, network 16 can be a wireless network and controlled network 18 can be the Internet. An access control device 20 ("control device 20") can control access to network 18 by users of network 16.

According to one embodiment of the present invention, when user 12 connects to control device 20 (e.g., by sending a network communication destined for network 18 from user device 14), control device 20 can retrieve a user profile for user 12 that governs the bandwidth allocations to user 12. In one embodiment of the present invention, control device 20 can receive the user profile for user 12 from an authentication database 24 at an authentication system 22 based on a set of user credentials provided by user 12 (e.g., password, user id, biometric data, certificates and or other user provided or hardware credentials known in the art). In another embodiment of the present invention, the user profile for user 12 can be stored at control device 10 in, for example, a local authentication database.

Example authentication technologies include LDAP, Remote Authentication Dialup Internet User Specification ("RADIUS"), Microsoft Active Directory Service, Tivoli Access Manager, and Cisco TACACS/TACACS+. Authentication can occur as described in United States Patent Application Serial No._____, entitled "System and Method for Providing Access Control," filed October 10, 2003, to MacKinnon et al., which is hereby fully incorporated by reference herein (the "Access Control Application").

Based on the user profile, control device 20 can establish a traffic control rule specifying maximum upload and download bandwidths for user 12. When network communications are received from user 12, control device 20 can determine if the maximum upload bandwidth has been exceeded and, if so, drop or queue the communication. When communications to user 12 are received from controlled network 18, control device 20 can determine if the maximum download bandwidth has been exceeded and, if so, drop or queue the communication. If the bandwidth allocations are not exceeded, control device 20 can pass the communication to/from user 12.

FIGURE 2 is a flow chart illustrating one embodiment of a method for providing per user bandwidth allocation. In one embodiment of the present invention, a control device (e.g., control device 20 of FIGURE 1) can authenticate a user (step 26) based on a network communication from a network application such as a web browser, ftp client, telnet client, mail user agent or other publicly available or proprietary network application running on a user device (e.g., laptop 14). Authentication can occur in any manner known in the art and, in one embodiment, can be carried out by the control device as described in the Access Control Application.

At step 28, the control device can retrieve a user profile. The user profile can be retrieved from remote storage (e.g., a remote authentication system) or from local storage (e.g., a local authentication database). The user profile can contain attributes that govern bandwidth allocation to an associated user. For example, the user profile can contain indicators of the upload and download bandwidth to which the user is entitled. The user profile can be received in a canonical format as an HTTP Post from the authentication system to the control device or in any manner known in the art.

According to one embodiment of the present invention, each user profile can have a predefined set of attributes. In some cases, the retrieved profile may not provide values for each of these attributes. Therefore, the control device can determine if the received user profile is complete, and, if it is not complete, can fill in the missing attribute values with default values, which can be part of the control device's local configuration or may be retrieved from remote storage by the control device during, for example, its initialization or startup phase.

At step 30, the control device can initiate a control session for the authenticated user. The control session can have a specified time limit, a time out limit and/or other session features known in the art. While the control session is active, the control device can govern a user's access to a network according to the user profile associated with that user and defaults and monitor the control session for characteristics such as bandwidth used or network session characteristics known in the art. The control session can be tracked by credentials, IP address, MAC address and/or other identifier.

At step 32, the control device can establish user specific rules and conditions based on attributes in the user profile. According to one embodiment of the present invention, the control device can map the attributes to a traffic control rule. By way of example, but not limitation, a user profile can contain attributes to specify upload and download bandwidth allocations for a user that can be mapped to a traffic control rule usable by a traffic conditioning module, such as the Linux based Traffic Control application, to regulate bandwidth usage by the corresponding user.

In one embodiment of the present invention, rules can be represented in an IP table. As would be understood by those of ordinary skill in the art, IP tables are essentially tables of rules that can be accessed by applications, such as a firewall or other application configured to access the IP tables. Rules in the IP table can be associated to a user through any arbitrary identifier. Using the example of FIGURE 1, the IP table rule(s) for user 12 can be bound to user 12 based on the MAC address and IP address of user device 14 and the credentials provided by user 12 for the particular control session. If, for example, laptop 14 is associated with the MAC address 08:00:69:02:01:FF and the IP address 100.100.100, the user specific rules for user 12 can be indexed under these addresses and, for example, a user name for the control session.

An IP table rule can reference other rules or parameters for providing user specific provisioning. As an example, the IP table rule for user 12 can reference a traffic control rule that dictates that the bandwidth allocated to user 12 is 128 Kbps for uploads and 512 Kbps for downloads. A traffic control application, such as the Linux based Traffic Control application, can access the traffic control rule through the IP table and enforce the bandwidth allocation.

It should be noted that a user specific rule in an IP table can reference rules or parameters usable by any number of applications or processes, such as firewalls, traffic conditioning modules, virus scan applications or other applications known in the art. For example, a user specific rule can contain or reference parameters usable by a virus scan application to provide user specific virus scanning. It should be further noted that the use of IP tables to index user specific rules for provisioning of bandwidth is provided by way of example only, and user specific rules can be implemented in any suitable manner, as would be understood by those of ordinary skill in the art.

The control device, at step 34, can receive a network communication to/from a particular user. The network communication can include, by way of example, but not limitation, an HTTP message, an email message, a telnet message, an FTP message, UDP message or other network communication known in the art. As would be understood by those of ordinary skill in the art, many network communications (e.g., HTTP requests/responses, email messages, instant chat messages and other network communication known in the art) are carried by one or more IP packets. Each IP packet includes a header with originating IP address, destination IP address, originating MAC address, destination MAC address and/or other addressing information.

At step 36, the control device can determine which user specific rule(s) to apply to the network communication. This can be done, for example, by extracting information from IP packets associated with the network communication. For a network communication from a particular user, the control device can compare the originating IP address and/or MAC address to the IP addresses and/or MAC addresses used to index user specific rules in the IP table. For a network communication to a user, the control device can compare the destination IP address and/or MAC address to the IP addresses and/or MAC addresses used to index user specific rules in the IP table. Based on this information, the control device can access the appropriate user specific traffic control rule(s).

In one embodiment of the present invention, a traffic control rule can specify user specific upload and download bandwidths. The control device can apply the traffic control rule(s) for a user to regulate bandwidth usage by the user. Thus, the control device, at step 38 can determine if a network communication causes the maximum upload bandwidth limit for an originating user or the maximum download bandwidth for a destination user to be exceeded. If appropriate bandwidth limit is exceeded, the control device can queue or drop the network communication (step 40). If, on the other hand, the bandwidth limit is not exceeded, the control device can transmit the network communication to its destination (step 42). This process can be repeated (step 44) for each network communication.

FIGURE 3 is a diagrammatic representation of one embodiment of a software system for providing per user bandwidth allocation. According to one embodiment of the present invention, a set of computer instructions 48 running at control device 20 can include a provisioning module 50 to provision or allocate bandwidth to users. Provisioning module 50, according to one embodiment of the present invention can establish rules associated with a particular user based on a user's profile. For example, provisioning module 50 can establish user specific rule 52 for user 12 based on user profile 54. The user specific rules, in one embodiment of the present invention can be indexed through an IP table 56. Each user specific rule can be associated with a user based on an arbitrary

identifier. For example, IP table 56 can contain user specific rule 52 for user 12 indexed to MAC address 08:00:69:02:01:FF and the IP address 100.100.100 of user device 14.

Each user specific rule in IP table 56 can optionally point to additional rules and parameters. For example user specific rule 52 can point to traffic control rule 58, which can also be based on user profile 54, to govern bandwidth provisioning to user 12. For example, user profile 54, in one embodiment of the present invention, can specify that user 12 is entitled to 128 Kbps for uploads and 512 Kbps for downloads. Provisioning module 50 map these attributes to a traffic control rule that contains these limitations and is usable by traffic conditioning module 60 to regulate bandwidth usage. One example of a traffic conditioning module that can be configured to access traffic control rules through an IP table is the Linux based Traffic Control application, however, any known or proprietary traffic conditioning set of computer instructions can be used by various embodiments of the present invention to apply per user traffic control rules.

In operation, provisioning module 50 can receive an IP packet 62 from user device 14. In one embodiment of the present invention, traffic conditioning module 60 can extract the originating IP address and/or MAC address from IP packet 62, access IP table 56 and locate user specific rule 54 on the originating MAC address and IP address. From user specific rule 52, traffic conditioning module 60 can locate traffic control rule 58 that specifies a maximum upload bandwidth of 128 Kbps. If packet 62 causes this limit to be exceeded, traffic conditioning module 60 can queue or drop packet 62. Otherwise, traffic conditioning module 60 can communicate packet 62 to its destination. Packet flow in the reverse direction can be processed in an analogous manner. For example, a packet arriving from the Internet destined for a user device 14 can be examined for destination IP address and MAC address. Based on these identifiers, traffic conditioning module 60 can access and apply traffic control rule 58 to limit the download bandwidth to 512 Kbps.

In the above example, user profile 54 contained attributes to govern the upload and download bandwidth allocations to user 12 regardless of the network application generating or receiving the IP packets. In another embodiment of the present invention, user profile 54 can prioritize network applications. As an example, user profile 54 can specify that IP packets associated with a game have priority over email messages, which have priority of HTTP messages. The priorities can be mapped to user specific traffic control rule 58. Continuing with the previous example, for the network application that is assigned a highest priority, traffic control rule 58 can specify that that network application is entitled to 320 Kbps for downloads and 80 Kbps for uploads, the network application assigned the next highest priority is entitled to 120 Kbps for downloads and 32 Kbps for uploads, and the network application assigned the lowest priority is entitled to maximum download and upload

bandwidths of 64 Kbps and 16 Kbps, respectively. Traffic conditioning module 60 can read each IP packet to determine the network application with which it is associated, using any application detection scheme known in the art, and apply the application specific bandwidth limitations for user 12 in traffic control rule 58.

In another embodiment of the present invention, if user 12 exceeds the user specific bandwidth limits (e.g., 128 Kbps for uploads or 512 Kbps for downloads), traffic conditioning module 60 can simply drop packets associated with lower priority network applications until the upload or download bandwidth usage falls within the specified limit rather than assigning specific bandwidth limits to each application or class of applications. The present invention can also employ any other prioritization scheme as would be understood by those of ordinary skill in the art.

In addition to provisioning bandwidth to users on a per user basis, the control device can provide session monitoring at, for example, monitoring module 61. Monitoring module 61 can perform any session monitoring functions known in the art, including, but not limited, tracking session time, tracking timeouts, generating reports and metering bandwidth usage on a per session basis. One example of a monitoring module can be a Radius client. It should be noted that because bandwidth allocation occurs on a per user basis bandwidth metering can also occur on a per user basis. Any bandwidth metering scheme known in the art can be used.

FIGURE 4 is a diagrammatic representation of traffic conditioning module 60, according to one embodiment of the present invention. Conditioning module 60 can include interface master queue 68, user discriminator 70 and user specific conditioners 72. User discriminator 70 can read a packet header to determine the appropriate user specific conditioner that will process the packet based on, for example, the IP address and MAC address of the packet. The user conditioner 72 can access the appropriate traffic control rule from IP table 56 to enforce user specific traffic conditions (i.e., upload and download bandwidth limits).

According to one embodiment of the present invention, conditioning module 60 can locate the user specific traffic control rule based on user specific IP table 56. For example, for a packet having the originating MAC address 08:00:69:02:01:FF and the IP address 100.100.100, traffic conditioning module 60 can access user specific rule 52 and, from user specific rule 52, user specific traffic control rule 58. The user specific traffic control rule can be enforced at the corresponding user specific conditioner.

For a particular network interface, each user can have an inward (i.e., download) and outward (i.e., upload) bandwidth allowance, based on attributes in the user's user profile. A bandwidth limit is the

maximum rate at which a user is permitted to transmit or receive network traffic over a particular interface. User specific traffic conditioners 72 ensure that, if a user exceeds his or her bandwidth allowance for that interface, further network traffic for the user in that direction will be queued or dropped until the average data rate falls back within the bandwidth allowance. Thus, traffic conditioning module 60 can regulate bandwidth on a per user basis.

Interface master queue 68 can control the flow of network traffic over a particular interface (e.g., a particular Ethernet interface, wireless interface T1 interface, or other interface known in the art). It can be configured to send out data at whatever rate is appropriate for the corresponding network connection. Interface master queue 68 can be feed IP packets by user specific conditioners 72, each of which can have its own queue to hold packets the conditioner has accepted, but interface master queue 68 is not ready to accept.

Interface master queue 68, according to one embodiment o the present invention, can also reallocate bandwidth to particular users based on excess capacity, usage patterns, time of day, user priorities or other factors known in the art. As an example, when bandwidth is available due to low demand by other users, a particular user may achieve rates in excess of the limits specified in the user's user profile. Excess bandwidth can be divided "fairly" between subscribers. When demand exceeds the available bandwidth, the bandwidth allocated to a user can throttled to or below the amount of bandwidth designated by the user profile.

It should be noted that the architectures of FIGURE 3, and FIGURE 4 are provided by way of example only and bandwidth provisioning and monitoring can be implemented using any suitable programming language and/or structure known in the art. In the example of FIGURE 3, provisioning module 50 provides traffic conditioning based on a set of IP tables. It should be noted, however, that the rules for traffic conditioning can be defined in any arbitrary manner usable by a traffic conditioning module. It should be further noted, that provisioning module 50 can provide additional services on a per user basis, such as virus scanning, worm detection, firewall services or any other service known in the art. Each of these additional services can access rules and parameters based, for example, on IP table(s). Moreover, the use of IP tables to index and provide access to rules and parameters for particular processes is also provided by way of example. In other embodiments of the present invention, a user profile can be mapped to rules and parameters for various applications in any suitable programming manner known in the art.

In the example of FIGURE 3, traffic conditioning module 60 applied the bandwidth limitations in traffic control rule 58 as hard limits. That is, regardless of overall available bandwidth, traffic conditioning module 60 will limit the upload and download bandwidths to 128 Kbps and 512 Kbps

limits specified in traffic control rule 58. In another embodiment of the present invention, the traffic conditioning module at, for example, interface master queue 68, can alter the bandwidth limits for a user dynamically to account for excess capacity, usage patterns, number of user, or any other factor.

FIGURE 5 is a diagrammatic representation of a system for dynamically allocating bandwidth to users on a per user basis, according to one embodiment of the present invention. In FIGURE 5, user 80 (User A) using user device 82, user 84 (User B) using user device 86 and user 88 (User C) using user device 90 on network 92 can send a network communications destined for locations on a controlled network 94. Network 92 and network 94 can be any networks known in the art including, but not limited to, LANs, WANs, the Internet, global communications networks, wireless networks and/or any other communications networks known in the art. For the sake of example, network 92 can be a wireless network and controlled network 94 can be the Internet. A control device 96 can control access by users on network 92 to controlled network 94 and allocate bandwidths to the users on a per user basis.

In one embodiment of the present invention, control device 96 can retrieve a user profile for each user on network 92 (e.g., user profile 98 for User A, user profile 100 for user B and user profile 102 for User C). For each user profile, a provisioning module 104 at control device 96 can establish a user specific rule (user specific rule 106 for User A, user specific rule 108 for User B and user specific rule 110 for User C) indexed, for example, in IP table 112. Additionally, based on the user profiles, provisioning module 104 can establish traffic control rules for each user (e.g., traffic control rule 114 for User A, traffic control rule 116 for User B and traffic control rule 118 for User C) which can be referenced by the respective user specific rule in IP table 112. Each traffic control rule can be based on the user profile and can specify bandwidth allocations for the corresponding user. It should be noted that the use of one or more IP tables to index traffic control rules through user specific rules is provided by way of example only, and the present invention can specify bandwidth allocations on a per user basis in any suitable manner.

In operation, traffic conditioning module 120 can receive packets to/from User A, User B and/or User C and process the packets according to the corresponding traffic control rules. For example, traffic conditioning module 118 can receive a packet from User A, access user specific rule 106 in IP table 112 based, for example, on a MAC address and IP address for user device 82, access traffic control rule 114 referenced by user specific rule 106, and apply traffic control rule 114 to drop the packet, queue the packet or communicate the packet to network 94 based on whether or not the packet causes bandwidth limits in traffic control rule 114 to be exceeded.

Each user profile, in one embodiment of the present invention, can specify that a corresponding user is entitled to a particular bandwidth. Provisioning module 104 can establish traffic control rules that contain these limitations. However, the traffic control rules if simply based on the user profiles may not account for a variety of network conditions, such as, for example excess capacity, new users, usage conditions and other such factors.

As an example, assume control device 96 has 1000 Kbps available as its overall download bandwidth capacity, user A is allocated a maximum of 500 kbps download bandwidth based on user profile 98, user B is allocated a maximum of 250 kbps download bandwidth based on user profile 100 and only User A and User B are using network 92 to access controlled network 94 (i.e., User C is not connected to network 92). In this case, based on the user profiles, traffic control rule 114 and traffic control rule 116 will specify maximum download bandwidths of 500 Kbps and 250 kbps respectively. If traffic conditioning module 120 applies traffic control rule 114 and traffic control 116 with download bandwidth limits of 500 kbps and 250 kbps, control device 96 will have an excess capacity of 250 kbps for downloads.

In one embodiment of the present invention, traffic conditioning module 120, at for example the interface master queue corresponding to network 94, can reassign the bandwidth limits to User A and User B to account for the excess bandwidth. For example, traffic conditioning module 120 can evenly divide the excess capacity to provide User A and User B with an additional 125 Kbps each for downloads. According to one embodiment, traffic conditioning module 120 can establish the new download bandwidth limits of 625 Kbps and 375 Kbps for User A and User B by modifying traffic control rule 114 and traffic control rule 116, respectively. Because, in this embodiment of the present invention, the traffic control rule is referenced for each user by the IP table, but is not part of the IP table, the new bandwidth limits for User A and User B can be implemented without modifying IP table 112.

As a further example, assume that based on their user profiles, User A is allocated 500 Kbps for downloads and User B has been allocated 250 Kbps for downloads, leaving an excess capacity of 250 Kbps. Assume that User C connects to network 92 to gain access to controlled network 94. Control device 96 can retrieve user profile 102 and, based on user profile 102, establish user specific rule 110 and traffic control rule 118 for User C. If user profile 102 specifies that User C is entitled to 500 Kbps for downloads, the overall provisioned bandwidth will exceed the available bandwidth at control device 96 (i.e., the overall provisioned bandwidth will be 1250 Kbps in comparison to the available 1000 Kbps). Therefore, traffic conditioning module 120 can reallocate bandwidth among the users by modifying the traffic control rules for each user.

In one embodiment of the present invention, where there is insufficient capacity to serve all users fully, the users must essentially "compete" for what is available. If the total available bandwidth is less than the sum of all nominal allowances (e.g., the total available bandwidth of 1000 Kbps is less than the allocated bandwidth of 1250 Kbps), then the effective bandwidth offered to each user can governed by the following:

$$W = \sum w_i \qquad \text{[EQ. 1]}$$

$$e_i = a_i w_i / W \qquad \text{[EQ. 2]}$$

where: w_i is the weight applied to bandwidth allowance i for a user using an interface (e.g., the interface to network 94); W is the sum of all weights on all bandwidth allowances on this interface; e_i is the effective bandwidth for allowance i; and a_i is the nominal bandwidth for allowance i. In the above example, User A's nominal bandwidth (a_i) allowance for using controlled network 94 is 500 Kbps. The weight w_i for each user for a given interface can be calculated based on, for example, a service factor specified in each user's user profile. If all user profiles specify the same service factor, then all users will have their bandwidth limits reduced by the same amount to bring the allocated bandwidth within the bandwidth capacity of the control device. If a user profile specifies a smaller service factor, then that user will lose a correspondingly less amount of bandwidth. If a user profile specifies that a user's bandwidth is incompressible, this means that, even if there is insufficient available bandwidth to serve all other users fully, this user's bandwidth allowance will not be reduced. This will result in more severe effective reductions for other users whose bandwidth allowances are not marked as incompressible.

In the above example, if each user profiles for User A, User B and User C specify the same service factor, traffic conditioning module 120 can reduce the maximum download bandwidth limit for each of User A, User B and User C by 83.3 Kbps (i.e., the total excess allocation of 250 Kbps divided evenly among the users). To effect this change, traffic conditioning module 120 can modify traffic control rule 114 to include a download bandwidth limit of 416.7 Kbps, traffic control rule 116 to include a download bandwidth limit of 166.6 Kbps, and traffic control rule 118 to include a download bandwidth limit of 416.7 Kbps, for a total bandwidth allocation of 1000 Kbps among User A, User B and User C. Thus, a control device can dynamically change the allocations of bandwidth on a per user basis to account for new users.

In the above examples, traffic conditioning module 120 dynamically calculated bandwidth allocations for Users A, B and C. In another embodiment of the present invention, control device 96 can receive a new user profile for a particular user and update the traffic control rule for that user to reflect

changes in the user profile. As an example, if control device 96 controls access to network 94 based on paid subscriptions by users, the initial user profile 98 for User A can specify upload and download bandwidth limits, say 250 Kbps for uploads and 500 Kbps for downloads. If User A then pays for more bandwidth during a session, user profile 98 can be updated by control device 96 or by another system (e.g., a backend system). The new user profile can now specify, for example, that User A is now entitled to 750 Kbps for downloads. Control device 96 can update traffic control rule 114 to reflect the change in maximum bandwidth for User A without requiring User A to reauthenticate to get the new bandwidth limits.

In yet another embodiment of the present invention, control device 96 can dynamically change per user bandwidth allocations if a higher priority user or user device is sending/receiving network communications. Assume, for example, User C is considered to have a higher priority than User A or User B. When User C connects to control device 96 with user device 94, User C can be allocated the full 500 Kbps for downloads specified in user profile 102. The download bandwidth allocations for User A and User B can be reduced to bring the total download allocation among all users to the 1000 Kbps capacity of user device 96. It should be noted that although the above examples discussed dynamic allocation of bandwidth in terms of downloads, upload bandwidth allocations can be similarly modified.

The program architecture of FIGURE 5 is provided by way of example only and dynamic bandwidth allocation on a per user basis can be implemented in any suitable programming manner known in the art. Additionally, control device 96 can dynamically change the bandwidth allocations to users according to any bandwidth shaping scheme known in the art. For example, control device 96 can adjust the bandwidth limits for users based on time of day, usage patterns or utilization averaging.

Dynamic bandwidth shaping based on time of day can allow control device 96 to provide particular users with additional bandwidth during peak hours. Allocating bandwidth based on usage patterns can allow a control device to set higher bandwidth limits for a user for a short period of time to account for, for example, bursty traffic. For short interactive traffic or short file transfers, this can give the user a high available bandwidth. If the user continues to use a high amount of bandwidth, the user's bandwidth limits can be lowered so that user does not use too much of the control device's bandwidth capacity for too long. Utilization averaging allows for better fairness in allocation of excess bandwidth based upon measured utilization rates of competing users over a period of time. If the control device affords a users a higher bandwidth than specified in the user's user profile, the control device can dynamically lower the bandwidth allocation for that user to a level lower than specified in the user's user profile to allow other users additional bandwidth.

In summary, control device 96 can retrieve a set of user profiles (e.g., user profile 98, user profile 100 and user profile 102) for a set of users (User A, User B and User C) and establish upload and/or download bandwidth limits for each user based on the corresponding user profile for that user (e.g., user profile 98 for user A, user profile 100, for User B and user profile 102 for User C). The control device can regulate bandwidth usage for each user based on the bandwidth limit(s) established for that user. Additionally, the control device, according to one embodiment of the present invention, can update the bandwidth limit(s) for one or more of the users based on new users connecting to control device 96, excess capacity, utilization averaging, time of day or other factors known in the art.

FIGURES 6A-6D illustrate various embodiments of bandwidth shaping, using the example of User A and User C from FIGURE 5. In this case, it is assumed, for the sake of example, that User B is not connected to the control device. FIGURE 6A illustrates example bandwidth demands for User A and User C respectively. User A has a constant bandwidth demand (e.g., a file transfer), whereas User C has bursty traffic (e.g., web traffic). Both user's are initially allocated the same amount of bandwidth based on their respective user profiles (i.e., 500 Kbps). The dashed lines represents User A's bandwidth demand and User C's bandwidth demand for six time periods (period 122, period 124, period 126, period 128, period 130 and period 132). The control device, by way of example, but not limitation, has a maximum capacity of 1000 Kbps.

FIGURE 6B illustrates one embodiment of dynamically allocating bandwidth between User A and User C. The dashed lines represent the bandwidth demands from FIGURE 6A and the squared lines represent the bandwidth allocated to each user in a given time period. During all time periods User A is demanding more than the 500 Kbps specified in the User A's user profile. User C however, can be demanding more or less bandwidth in a given period. For example, in period 122, User C is demanding less bandwidth. Therefore, a control device can update the traffic control rules for User A and User C to allocate more bandwidth to User A and less bandwidth to User C. During time period 126, both User A and User C are demanding at least 500 Kbps of bandwidth, making the total bandwidth demand greater than the available 1000 Kbps. The control device can again update the bandwidth allocations for User A and User C to limit User A and User C to the 500 Kbps specified in each user's profile. The control device can continue to allocate bandwidths to User A and User C as shown in FIGURE 6B. In one embodiment of the present invention, this can be done by updating the traffic control rules for each user, as described in conjunction with FIGURE 5.

FIGURE 6C illustrates another embodiment of bandwidth shaping using utilization averaging. As shown in FIGURE 6C, there will be periods (e.g., time period 128 and period 130) in which User C is able to use more than 500 Kbps, even though User A is continuing to have high demand. The

allocation of bandwidth for each user can be based on a dynamic limit calculated for that user based on the user's utilization of bandwidth. The dynamic limit can be enforced whenever User A and User C compete for capacity (i.e., whenever their joint demands exceed 1000 Kbps). In one embodiment of the present invention, the dynamic limit for each user can be inserted into the traffic control rule for that user, whenever the user's compete for capacity. FIGURE 6D provides an example of the changing dynamic limit for User A, to produce the bandwidth allocation for User A shown in FIGURE 6C.

FIGURE 6D illustrates how a dynamic limit for User A can be changed in order to allow utilization averaging. In FIGURE 6D, the dashed line represents User A's demand, the solid line represents the dynamic limit for User A and the blocked line the represents the bandwidth allocated to User A. The demand and bandwidth allocation are the same as in Figure 6C for User A. The dynamic limit can be enforced for User A whenever User A and User C compete for bandwidth (i.e., when their demands exceed 1000 Kbps in this example). As shown in the example of FIGURE 6D, User A is permitted to take advantage of surplus bandwidth in periods 122 and 124 because User A and User C are not competing for capacity (see FIGURE 6C). The dynamic limit though not the bandwidth limit for User A is adjusted downward, based on the cumulative total of surplus bandwidth used.

At time period 126, the bandwidth allocation remains steady. During this time period, User C is only demanding 500 Kbps, so User A can be allocated the remaining 500 Kbps, even though the dynamic limit is below 500 Kbps. Both users can, therefore, be allocated 500 Kbps. When user C exceeds 500 Kbps (i.e., when User C competes for the excess bandwidth), the control device can enforce the dynamic limit for User A in time period 128. User A will see a throughput of less than 500 Kbps because the dynamic limit for User A is below 500 Kbps. During the time period in which User A is limited to less than 500 Kbps, the dynamic limit for User A can be slowly increased. The pattern follows another decrease and increase in periods 130 and 132.

In one embodiment of the present invention, whether a dynamic limit for a user is adjusted up or down can be based on whether a user uses more or less bandwidth than the bandwidth limit specified in that user's user profile. In another embodiment of the present invention, whether a dynamic limit for a user is adjusted up or down can be based on whether a user uses more or less bandwidth than his or her proportional share of the available capacity (e.g., more or less than 50% if there are two users). The dynamic limit can be enforced for a user by modifying the traffic control rule for that user to include the dynamic limit as a bandwidth limit for the user. The traffic control rule for each user can be updated on an arbitrary schedule to enforce the changing dynamic limits.

It should be noted that, according to one embodiment of the present invention, a user who sustains a long period of high demand should not be subject to an ever-decreasing allocation of bandwidth. This could result in severe attenuation of the user's bandwidth the moment other users have an increased demand. In one embodiment of the present invention, two approaches can be used separately or in combination to remedy this: a lower limit on the dynamic bandwidth, and a rolling window for cumulative measurement. A lower limit would establish that a user's bandwidth allocation never drop below some point, for instance half of the rate specified in the user's user profile. A rolling window defines a limited period of time, say ten minutes, for the cumulative measurement. This would mean that the user's bandwidth allocation calculated as though prior to the last ten minutes, no surplus bandwidth had been used, and the bandwidth allocation for the user had been set as specified in the user's user profile.

It should be noted that above examples of dynamic bandwidth allocation are provided by way of example only. A control device can dynamically calculate bandwidth allocations for users according to any bandwidth shaping scheme known in the art. Moreover, updated bandwidth limits can be provided to a traffic conditioning module in any suitable manner, as would be understood by those of ordinary skill in the art.

FIGURE 7 is a diagrammatic representation of one embodiment of a control device 141 that can provide user based provisioning of bandwidth. For the purposes of example, control device 141 can comprise a main bus 142, a main processor 144, a primary storage medium 146, a secondary storage controller 148, a storage medium 150, a user side network interface 152 and a controlled network network interface 154. The network interfaces can include Ethernet interfaces, fibre channel interfaces, T1 interfaces, wireless interfaces or other network interfaces known in the art. Other devices may be connected to or be part of such a control device include, by way of example, but not limitation, controllers, a display, a mouse, a keyboard, and so forth. Additionally, control device 140 can include additional interfaces to communicate to additional networks using various protocols and can include interfaces for administrative functions.

The main processor 144 communicates with the other components by way of the main bus 142. This main processor 144 can be a general purpose processor, a limited processor such as an ASIC or microcontroller, or any other instruction execution machine. The primary storage 146 can provide transient memory or storage space for use by programs executing on the main processor 144. The main processor 144 communicates with the primary storage in any manner known in the art.

The secondary storage controller 148 connects a storage medium 150 such as a hard drive, CD-ROM, floppy, tape drive, optical storage medium, memory or other storage device to the main processor 144

by way of the main bus 142. The main processor 144 communicates with the secondary storage controller 148 by way of the main bus 142, and the secondary storage controller 148 is used to read and /or write the storage medium 150 on behalf of the main processor 144.

Control device 141 may communicate with other computing devices (e.g., user devices, network servers, etc.) by way of networks using network interfaces (e.g., user side network interface 152 and controlled network network interface 154 or other network interface). Computer instructions running on the main processor may then access other computers across the network in any of the conventional ways, e.g. by executing "protocols" which affect the transmission and reception of protocol data units, packages, etc. over the data transmission network.

In one embodiment of the present invention, storage medium 150 can store a set of computer instructions 156 that are executable by processor 144. During execution, portions of computer instructions 156 and data can be stored in primary storage 146, as would be understood by those of ordinary skill in the art. Processor 144 can execute computer instructions 156 to allocate bandwidths on a per user basis and enforce the bandwidth allocations.

Although shown as a standalone device in FIGURE 7, control device 141 may be integrated with and share components with other devices such as routers, servers, hubs or other devices known in the art. Additionally, computer instructions 156 can be distributed across multiple storage media and can be executed by multiple processors. One example of an exemplary control device is the Rocksteady NSA Server, from Rocksteady Networks, Inc. of Austin, Texas.

Control device 141, as described in the Access Control Application, can also provide any arbitrary services known in the art, including, but not limited to, web server functions, DHCP client for negotiation with ISPs, DHCP server to assign IP addresses to user devices, kernel based packet filtering and stateful inspection, IP sharing, NATplus, port redirection, information and attack logging, automatic updating, VPN masquerade, remote support and configuration, name server configuration and/or web content filtering. User profiles can be used by the control device to govern provisioning of network access on a user specific basis. By way of example, but not limitation, a user profile can contain attributes to specify upload and download bandwidth allocations for a user, firewall settings, whether the user can use transient VPNs, whether the user can use streaming services or voice over IP services, whether the user should be permitted to perform video teleconferencing, whether the control device should perform virus scanning or worm detection for the user, whether the user can utilize print services, surcharges for services or other settings.

While the present invention has been described with reference to particular embodiments, it should be understood that the embodiments are illustrative and that the scope of the invention is not limited to these embodiments. Many variations, modifications, additions and improvements to the embodiments described above are possible. It is contemplated that these variations, modifications, additions and improvements fall within the scope of the invention as detailed in the following claims.

WHAT IS CLAIMED IS:

1. A device for allocating bandwidth on a per user basis comprising:

a processor;

a first network interface coupled to the processor;

a second network interface coupled to the processor;

a storage medium accessible by the processor;

a set of computer instructions stored on the storage medium, executable by the processor to:

retrieve a set of user profiles, wherein each user profile corresponds to a specific user in a set of users;

establish at least one bandwidth limit for each user in the set of users based on the corresponding user profile for that user;

for each user in the set of users, regulate bandwidth usage associated with that user based on the at least one bandwidth limit established for that user; and

update the at least one bandwidth limit for at least one user from the set of users.

2. The device of Claim 1, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a new user profile.

3. The device of Claim 1, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a new user connecting to the device.

4. The device of Claim 1, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a time of day.

5. The device of Claim 1, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on utilization averaging for the corresponding user.

6. The device of Claim 1, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit by modifying a traffic control rule containing the at least one bandwidth limit.

7. The device of Claim 1, wherein the computer instructions are further executable to meter bandwidth usage on a per user basis.

8. The device of Claim 1, wherein the computer instructions are further executable to establish a traffic control rule for each user containing the at least one bandwidth limit for that user.

9. The device of Claim 8, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit for the at least one user by updating the traffic control rule for the at least one user.

10. The device of Claim 9, wherein the computer instructions are further executable to access each traffic control rule from an IP table based on an indicator associated with each traffic control rule.

11. The device of Claim 10, wherein the indicator comprises a MAC address.

12. The device of Claim 10, wherein the indicator comprises an IP address.

13. The device of Claim 1, wherein the computer instructions are further executable to:

receive a network communication from a first user from the set of users over the first network interface destined for a network connected to the second network interface;

access a traffic control rule for the first user that includes an upload bandwidth limit for the first user; and

determine if the network communication causes the upload bandwidth limit to be exceeded.

14. The device of Claim 13, wherein the computer instructions are further executable to receive the network communication from the user over a wireless network.

15. The device of Claim 1, wherein the computer instructions are further executable to:

receive a network communication over a network connected to the second network interface, destined for a first user from the set of users;

access a traffic control rule for the first user that includes a download bandwidth limit for the first user; and

determine if the network communication causes the upload bandwidth limit to be exceeded.

16. The device of Claim 15, wherein the computer instructions are further executable to receive the network communication from the user over a wireless network.

17. The device of Claim 1, wherein the computer instructions are further executable to monitor sessions on per user basis.

18. The device of Claim 1, wherein the computer instructions are further executable to:

prioritize bandwidth allocations for network applications for at least one user based the corresponding user profile for that user.

19. A device for allocating bandwidth on a per user basis comprising:

a storage medium;

a set of computer instructions stored on the storage medium, executable by a processor to:

retrieve a set of user profiles, wherein each user profile corresponds to a specific user in a set of users;

establish at least one bandwidth limit for each user in the set of users based on the corresponding user profile for that user;

for each user in the set of users, regulate bandwidth usage associated with that user based on the at least one bandwidth limit established for that user; and

update the at least one bandwidth limit for at least one user from the set of users.

20. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a new user profile.

21. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a new user connecting to the device.

22. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a time of day.

23. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on utilization averaging for the corresponding user.

24. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit by modifying a traffic control rule containing the at least one bandwidth limit.

25. The device of Claim 19, wherein the computer instructions are further executable to meter bandwidth usage on a per user basis.

26. The device of Claim 19, wherein the computer instructions are further executable to establish a traffic control rule for each user containing the at least one bandwidth limit for that user.

27. The device of Claim 19, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit for the at least one user by updating the traffic control rule for the at least one user.

28. The device of Claim 27, wherein the computer instructions are further executable to access each traffic control rule from an IP table based on an indicator associated with each traffic control rule.

29. The device of Claim 28, wherein the indicator comprises a MAC address.

30. The device of Claim 28, wherein the indicator comprises an IP address.

31. The device of Claim 19, wherein the computer instructions are further executable to:

receive a network communication from a first user from the set of users over a first network interface destined for a network connected to a second network interface;

access a traffic control rule for the first user that includes an upload bandwidth limit for the first user; and

determine if the network communication causes the upload bandwidth limit to be exceeded.

32. The device of Claim 31, wherein the computer instructions are further executable to receive the network communication from the user over a wireless network.

33. The device of Claim 19, wherein the computer instructions are further executable to:

receive a network communication over a network connected to a first network interface destined for a first user from the set of users;

access a traffic control rule for the first user that includes a download bandwidth limit for the first user; and

determine if the network communication causes the upload bandwidth limit to be exceeded.

34. The device of Claim 33, wherein the computer instructions are further executable to receive the network communication from the user over a wireless network.

35. The device of Claim 19, wherein the computer instructions are further executable to monitor sessions on per user basis.

36. The device of Claim 19, wherein the computer instructions are further executable to:

prioritize bandwidth allocations for network applications for at least one user based the corresponding user profile for that user.

37. A method for allocating bandwidth on a per user basis comprising:

retrieving a set of user profiles, wherein each user profile corresponds to a specific user in a set of users;

establishing at least one bandwidth limit for each user in the set of users based on the corresponding user profile for that user;

for each user in the set of users, regulating bandwidth usage associated with that user based on the at least one bandwidth limit established for that user; and

updating the at least one bandwidth limit for at least one user from the set of users.

38. The method of Claim 37, wherein the computer instructions are further executable to dynamically update the at least one bandwidth limit based on a new user profile.

39. The method of Claim 37, further comprising:

dynamically updating the at least one bandwidth limit based on a new user connecting to the device.

40. The method of Claim 37, further comprising dynamically updating the at least one bandwidth limit based on a time of day.

41. The method of Claim 37, further comprising dynamically updating the at least one bandwidth limit based on utilization averaging for the corresponding user.

42. The method of Claim 37, further comprising dynamically updating the at least one bandwidth limit by modifying a traffic control rule containing the at least one bandwidth limit.

43. The method of Claim 37, further comprising metering bandwidth usage on a per user basis.

44. The method of Claim 37, further comprising establishing a traffic control rule for each user containing the at least one bandwidth limit for that user.

45. The method of Claim 37, further comprising dynamically updating the at least one bandwidth limit for the at least one user by updating the traffic control rule for the at least one user.

46. The device of Claim 45, further comprising accessing each traffic control rule from an IP table based on an indicator associated with each traffic control rule.

47. The method of Claim 46, wherein the indicator comprises a MAC address.

48. The method of Claim 46, wherein the indicator comprises an IP address.

49. The method of Claim 37, further comprising:

receiving a network communication from a first user from the set of users over a first network interface destined for a network connected to a second network interface;

accessing a traffic control rule for the first user that includes an upload bandwidth limit for the first user; and

determining if the network communication causes the upload bandwidth limit to be exceeded.

50. The method of Claim 49, further comprising receiving the network communication from the user over a wireless network.

51. The method of Claim 37, further comprising:

receiving a network communication over a network connected to a first network interface destined for a first user from the set of users;

accessing a traffic control rule for the first user that includes a download bandwidth limit for the first user; and

determining if the network communication causes the upload bandwidth limit to be exceeded.

52. The method of Claim 51, further comprising further comprising receiving the network communication from the user over a wireless network.

53. The method of Claim 37, further comprising monitoring sessions on per user basis.

54. The method of Claim 37, further comprising prioritizing bandwidth allocations for network applications for at least one user based the corresponding user profile for that user.

55. A device comprising a set of computer instructions stored on a computer readable storage medium, the computer instructions executable by a processor to:

establish a bandwidth limit for a user based on a user profile for the user;

receive a first network communication;

determine if the first network communication causes the bandwidth limit to be exceeded;

if the first network communication causes the bandwidth limit to be exceeded, drop the network communication; and

update the bandwidth limit for the user.

56. The device of Claim 55, wherein the instructions are further executable to establish a traffic control rule for the user containing the bandwidth limit.

57. The device of Claim 56, wherein the computer instructions are further executable to access the traffic control rule from an IP table based on an indicator.

58. The device of Claim 57, wherein the indicator comprises a MAC address and an IP address associated with the user.

59. The device of Claim 55, wherein the user profile specifies network application priorities for network applications.

60. The device of Claim 55, wherein the user connects to the device via a network comprising a wireless network.

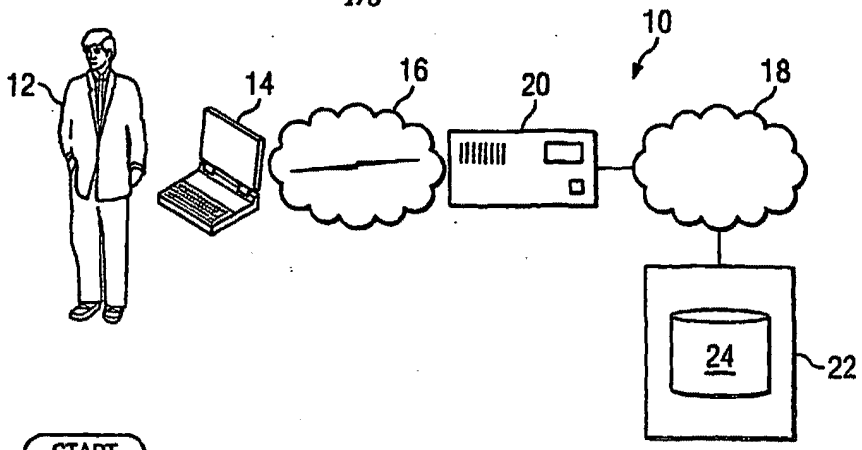

10
12
14
16
20
18
24
22

FIG. 1

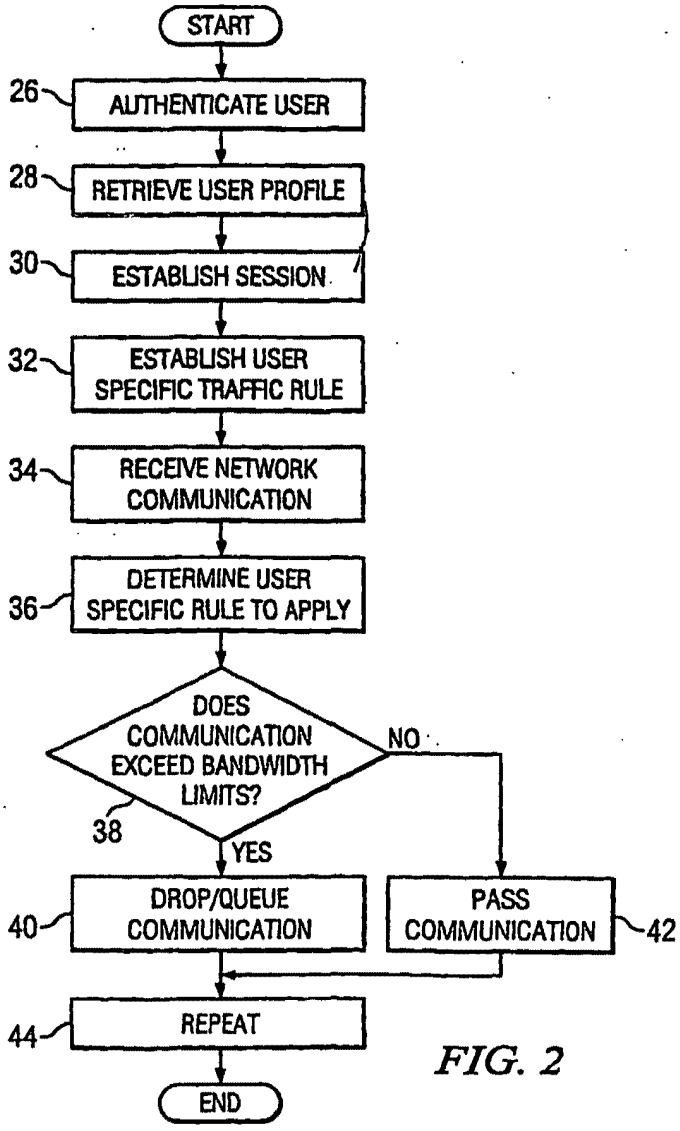

START
26
AUTHENTICATE USER
28
RETRIEVE USER PROFILE
30
ESTABLISH SESSION
32
ESTABLISH USER SPECIFIC TRAFFIC RULE
34
RECEIVE NETWORK COMMUNICATION
36
DETERMINE USER SPECIFIC RULE TO APPLY
DOES COMMUNICATION EXCEED BANDWIDTH LIMITS?
38
NO
YES
40
DROP/QUEUE COMMUNICATION
PASS COMMUNICATION
42
44
REPEAT
END

FIG. 2

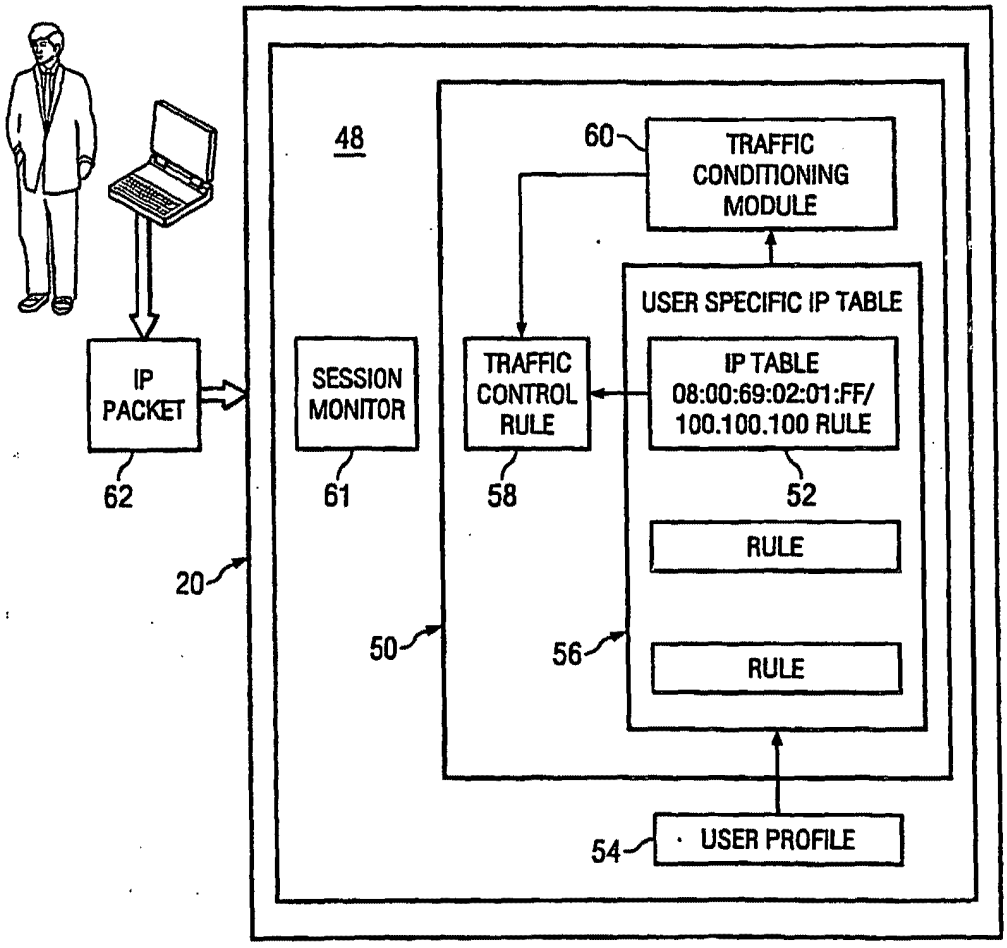

48
60
TRAFFIC CONDITIONING MODULE
USER SPECIFIC IP TABLE
IP PACKET
SESSION MONITOR
TRAFFIC CONTROL RULE
IP TABLE 08:00:69:02:01:FF/ 100.100.100 RULE
62
61
58
52
RULE
20
50
56
RULE
54
USER PROFILE

FIG. 3

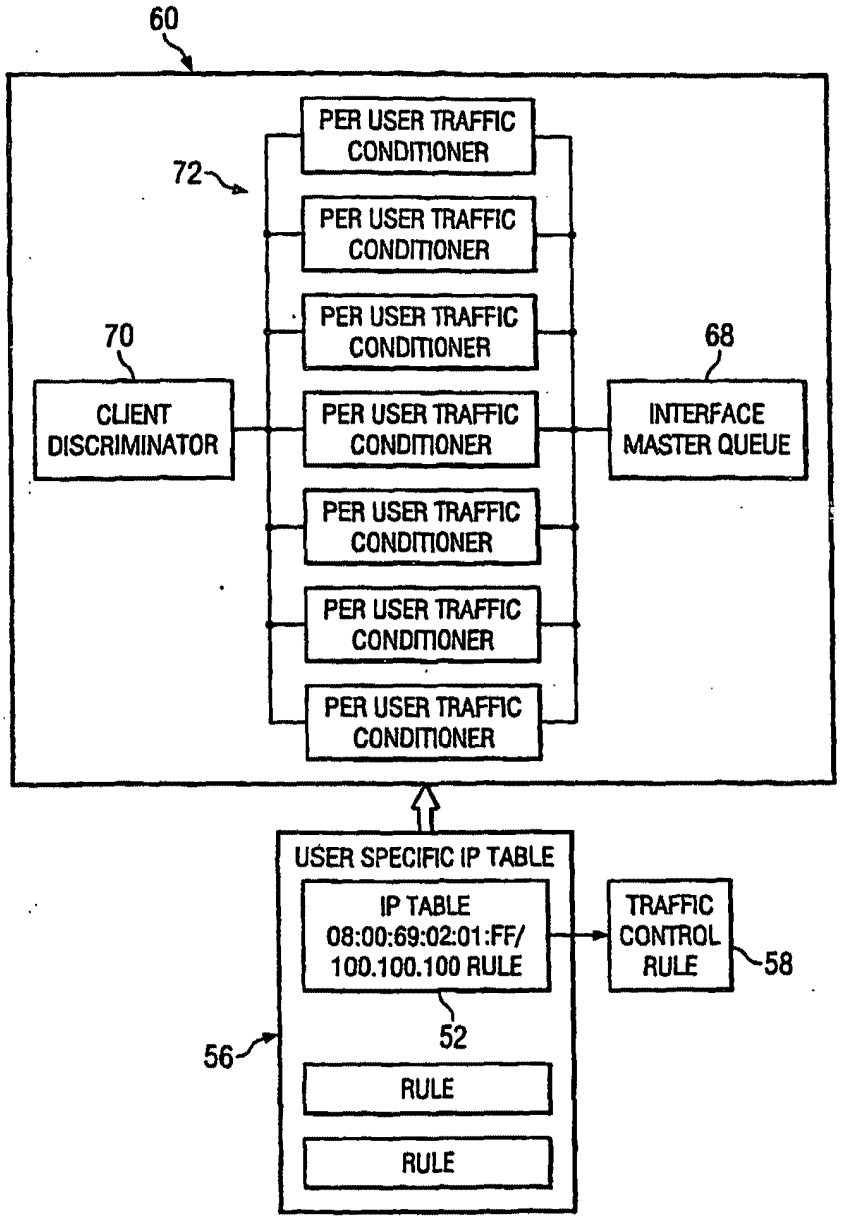

60
72
PER USER TRAFFIC CONDITIONER
PER USER TRAFFIC CONDITIONER
PER USER TRAFFIC CONDITIONER
70
68
CLIENT DISCRIMINATOR
PER USER TRAFFIC CONDITIONER
INTERFACE MASTER QUEUE
PER USER TRAFFIC CONDITIONER
PER USER TRAFFIC CONDITIONER
PER USER TRAFFIC CONDITIONER
USER SPECIFIC IP TABLE
IP TABLE 08:00:69:02:01:FF/ 100.100.100 RULE
TRAFFIC CONTROL RULE
58
52
56
RULE
RULE

FIG. 4

FORTINET EX1002 Page 438

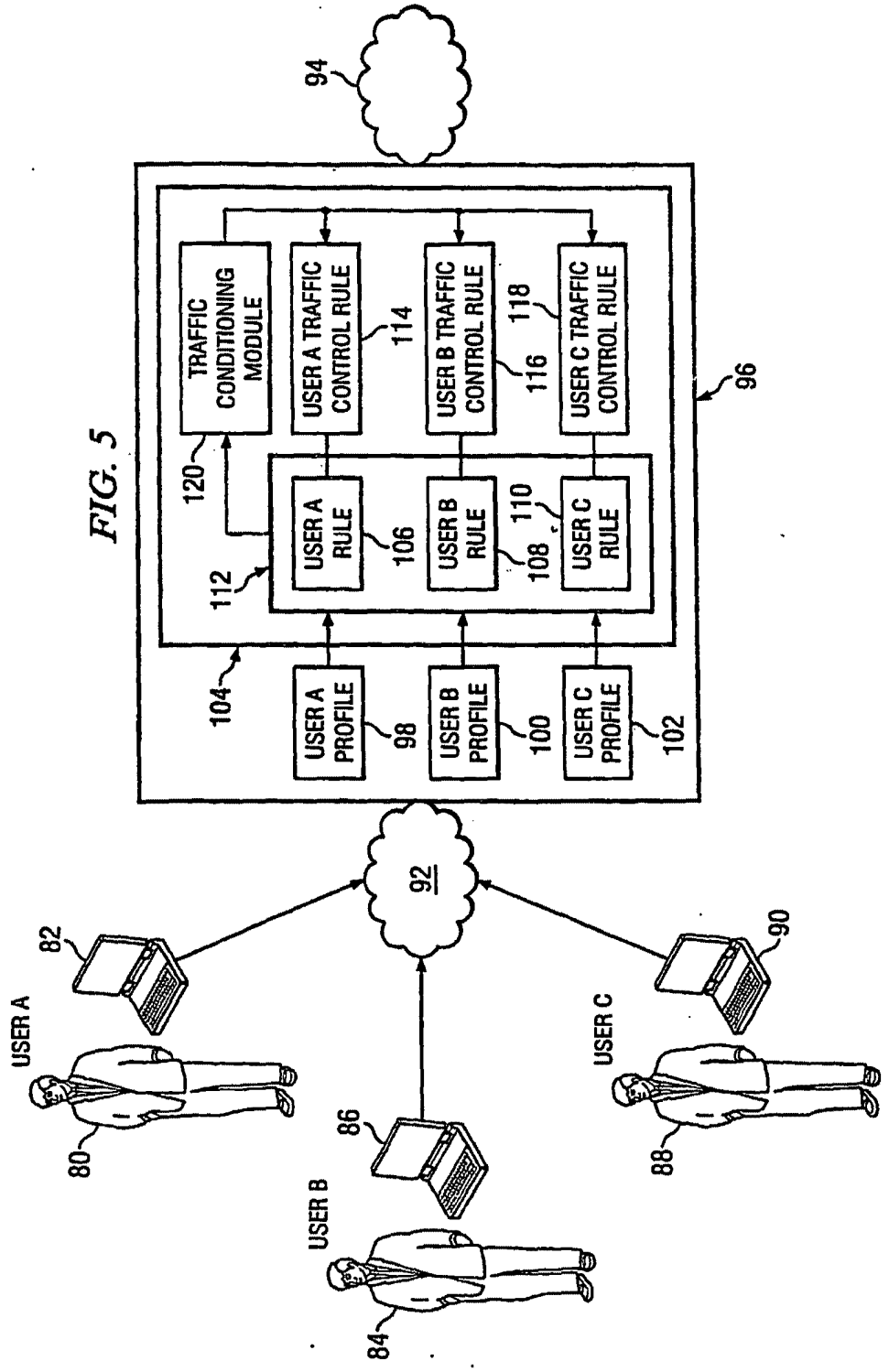


FIG. 5

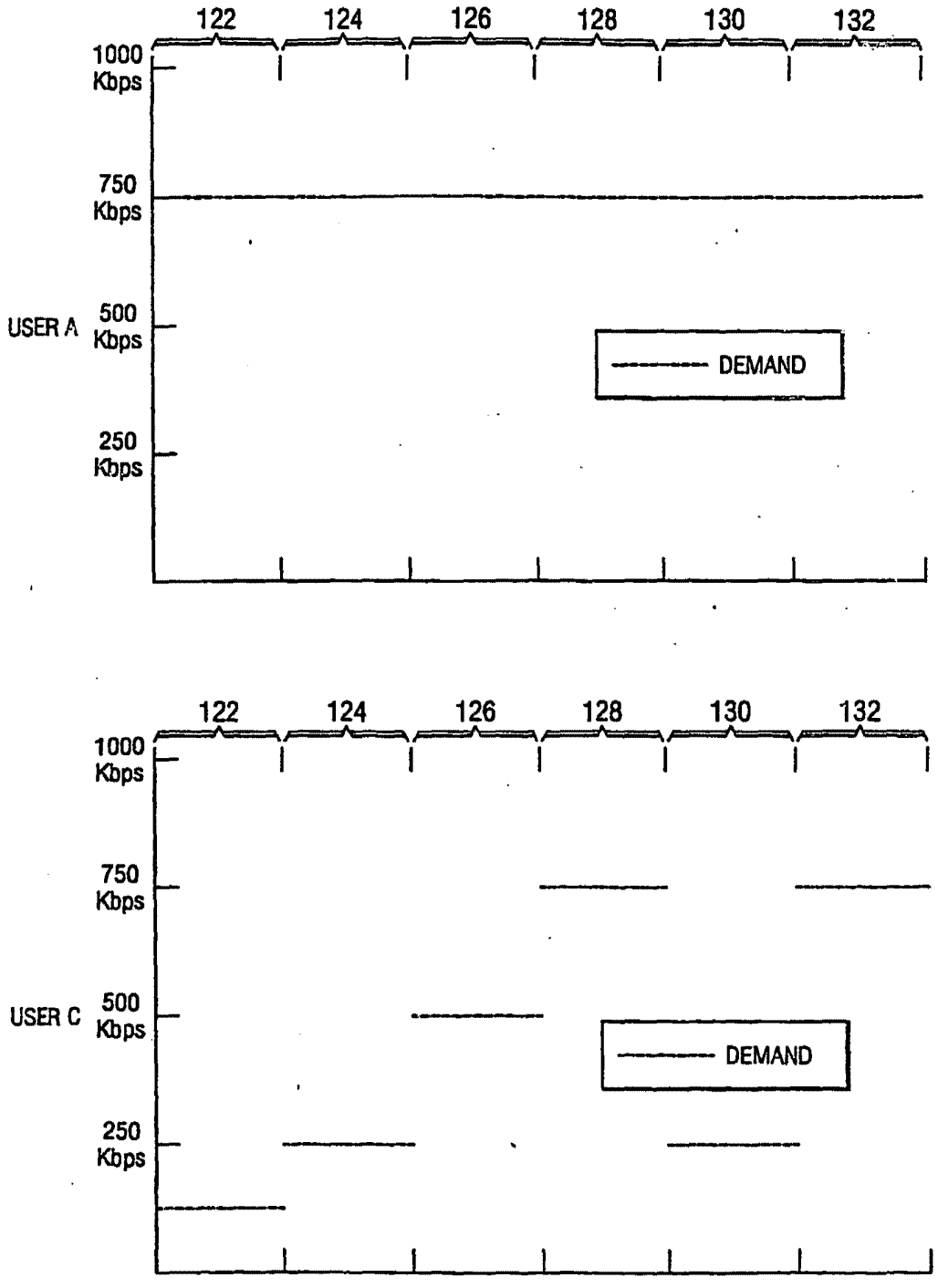

122
124
126
128
130
132
1000 Kbps
750 Kbps
USER A
500 Kbps
250 Kbps
DEMAND
122
124
126
128
130
132
1000 Kbps
750 Kbps
USER C
500 Kbps
250 Kbps
DEMAND

FIG. 6A

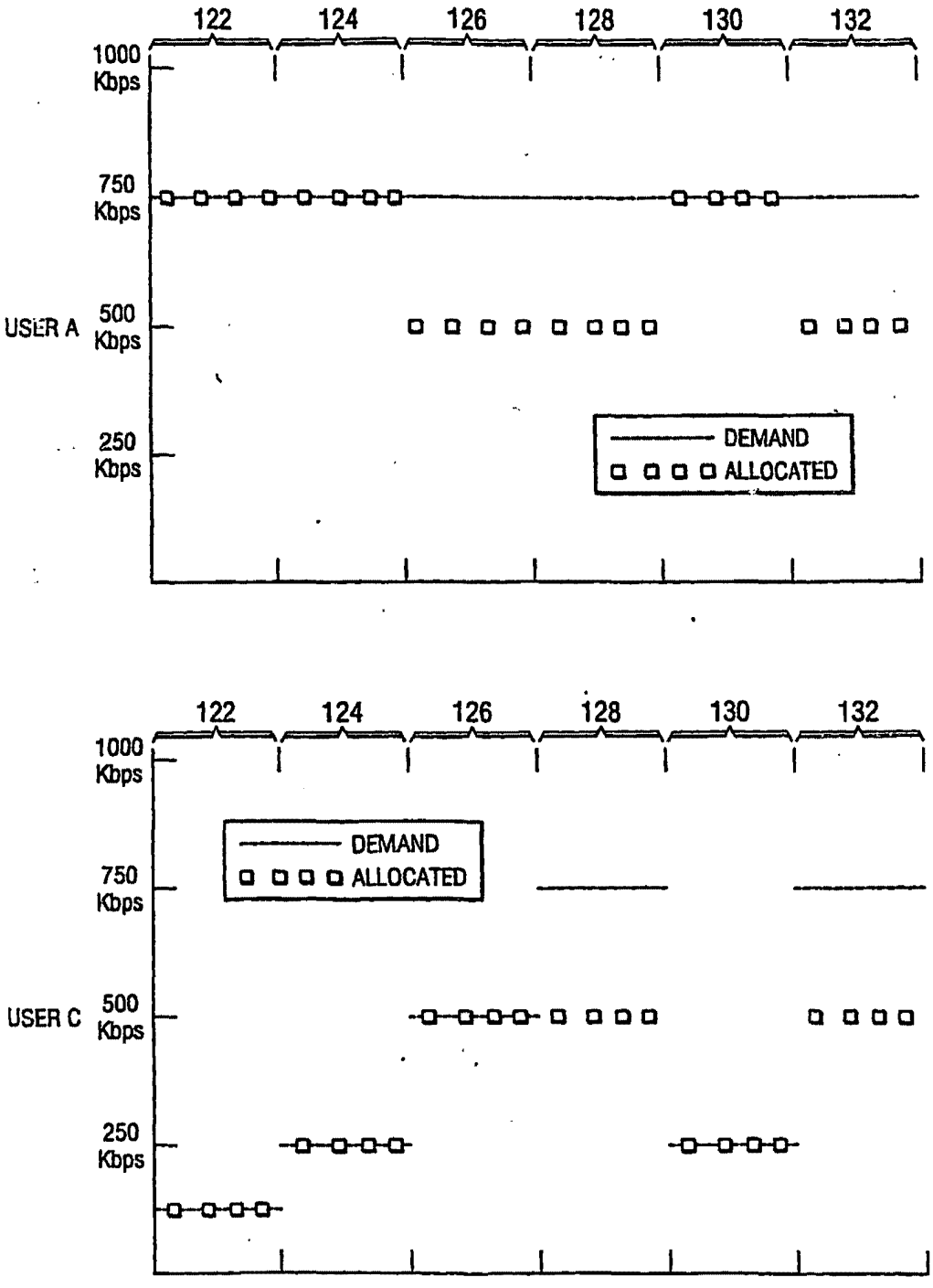

122
124
126
128
130
132
1000 Kbps
750 Kbps
USER A
500 Kbps
250 Kbps
DEMAND
ALLOCATED
122
124
126
128
130
132
1000 Kbps
DEMAND
ALLOCATED
750 Kbps
USER C
500 Kbps
250 Kbps

FIG. 6B

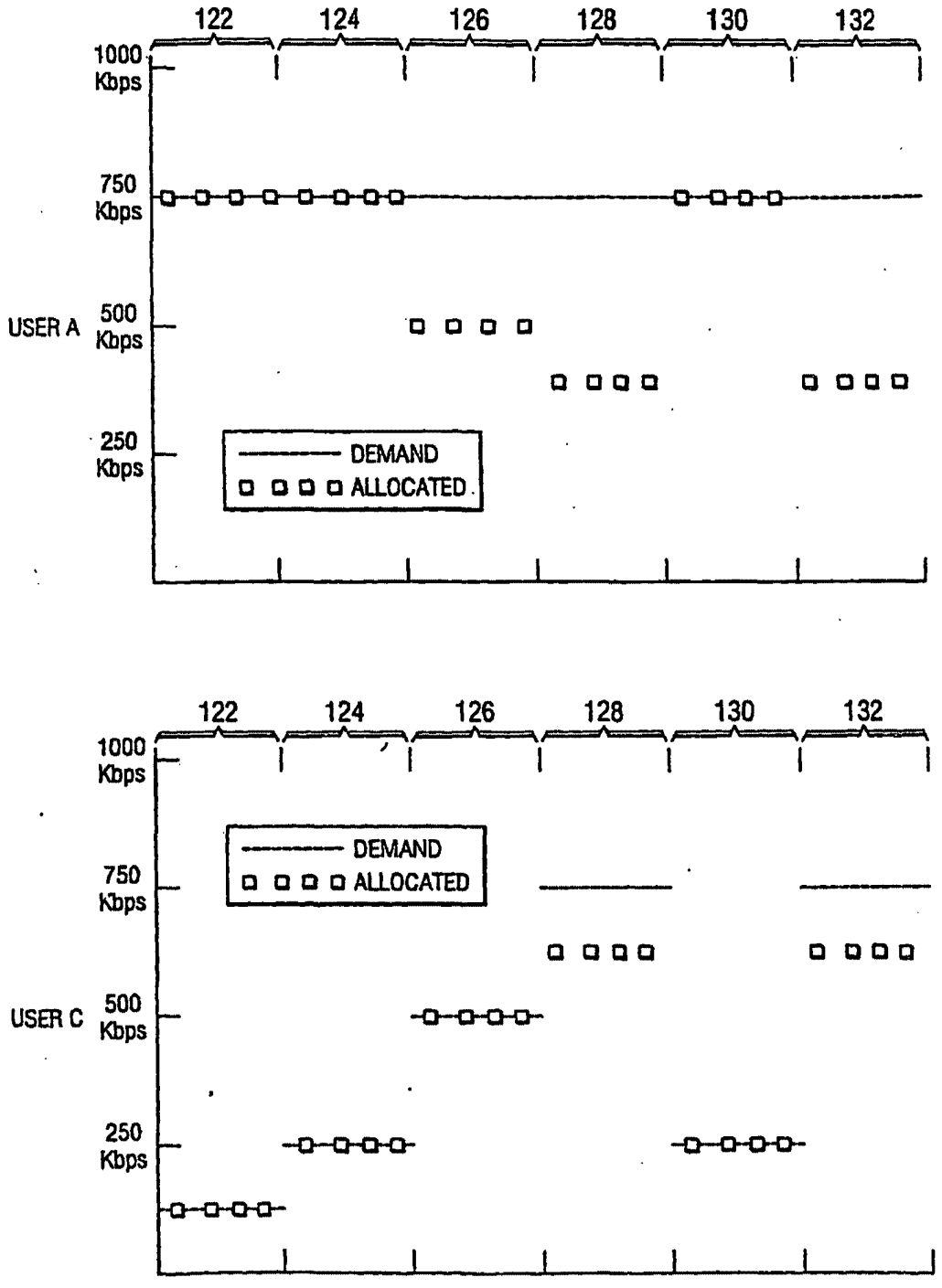

122
124
126
128
130
132
1000 Kbps
750 Kbps
USER A
500 Kbps
250 Kbps
DEMAND
ALLOCATED
122
124
126
128
130
132
1000 Kbps
DEMAND
ALLOCATED
750 Kbps
USER C
500 Kbps
250 Kbps

FIG. 6C

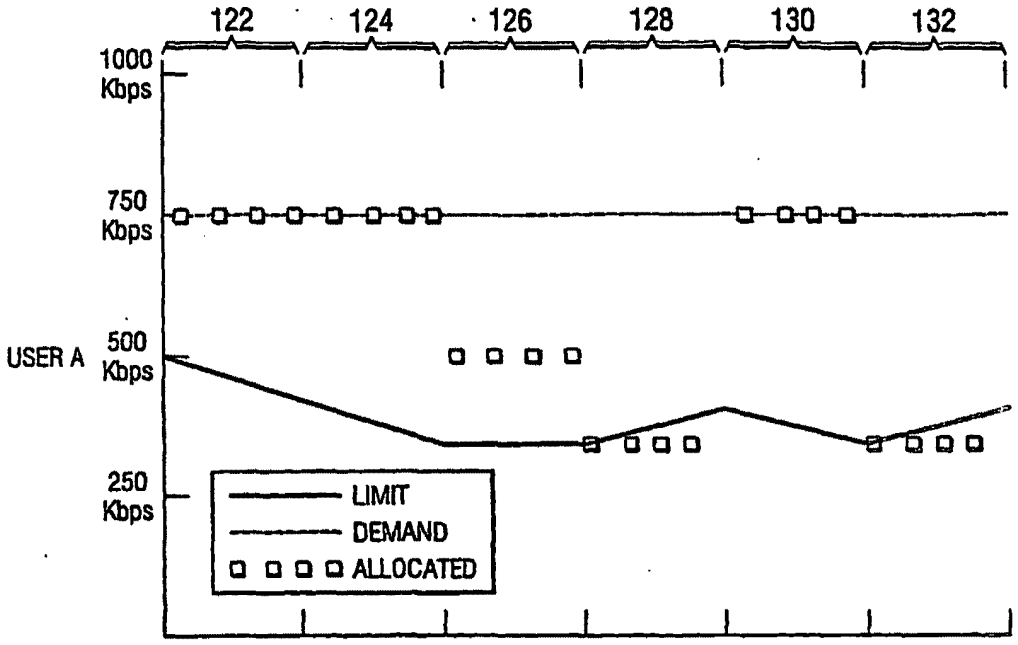

122
124
126
128
130
132
1000 Kbps
750 Kbps
USER A
500 Kbps
250 Kbps
LIMIT
DEMAND
ALLOCATED

FIG. 6D

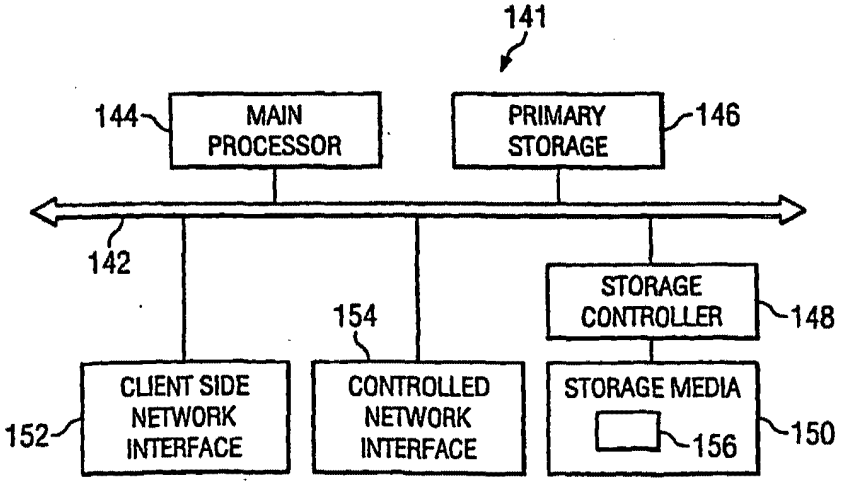

141
144
MAIN PROCESSOR
PRIMARY STORAGE
146
142
154
STORAGE CONTROLLER
148
CLIENT SIDE NETWORK INTERFACE
CONTROLLED NETWORK INTERFACE
STORAGE MEDIA
156
152
150

FIG. 7

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 March 2005 (03.03.2005)

PCT

(10) International Publication Number
WO 2005/020035 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/029249

(22) International Filing Date: 20 August 2004 (20.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/496,629 20 August 2003 (20.08.2003) US

(71) Applicant *(for all designated States except US)*: ROCK-STEADY NETWORKS, INC. [US/US]; 3410 Far West Blvd., Suite 210, Austin, TX 78731 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WHITE, Eric [US/US]; 1717 Bartoncliff Drive, Austin, TX 78704 (US). TURLEY, Patrick [US/US]; 1820 Treadwell Lane, Austin, TX 78704 (US).

(74) Agent: AKMAL, Ariyeh; Sprinkle IP Law Group, P.O. Box 684767, Austin, TX 78768-4767 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING A SECURE CONNECTION BETWEEN NETWORKED COMPUTERS

(57) Abstract: Systems and methods for providing a secure connection between networked computers are disclosed. A computer may make a request for a secure connection to another networked computer. In response, configuration data may be sent to the requesting computer which configures a protocol on the requesting computer and establishes a secure connection with the other networked computer. This configuration data may advantageously utilize protocole inherent to particular operating systems to setup and establish this secure connection in an automated fashion, and may include a controller designed to both automatically configure such a protocol and automatically establish a secure connection using the protocol.

WO 2005/020035 A2

DESCRIPTION

SYSTEM AND METHOD FOR PROVIDING A SECURE CONNECTION BETWEEN NETWORKED COMPUTERS

TECHNICAL FIELD OF THE INVENTION

The invention relates in general to methods and systems for computer connectivity, and more particularly, to methods and systems for establishing and providing secure connections between computers.

BACKGROUND OF THE INVENTION

The use of computer networks to store data and provide information to users is increasingly common. In fact, in many cases it may be necessary for a computer to be connected to a specific network to retrieve data desired or needed by a user. To connect to a specific network, a user at a client computer may utilize a network connection, such as the Internet, to connect to a computer belonging to the network.

The Internet is a loosely organized network of computers spanning the globe. Client computers, such as home computers, can connect to other clients and servers on the Internet through a local or regional Internet Service Provider ("ISP") that further connects to larger regional ISPs or directly to one of the Internet's "backbones." Regional and national backbones are interconnected through long range data transport connections such as satellite relays and undersea cables. Through these layers of interconnectivity, each computer connected to the Internet can connect to every other (or at least a large percentage) of other computers on the Internet. Utilizing the Internet, a user may connect to any of the networks within the Internet.

The arrangement of the Internet, however, presents a whole host of security concerns. These concerns revolve mainly around the fact that communications between a client computer and a server computer residing in a remote network may travel through a wide variety of other computers and networks before arriving at their eventual destinations. If these communications are not secured, they are readily accessible to anyone with a basic understanding of network communication protocols.

To alleviate these security concerns, a virtual private network or VPN may be established between a client computer and another network. A VPN may allow private and secure communications between computers over a public network, while maintaining privacy through

the use of a tunneling protocol and security procedures. These tunneling protocols allow traffic to be encrypted at the edge of one network or at an originating computer, moved over a public network like any other data, and then decrypted when it reaches a remote network or receiving computer. This encrypted traffic acts like it is in a tunnel between the two networks or computers: even if an attacker can see the traffic, they cannot read it, and they cannot change the traffic without the changes being seen by the receiving party and therefore being rejected.

VPNs are similar to wide area networks (WAN), but the key feature of VPNs is that they are able to use public networks like the Internet rather than rely on expensive, private leased lines. At they same time, VPNs have the same security and encryption features as a private network, while adding the advantage of the economies of scale and remote accessibility of large public networks.

VPNs today are set up a variety of ways, and can be built over ATM, frame relay, and X.25 technologies. However, the most popular current method is to deploy IP-based VPNs, which offer more flexibility and ease of connectivity. Since most corporate intranets use IP or Web technologies, IP-VPNs can more transparently extend these capabilities over a wide network. An IP-VPN link can be set up anywhere in the world between two endpoints, and the IP network automatically handles the traffic routing.

A VPN, however, is not without its flaws. First of all, to establish a VPN, both computers must utilize identical VPN protocols. As there are a wide variety of VPN protocols in use, such as PPTP, IPsec, L2TP etc. this is by no means guaranteed. If identical protocols are not originally on one or more of the computers, identical protocols must be installed on both of these systems before a VPN may be established.

Additionally, even if the computers are running the same protocol, this protocol may still have to be manually setup and configured. In many cases, every time a remote user wishes to establish a VPN with a computer over an existing network he must bring up the VPN protocol he wishes to use and properly configure it to work with the remote computer or network he wishes to access.

These installation and configuration issues may present problems to someone who is not well versed in the area of network protocols, and may even present problems for those who are familiar with these protocols, as typically a remote user must configure his computer without access to the gateway to which he wishes to connect.

Even more problematic, however, is that setting up a VPN still presents security issues. Almost universally, a gateway at a remote network is not going to establish a VPN with a random remote computer. In most cases, the remote gateway requires a username and a password before it will establish a VPN connection. This username and password is sent from the remote user in an unsecured form, or encrypted using a weak encryption algorithm. As this username and password are easily snooped by malicious users of a public network, a security hole exists within the very process of trying to create a VPN to provide greater security.

Thus, a need exists for more secure methods and systems for establishing a secure connection between computers which require minimum amounts of manual configuration.

SUMMARY OF THE INVENTION

Systems and methods for establishing or providing a secure connection between networked computers are disclosed. A computer may make a request for a secure connection to another computer. In response, configuration data may be sent to the requesting computer. This configuration data may execute on the requesting computer in order to create a secure connection between the two computers. Using this secure connection, data may be passed between the two computers with a greater degree of privacy.

Furthermore, protocols inherent to particular operating systems may be utilized to setup and establish a secure connection between networked computers in an automated fashion, requiring no manual intervention or configuration by the user of a computer. The configuration data sent to the requesting computer may automatically configure a protocol on the requesting computer and automatically establish a secure connection with another networked computer.

In one embodiment, a connection is requested in a first protocol, data is sent in response to the request, a second protocol is configured using the data and a secure connection is established using the second protocol.

In another embodiment, the first protocol is HTTPS.

In yet another embodiment, the data is sent using the first protocol.

In other embodiments, the request for the connection includes a username and a password.

In still other embodiments, data is sent only if the username and password are verified.

In yet other embodiments, the data includes a controller.

In some embodiments, the controller is an Active X controller.

In a particular embodiment, the data includes a credential and the secured connection is established using the credential.

In one embodiment, the credential is dynamically generated in response to the request and includes a password and a username.

In additional embodiments, the credential is valid only for the duration of the secure connection.

In other embodiments, the second protocol is PPTP and is configured automatically using the controller.

In one embodiment, the secure connection is established automatically using the controller.

These, and other, aspects of the invention will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. The following description, while indicating various embodiments of the invention and numerous specific details thereof, is given by way of illustration and not of limitation. Many substitutions, modifications, additions or rearrangements may be made within the scope of the invention, and the invention includes all such substitutions, modifications, additions or rearrangements.

BRIEF DESCRIPTION OF THE DRAWINGS

The drawings accompanying and forming part of this specification are included to depict certain aspects of the invention. A clearer impression of the invention, and of the components and operation of systems provided with the invention, will become more readily apparent by referring to the exemplary, and therefore nonlimiting, embodiments illustrated in the drawings, wherein identical reference numerals designate the same components. Note that the features illustrated in the drawings are not necessarily drawn to scale.

FIGURE 1 includes an illustration of exemplary architecture for use in describing various

embodiments of the systems and methods of the present invention.

FIGURE 2 includes a flow diagram of one embodiment of a method for establishing a secure connection between two computers.

FIGURE 3 includes a representation of applying an embodiment of a method for establishing a secure connection to portions of the architecture depicted in FIGURE 1.

FIGURE 4 includes a representation of one embodiment of VPN client software.

FIGURE 5 includes an illustration of another exemplary architecture where embodiments of the systems and methods of the present invention may find applicability.

DESCRIPTION OF PREFERRED EMBODIMENTS

The invention and the various features and advantageous details thereof are explained more fully with reference to the nonlimiting embodiments that are illustrated in the accompanying drawings and detailed in the following description. Descriptions of well known starting materials, processing techniques, components and equipment are omitted so as not to unnecessarily obscure the invention in detail. It should be understood, however, that the detailed description and the specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only and not by way of limitation. After reading the specification, various substitutions, modifications, additions and rearrangements will become apparent to those skilled in the art from this disclosure which do not depart from the scope of the appended claims.

Initially, a few terms are defined to aid the reader in an understanding of the following disclosure. The term "controller" is intended to mean any set of data or instructions operable to perform certain tasks or a combination of hardware (such as a processor) and software instructions capable of performing a certain task.

The term "networked" is intended to mean operable to communicate. For example, two networked computers are operable to communicate with one another using techniques known in the art, such as via a wireless or wired connection using TCP/IP. Two computers may be networked through a variety of networks, sub-networks etc.

Before discussing embodiments of the present invention, an exemplary architecture for use in illustrating embodiments of the present invention is described. It will be apparent to those of

ordinary skill in the art that this is a simple architecture intended for illustrative embodiments only, and that the systems and methods described herein may be employed with any variety of more complicated architectures. Each of the computers depicted may include desktops, laptops, PDAs or any other type of device capable of communicating, either via wireless or wired connection, over a network. Each network depicted, whether they be intranets or any other type of network, may include sub-networks or any combination of networks and sub-networks

FIGURE 1 illustrates just such an exemplary architecture. In FIGURE 1, intranet 100 is a private network composed of client computers 110 and server 120. Client computers 110 may be coupled to server 120, which is in turn coupled to public network 130, such as the Internet. Client computers 110 may not be coupled directly to public network 130. Therefore, to access public network 130, client computers 110 may communicate with server 120, which in turn serves as a gateway to public network 130 as is commonly known in the art. Data residing within intranet 130 may be sensitive. Consequently, server 120 may also serve as a firewall for intranet 110, preventing unauthorized users of public network 130 from accessing intranet 110. Remote client computer 140 may also be coupled to public network 130 via a wired or wireless connection, as is known in the art. Therefore, remote client computer 140 and server 120 may be capable of communication via public network 130.

Attention is now directed to systems and methods for establishing a secure connection between two computers over a network according to one embodiment of the invention. Typically, a user at a remote client computer wishes to establish a connection with an intranet or a computer within an intranet. To accomplish this, the remote client computer and a server computer belonging to the intranet may create a VPN so information may be securely transferred between the remote client computer and the server computer or other computers within the intranet. To securely establish this VPN with a minimum of configuration, the remote client computer may make a request for a VPN connection to the server. In response, the server may send configuration data to the remote client computer. This configuration data may execute on the remote client computer in order to create a secure VPN connection between the remote client and the server. Using this secure connection, data may be passed between server and remote client with a greater degree of privacy.

These systems and methods may be explained in more detail with reference to the exemplary hardware architecture of FIGURE 1. Suppose a user at remote client computer 140 wishes to securely interact with intranet 100. To accomplish this, remote client computer 140 can request a secure connection from server 120 over network 130. In response, server 120 may send

configuration data to remote client computer 140. Using this configuration data, a secure connection may be established between remote client computer 140 and server computer 120, after which remote computer 140 may interact with computers 110, 120 of intranet 100 as if remote computer 140 belonged to intranet 100.

In one particular embodiment, to obtain connectivity between remote client computer 140 and server 120 a transient VPN may be established between server 120 and remote client computer 140 using public network 130. This transient VPN may provide a dynamic, secure connection between remote client computer 140 and server 120 by creating a transient VPN endpoint on remote client computer 140 that connects through a VPN tunnel to server 120. This VPN connection may be established using a wide variety of VPN protocols, as are known in the art, such as PPTP, IPsec, L2TP etc.

Furthermore, protocols inherent to particular operating systems may be utilized to setup and establish a transient VPN endpoint on remote client computer 140 in an automated fashion, requiring no manual intervention or configuration by the user of remote client computer 140. For example, suppose remote computer 140 and server are both executing a Windows based operating of the type developed by Microsoft, such as Windows98, WindowsXP, Windows2000 etc. As Windows based operating system have the PPTP VPN protocol built into them, this protocol may be used advantageously to automatically establish a VPN between remote client computer 140 and server 120 if both are executing a Windows based operating system.

Turning now to FIGURE 2, a flow diagram for one method of establishing a secure connection between networked computers is depicted. To establish a secure connection between two networked computer, the first step may be to ensure that the protocol to be utilized in establishing this secure connection is installed on both computers, and if it is not, to install the desired protocol on the computer(s) that do not have it (Step 210). For example, if a VPN connection is desired between remote client computer 140 and server computer 120 a wide variety of VPN protocols may be used to establish this connection, such as IPsec, L2TP, PPTP, MPLS etc. If, however, it is desired to use IPsec and remote client computer 140 does not have the IPsec protocol installed or configured, it may be necessary to install the IPsec protocol (Step 210) on remote client computer 140 before this particular protocol may be utilized in establishing a VPN connection. This installation may only need to occur once, and may, for example, be accomplished by an IT manager responsible for intranet 110 or remote client computer 140.

At any time after the desired protocol is installed on the computers (Step 210), a secure

connection may be requested by one of the computers (Step 220). For example, remote client computer 140 may request a secure connection from server computer 120. This request (Step 220) may be in any format used to communicate over the network connection between the two computers, such as FTP, HTTP or HTTPS. In response to this request (Step 220), a response may be sent to the requesting computer (Step 230). This response (Step 230) may be sent to the requesting computer using the same format used in the initial request (Step 220), such as FTP, HTTP or HTTPS, and include a set of data designed to establish a secure connection between the two computers using a particular protocol. This set of data may comprise a controller configured to execute on the requesting computer and a set of credentials to be used in conjunction with the controller.

The set of data sent in this response (Step 230) may provide information to be utilized by a protocol on the requesting computer when connecting to a particular networked computer using the protocol (Step 240). This information may include the IP address or host name of a server, the authentication domain name, whether MPPC is to be utilized, which call-control and management protocol is to be used, a DNS configuration etc. Providing this information to the protocol may be referred to as "configuring a protocol" and that phrase will be used as such herein. In some instances, a controller contained in the response to the requesting computer executes on the initiating computer and configures the protocol to establish a secure connection using the credentials contained in the response (Step 230).

After this configuration process (Step 240), a secure connection may be initiated using the configured protocol (Step 250), and a secure connection established (Step 260). In some instances, a request for a secure connection may be initiated by the same controller responsible for configuring the protocol, and include the credentials contained in the sent response (Step 230). After verifying the credentials a secure connection may be established (Step 260).

It will be clear to those of ordinary skill in the art that the method depicted in the flow diagram of FIGURE 2 may be tailored to implement a secure connection between two computers in a variety of architectures, and may employ a variety of different protocols for the various communications and secure connections.

Note that FIGURE 2 represents one embodiment of the invention and that not all of the steps depicted in FIGURE 2 are necessary, that a step may not be required, and that further steps may be utilized in addition to the ones depicted, including steps for communication, authentication, configuration etc. Additionally, the order in which each step is described is not necessarily the

order in which it is utilized. After reading this specification, a person of ordinary skill in the art will be capable of determining which arrangement of steps will be best suited to a particular implementation.

In fact, embodiments of the methods and systems of the present invention may be particularly useful in establishing a secure connection between two computers by automatically configuring a protocol built into an operating systems executing on both of the computers, alleviating the need for a user to install or configure such a protocol manually.

FIGURE 3 depicts one embodiment of a method for automatically establishing a transient VPN connection between a remote client computer and a server both executing a Windows based operating system containing the point-to-point tunneling protocol (PPTP) for establishing VPNs. Remote client computer 140 may send a connection request (Step 220) to server computer 120 indicating that remote client computer 140 wishes to establish a VPN connection with server 120. This request may be initiated by a user at remote computer 140. Though this request may be initiated in a variety of ways, in many instances a user at remote client computer 140 may initiate this request using an HTTP client. For example, via an internet browser of the type commonly know in the art, such as Netscape or Internet Explorer.

Using this browser, a client at remote client computer 140 may navigate to a particular URL in a known manner, perhaps by typing it directly into an address window within the browser, accessing the URL in his bookmarks file, or navigating to the URL by clicking on an HTTP link within a page. By pointing his browser to a particular URL, the user at remote client computer 140 initiates a connection request to server 120 computer. This URL may also contain an HTML form requesting a username and password from a user at remote computer 140, in order to authenticate a user at remote computer 140.

In some embodiments, this connection request (Step 220) is sent from HTTP client on remote client computer 140 to server 120 using HTTP. However, to better secure the connection request, in other embodiments the connection request from remote client computer 140 to server computer is made using HTTPS, which may be sent via an SSL connection between remote client computer 140 and server computer 120.

In response to the connection request (Step 220) from remote client computer 140, server computer 120 may send data to remote client computer 140 which will facilitate the establishment of a VPN connection between server and remote client computer (Step 230). If the

connection request (Step 220) from remote client computer 140 contained a username or password, server computer 120 may first authenticate or authorize the requesting user at remote client computer 140. Logic on server computer 120 may verify the username or password submitted in the connection request (Step 220) possibly by authenticating them against a form of user database (RADIUS, LDAP, etc.). If the user's authentication profile permits, server 120 may then send a response to remote client computer 140 with the configuration data (Step 230). This data may include VPN client software designed to utilize a VPN protocol on remote client computer 140 to automatically establish a secure VPN connection between server computer 120 and remote client computer 140 without any action by the user of remote client computer 140.

In one specific embodiment, the VPN client software is sent to remote client computer 140 using HTTPS, and includes a controller designed to establish a secure VPN connection between server 120 and remote client computer 140, and a set of credentials. These credentials may be session specific, and dynamically generated by server computer 120 using a random-seed. Additionally, this VPN client software may be digitally signed with an X.509 digital certificate, of the type know in the art, so that remote client computer 140 recognizes that the origin of the VPN client software is server computer 120. Once the origin of VPN client software is verified, it may then be installed or executed on remote client computer 140 to establish a secure VPN connection.

FIGURE 4 depicts a block diagram of one embodiment of the client software which may be sent from server computer 120 to remote client computer 140 (Step 230). VPN client software 400 may include controller 410 designed to configure a protocol on remote client computer 140 and establish the VPN connection between server 120 and remote client computer 140. In many cases, this controller 410 is designed to utilize a VPN protocol resident on remote client computer 140 to establish this connection. This controller may be written in a variety of programming or scripting languages as are known in the art, such as C, C++, Java, etc.

Once VPN client software 400 is downloaded and controller 410 executed, controller 410 may establish a secure VPN connection between remote client computer 140 and server 120. To continue with the above example, remote client computer 140 may be executing a Windows based operating system, and controller 410 may be an Active X controller designed specifically to configure the PPTP bundled in the Windows operating system software. Therefore, once VPN client software 400 is downloaded to remote client computer 140, Active X controller 410 may execute automatically on remote client computer 140, making system library calls to configure the PPTP resident on remote client computer 140 as a PPTP client.

Using the configured PPTP client, Active X controller 410 may then automatically establish a secure VPN connection with server computer 120. This secure connection may be automatically established by controller 410 by making additionally system library calls on remote client computer 140 to initiate a tunnel request (Step 240) from remote client computer 140 to server computer 120. As noted above, PPTP libraries are installed with most Windows based operating systems. Thus, Active X controller executing on remote client computer 140 may configure the PPTP to establish a secure VPN connection with remote server and initiate a tunnel request, without any interference or input by a user of remote client computer 140.

Additionally, in some embodiments, controller 410 may utilize credentials 420 in establishing the secure VPN connection between server computer 120 and remote client computer 140. As mentioned above, credentials 420 may have been dynamically generated by server computer 120 and sent in the response (Step 230) to initial connection request (Step 220). Credentials 420 may contain a password and username. Controller 410 may use this username and password as parameters when establishing the VPN connection between remote client computer and server computer. Credentials may be sent with tunnel request (Step 250) and verified by server computer 120 before establishing a VPN connection with remote computer 140. Since server computer 120 initially created credentials 420, server may identify the credentials from remote client computer 140 and associate a particular VPN connection with a particular remote client computer.

Credentials 420, including the username and password may then be used for the duration of that particular session between remote client computer 140 and server computer 140. Once the VPN connection between remote client computer and server computer is severed, username and password may lose their validity, preventing their unauthorized use in the future.

Embodiments of the systems and methods disclosed will be useful in a variety of architectures, as will be apparent to those of skill in the art after reading this disclosure. FIGURE 5 depicts an example of another architecture where these systems and methods might find useful application. Wireless router 510 and server 512 may serve as wireless access point 514 to Internet 520, as is known in the art. Remote server computers 140 may be wirelessly coupled to server 512 and Internet 520 thorough router 510. In this architecture, embodiments of these systems and methods may be utilized to secure wireless communications between remote client computer 140 and access point 514.

For example, after remote client computer 140 enters the range of wireless router 510, remote

client computer 140 may associate with access point 514. Remote client computer 140 may then request a secure connection with server 512 via a browser based interface. Client software 400, including controller 410 and credentials 420 may be downloaded to remote client computer 140 using HTTPS, at which point the controller automatically configures the PPTP on remote client computer 140 and establish a VPN tunnel between remote client computer 140 and wireless access point 514. From this point, wireless communications between remote client computer and access point 514 may be made using this VPN tunnel, and are therefore, more secure.

In the foregoing specification, the invention has been described with reference to specific embodiments. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of invention.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any component(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature or component of any or all the claims.

CLAIMS

1. A method for establishing a secure connection between two computers, comprising:
requesting a connection, wherein the request is in a first protocol;
sending data in response to the request;
configuring a second protocol using the data;
establishing the secure connection using the second protocol.

2. The method of claim 1, wherein the first protocol is HTTPS.

3. The method of claim 2, wherein the data is sent using the first protocol.

4. The method of claim 3, wherein the request for the connection includes a username and a password.

5. The method of claim 4, wherein the data is sent only if the username and password are verified.

6. The method of claim 1, wherein the data includes a controller.

7. The method of claim 6, wherein the controller is an Active X controller.

8. The method of claim 6, wherein the data includes a credential.

9. The method of claim 8, wherein the secured connection is established using the credential.

10. The method of claim 9, wherein the credential includes a password and a username.

11. The method of claim 8, wherein the credential is dynamically generated in response to the request.

12. The method of claim 11, wherein the credential is valid only for the duration of the secure connection.

13. The method of claim 6, wherein the second protocol is configured automatically using the controller.

14. The method of claim 13, wherein the second protocol is PPTP.

15. The method of claim 13, wherein the secure connection is established automatically using the controller.

16. A system for a secure connection between two computers, comprising:

a first computer operable to request a connection, wherein the request is in a first protocol;

a second computer operable to send data in response to the request, wherein the data contains instructions operable to configure a second protocol on the first computer and establish the secure connection using the second protocol.

17. The system of claim 16, wherein the first protocol is HTTPS.

18. The system of claim 17, wherein the data is sent using the first protocol.

19. The system of claim 18, wherein the request for the connection includes a username and a password.

20. The system of claim 19, wherein second computer is operable to verify the username and password and send the data only if the username and password are verified.

21. The system of claim 16, wherein the data includes a controller.

22. The system of claim 21, wherein the controller is an Active X controller.

23. The system of claim 21, wherein the data includes a credential.

24. The system of claim 23, wherein the secured connection is established using the credential.

25. The system of claim 24, wherein the credential includes a password and a username.

26. The system of claim 23, wherein second computer is operable to dynamically generate the credential in response to the request.

27. The system of claim 26, wherein the credential is valid only for the duration of the secure connection.

28. The system of claim 21, wherein the second protocol is configured automatically by the controller.

29. The system of claim 28, wherein the second protocol is PPTP.

30. The system of claim 28, wherein the secure connection is established automatically using the controller.

31. A computer readable medium, having data embodied thereon, the data translatable for:
configuring a protocol on a first computer; and
establishing a secure connection between the first computer and a second computer using the protocol.

32. The computer readable medium of claim 31, wherein the data is translatable to implement a controller.

33. The computer readable medium of claim 32, wherein the controller is an Active X controller.

34. The computer readable medium of claim 32, wherein the data further include includes a credential.

35. The computer readable medium of claim 34, wherein the secure connection is established using the credential.

36. The computer readable medium of claim 35, wherein the credential includes a password and a username.

37. The computer readable medium of claim 32, wherein the protocol is configured automatically by the controller.

38. The computer readable medium of claim 37, wherein the protocol is PPTP.

39. The computer readable medium of claim 37, wherein the secure connection is established automatically using the controller.

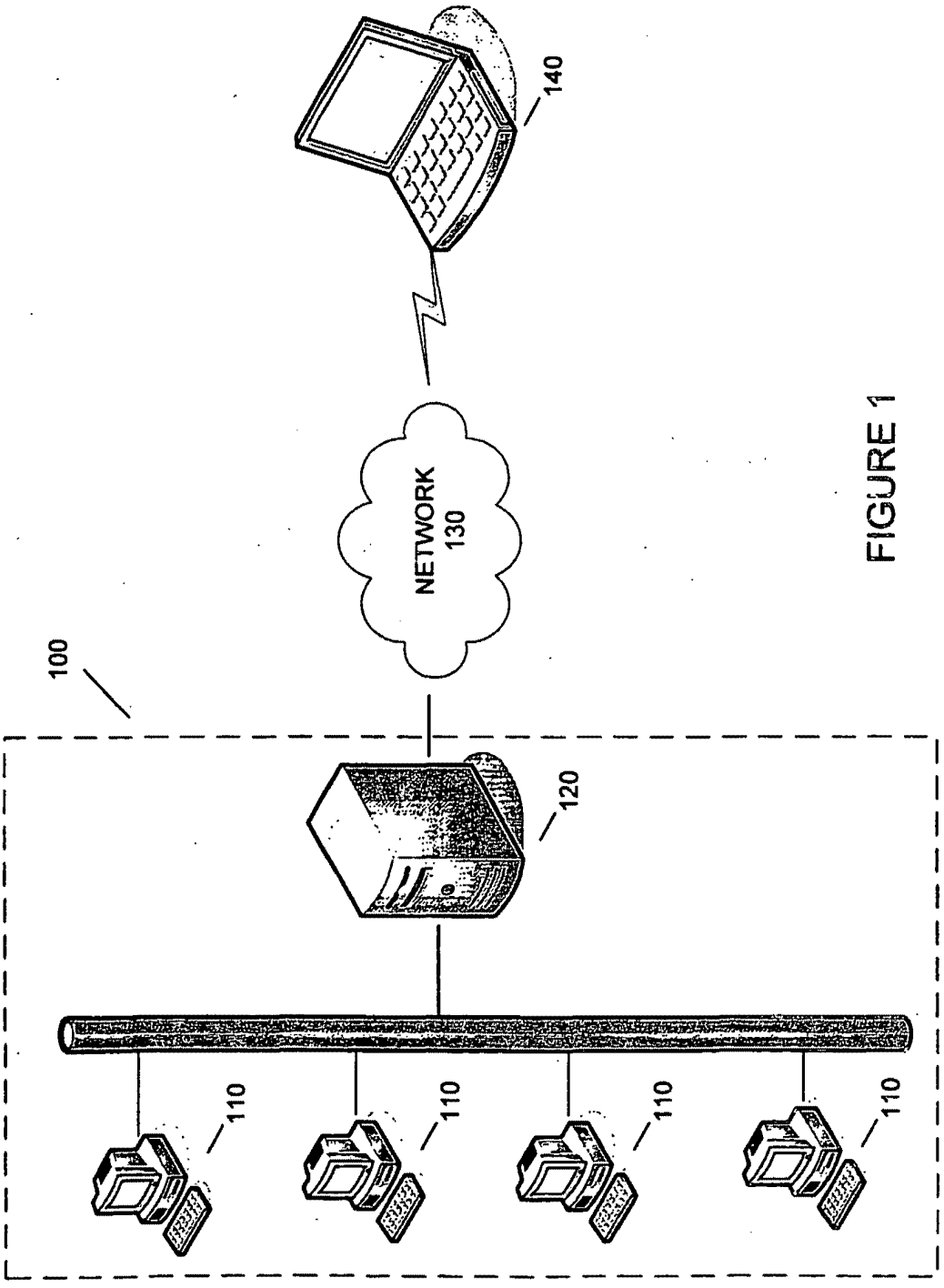


FIGURE 1

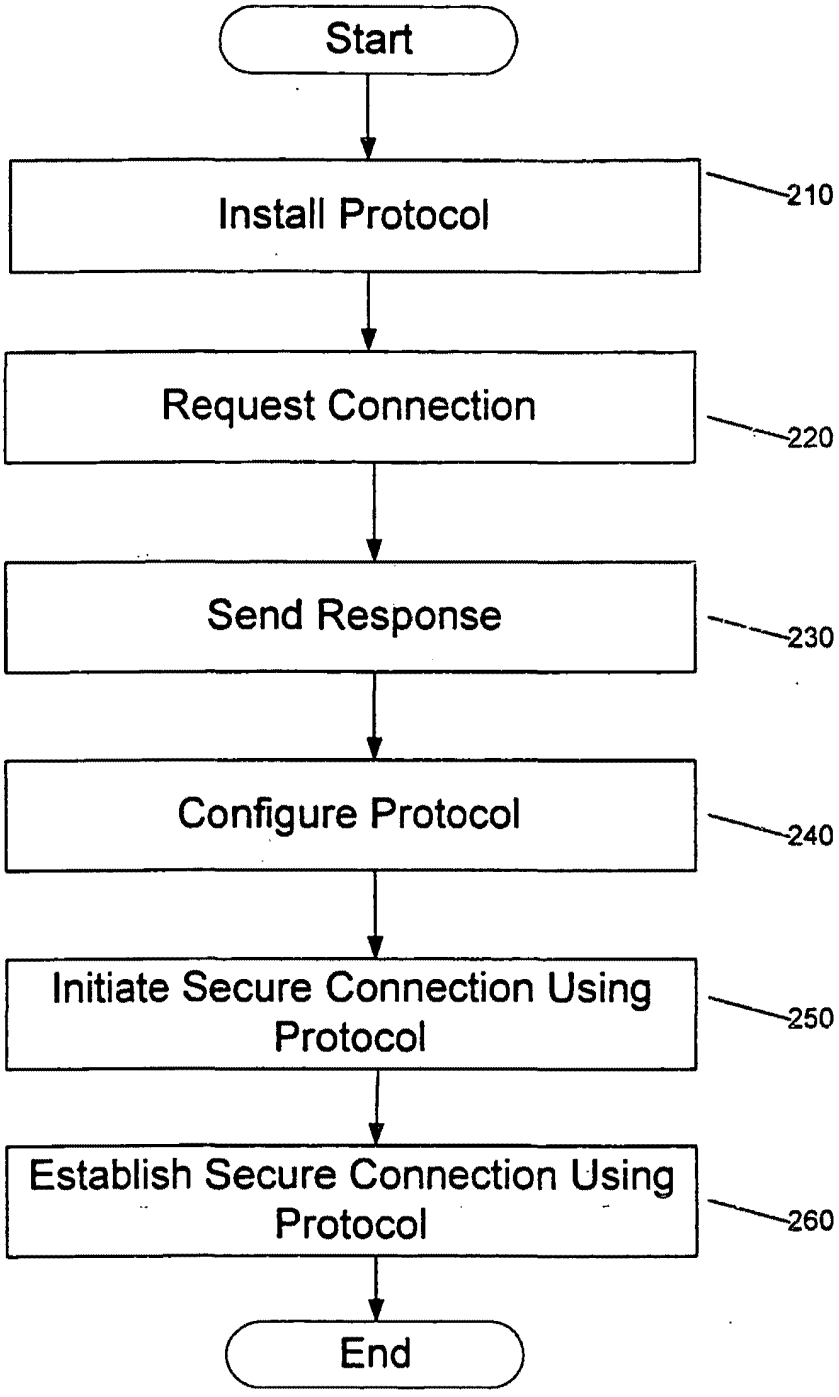

Start
Install Protocol
210
Request Connection
220
Send Response
230
Configure Protocol
240
Initiate Secure Connection Using Protocol
250
Establish Secure Connection Using Protocol
260
End

FIGURE 2

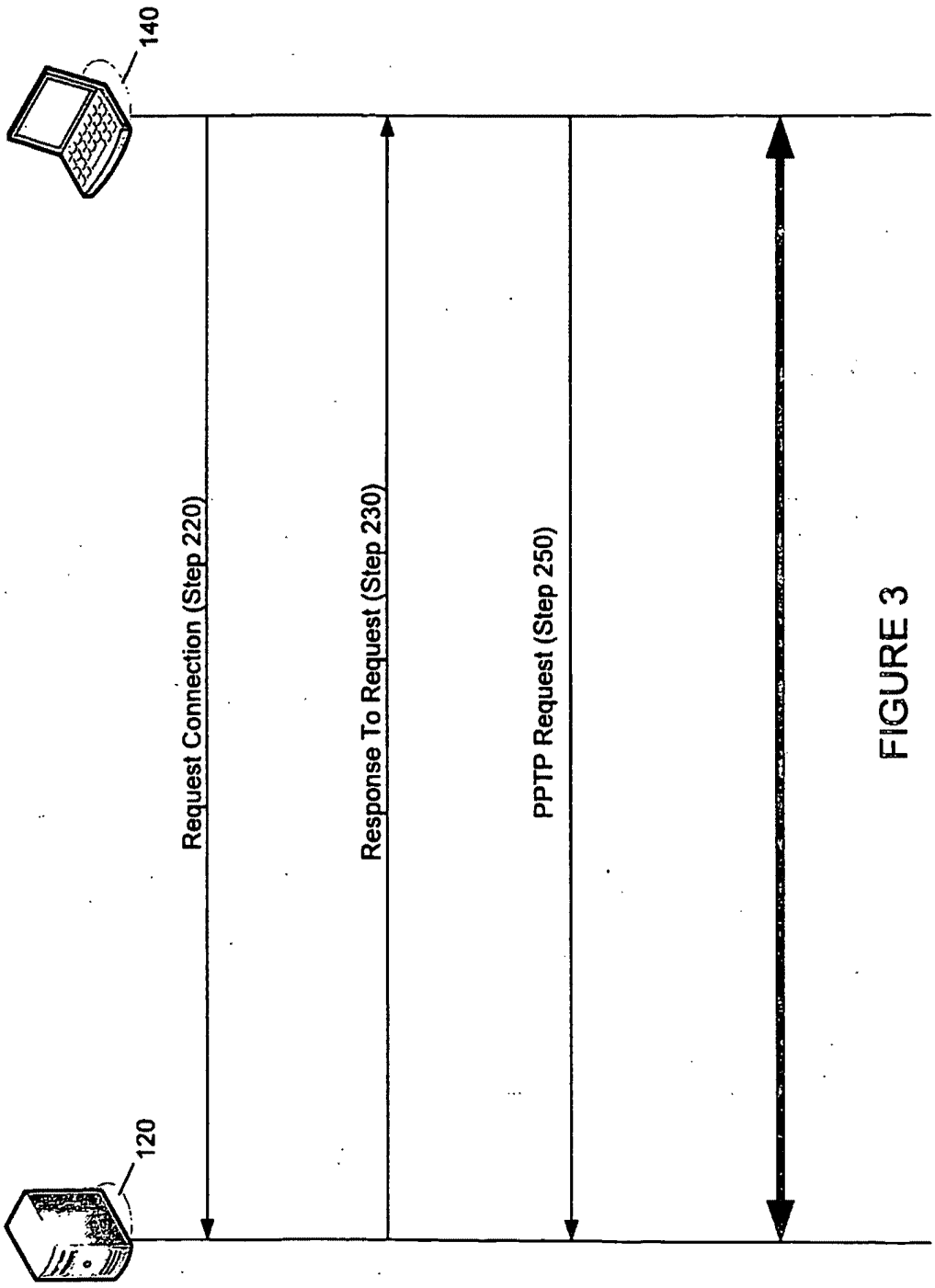

140
120
Request Connection (Step 220)
Response To Request (Step 230)
PPTP Request (Step 250)

FIGURE 3

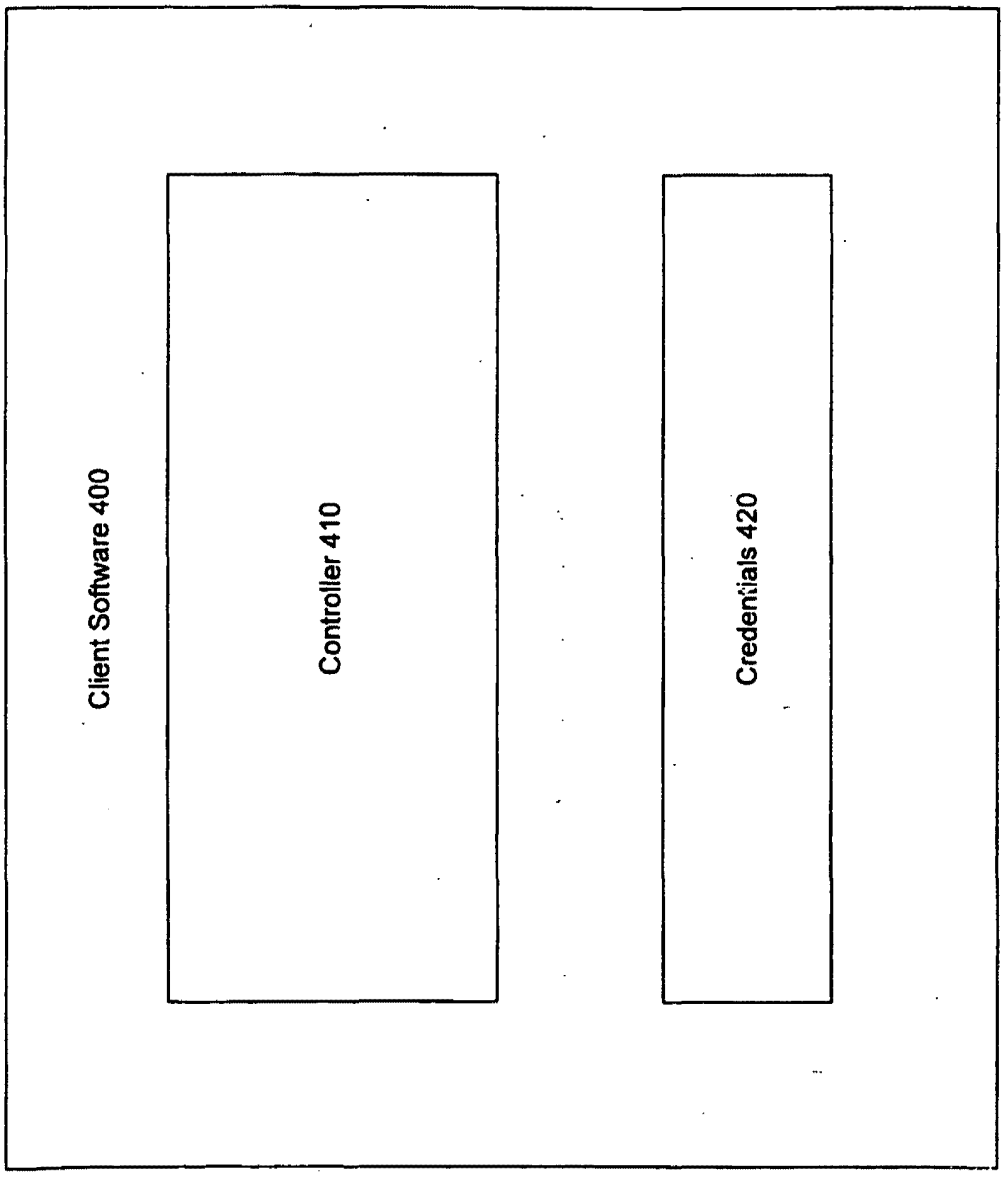


FIGURE 4

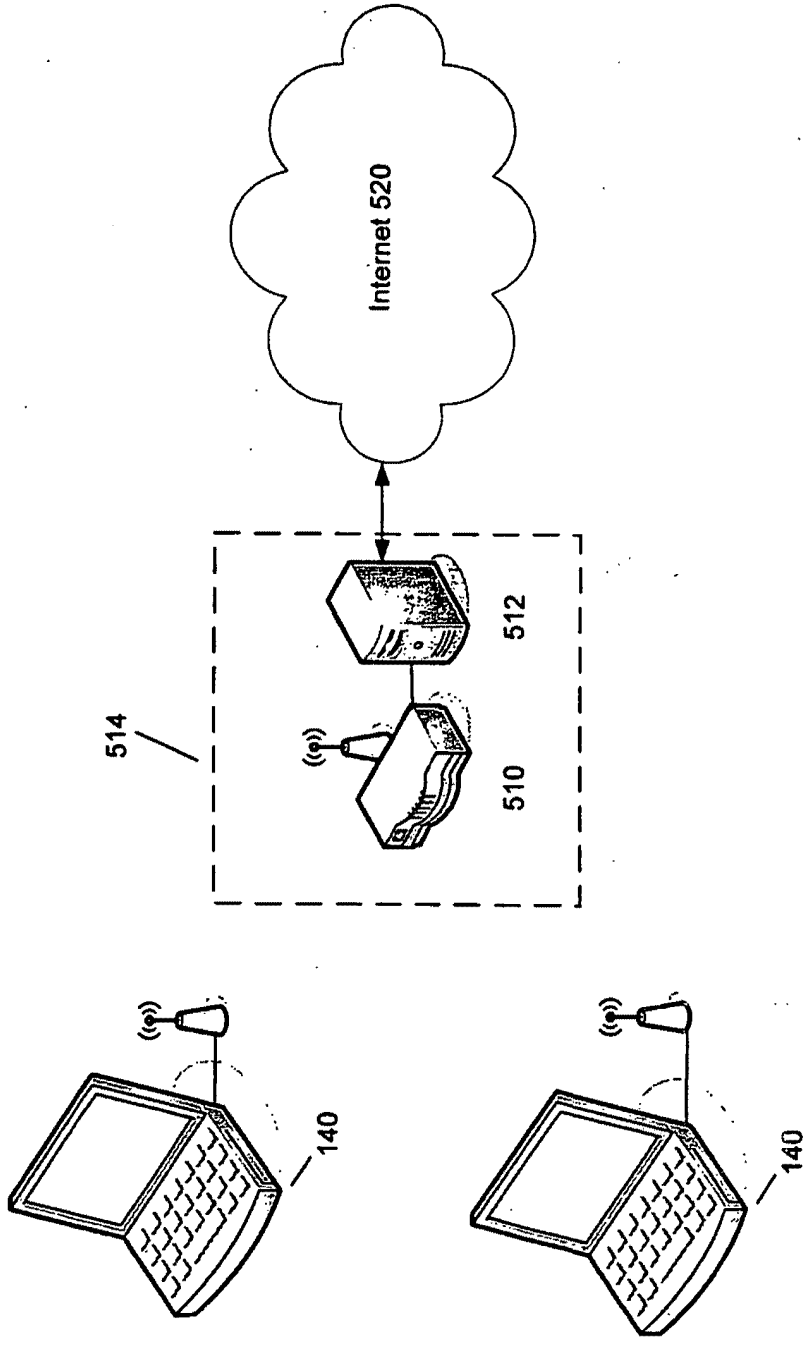


FIGURE 5

C10

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN L. ADAIR
GRAY CARY WARE & FREIDENRICH, LLP
1221 SOUTH MOPAC EXPRESSWAY
SUITE 400
AUSTIN, TX 78746-6875

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing (*day/month/year*) 08 APR 2004
Applicant's or agent's file reference ROCK1120-WO	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US03/32912	International filing date (*day/month/year*) 16 October 2003 (16.10.2003)
Applicant ROCKSTEADY NETWORKS, INC.	

1. ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34, chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 740.14.35

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90 *bis*.1 and 90 *bis*.3, respectively, before the completion of the technical preparations for international publication.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Michelle R. Eason for Rupal Dharia Telephone No. 703 305-9700

Form PCT/ISA/220 (April 2002) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ROCK1120-WO	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US03/32912	International filing date (*day/month/year*) 16 October 2003 (16.10.2003)	(Earliest) Priority Date (*day/month/year*) 16 October 2002 (16.10.2002)
Applicant ROCKSTEADY NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 5
   ☒ as suggested by the applicant. ☐ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.

Form PCT/ISA/210 (first sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/32912

Box III TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

NEW ABSTRACT

One embodiment of the present invention provides a device for allocating bandwidth on a per user basis. The device can be a computing device that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, and a storage medium accessible by the processor that contains a set of computer instructions. The computer instructions can be executable by the processor to retrieve a set of user profiles (98, 100, 102). Based on the user profile for each user (98, 100, 102), the computer instructions can be executable to establish at least one bandwidth limit for each user. For each user (80, 84, 88), the computer instructions can be further executable to regulate bandwidth usage associated with that user based on the at least one bandwidth limit established for that user. The computer instructions can also be executable to update the at least one bandwidth limit.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/32912

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 13/00, 11/30
US CL : 709/225, 226, 232, 229, 231
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/225, 226, 232, 229, 231

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST: USPT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,336,133 B1 (MORRIS et al.) 01 January 2002 (01.01.2002), column 11, line 65 - column 12, line 64, column 6, lines 1 - 4.	1-60
A	US 5,953,506 A (KALRA et al.) 14 September 1999 (14.09.1999), Abstract, Figure 2A.	1-60
A, P	US 6,502,131 B1 (VAID et al.) 31 December 2002 (31.12.2002), Abstract, Figure 2.	1-60

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
22 March 2004 (22.03.2004)

Date of mailing of the international search report
08 APR 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Rupal Dharia for
Michelle K. Eiseman
Telephone No. 703 305-9700

Form PCT/ISA/210 (second sheet) (July 1998)

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

C11

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
JOHN L. ADAIR
GRAY CARY WARE & FREIDENRICH, LLP
1221 SOUTH MOPAC EXPRESSWAY
SUITE 400
AUSTIN, TX 78746

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing (*day/month/year*) 29 OCT 2004
Applicant's or agent's file reference ROCK1100-WO	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US03/32268	International filing date (*day/month/year*) 10 October 2003 (10.10.2003)
Applicant ROCKSTEADY NETWORKS,INC.	

1. ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

Where? Directly to the International Bureau of WIPO, 34, chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders.**

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90 *bis*.1 and 90 *bis*.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise the applicant must, within **20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Michelle R. Eason Ayaz Sheikh Telephone No. (703) 305-9648

Form PCT/ISA/220 (April 2002) *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ROCK1100-WO	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US03/32268	International filing date (*day/month/year*) 10 October 2003 (10.10.2003)	(Earliest) Priority Date (*day/month/year*) 10 October 2002 (10.10.2002)
Applicant ROCKSTEADY NETWORKS,INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the language, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the title,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:
5. With regard to the abstract,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. The figure of the drawings to be published with the abstract is Figure No. 2
   ☐ as suggested by the applicant. ☐ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☒ because this figure better characterizes the invention.

Form PCT/ISA/210 (first sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/32268

Box III TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The technical features mentioned in the abstract do not include a reference sign between parentheses (PCT Rule 8.1(d)).

NEW ABSTRACT

More particularly, one embodiment of the present invention provides a system of providing network access comprising a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored in the storage media, executable by the processor. In one embodiment of the present invention, the computer instructions can be executable to receive a network communication (32) over the first network interface from a user using a user device and determine if the network communication is associated with an authenticated user (34). If the network communication is not associated with an authenticated user, the computer instructions can be executable to direct the user to an authentication interface (38). The computer instructions can be further executable to receive credentials (40) from the user and authenticate the user (42) based on the credentials (40). Another embodiment of the present invention can include a system for providing access to a network that comprises a processor, a first network interface coupled to the processor, a second network interface coupled to the processor, a storage media accessible by the processor and a set of computer instructions stored on the storage media. The computer instructions can be executable by the processor to receive a user profile (44) and provision a user with access to a network based on user profile (44).

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/32268

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/32; G06F 15/16
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182, 200,201;709/227

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/00112186 A1 (FORD et al.) 15 August 2002 (15.08.2002), abstract, Figure 1, elements 10, 11, 13, 12, 19, Fig. 2, elements 30, 39, page 2, paragraphs 0018-019, 024.	1-53
Y	US 2002/0138763 A1 (DELANY et al.) 26 September 2002 (26.09.2002), abstract, Fig. 1, elements 12, 16, 24, 34 and 40, Fig 6, elements 300, 308, 316, Fig. 7, element 360.	1-53
Y	US 6,088,451 A (HE et al.) 11 July 2000 (11.07.2000), the entire document.	1-53
Y	US 5, 878,231 A (BAEHR et al.) 02 March 1999 (02.03.1999),abstarct, Figure 3, elements 160, 170, 150, Figure 7, elements 440,450, col. col. 4, lines 12-26.	1-53
Y	US 2002/0123335 A1 (LUNA et al.) 05 September 2002 (05.09.2002), abstarct, the entire document.	54-75
Y	US 6,275,693 B1 (LIN et al.) 14 August 14 2001 (14.08.2001), the entire document.	54-75
Y	WO 02/23825 A1 (WP MEDIA INC) 12 March 2002 (12.03.2002), the entire document.	54-75

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 October 2004 (17.10.2004)	29 OCT 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. (703) 305-9648

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/32268

Continuation of B. FIELDS SEARCHED Item 3:
Uset West data bese, NPL via ProQuest and Google Internet. Search Terms: network access device AND authentication, Access adj Connector and Authentication, Proxy AND provisiong.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

FORTINET EX1002 Page 476

C35

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

BEST AVAILABLE COPY

PCT

To:
ARIYEH AKMAL
SPRINKLE IP LAW GROUP
P.O. BOX 684767
AUSTIN, TX 78768-4767

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing (*day/month/year*) 15 DEC 2005
Applicant's or agent's file reference ROCK1 130-WO	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/29249	International filing date (*day/month/year*) 20 August 2004 (20.08.2004)
Applicant ROCKSTEADY NETWORKS, INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two *months* from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 *months* from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer for Gilberto Barron Telephone No. 1

Form PCT/ISA/220 (January 2004) (*See notes on accompanying sheet*)

PATENT COOPERATION TREATY

PCT

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ROCK1130-WO	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US04/29249	International filing date (*day/month/year*) 20 August 2004 (20.08.2004)	(Earliest) Priority Date (*day/month/year*) 20 August 2003 (20.08.2003)
Applicant ROCKSTEADY NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the Report
   a. With regard to the language, the international search was carried out on the basis of:
      ☒ the international application in the language in which it was filed.
      ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.
2. ☐ Certain claims were found unsearchable (See Box No. II)
3. ☐ Unity of invention is lacking (See Box No. III)
4. With regard to the title,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,
   a. the figure of the drawings to be published with the abstract is Figure No. 2
      ☐ as suggested by the applicant.
      ☒ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (April 2005)

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/29249

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00,9/32
US CL : 726/3,5,15
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 726/3,5,15

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
acm online

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 20020199007 A1 (CLAYTON et al) 26 December 2002 (26.12.2002), paragraphs 105-0112, 0131, 0159.	1-6, 13, 15-21, 28, 30-32, 37, 39
Y, P	US 2003/02171126 A1 (POLCHA et al.) 20 November 2003 (20.11.2003), paragraphs 0044-0047, 0056, 0063, 0103, 0108-0112.	8-12, 14, 23-27, 29, 33-36, 38
Y, P	US 6,735,691 B1 (CAPPS et al.) 11 May 2004 (11.5.2004), column 7, line 32-col. 8, line 43.	7. 22. 33

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2005 (28.11.2005)	15 DEC 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Gilberto Barron Telephone No. 1

Form PCT/ISA/210 (second sheet) (April 2005)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

BEST AVAILABLE COPY

PCT

To:
ARIYEH AKMAL
SPRINKLE IP LAW GROUP
P.O. BOX 684767
AUSTIN, TX 78768-4767

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	15 DEC 2005
Applicant's or agent's file reference ROCK1130-WO	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/29249	20 August 2004 (20.08.2004)	20 August 2003 (20.08.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): H04L 9/00,9/32 and US Cl.: 726/3,5.15

Applicant

ROCKSTEADY NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	28 November 2005 (28.11.2005)	Gilberto Barron Telephone No. 1

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

BEST AVAILABLE COPY

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

BEST AVAILABLE COPY

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	7-12,14, 22-27, 29, 33-36 and 38	YES
	Claims	1-6, 13, 15-21, 28, 30-32, 37 and 39	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-39	NO
Industrial applicability (IA)	Claims	1-39	YES
	Claims	NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2005)

BEST AVAILABLE COPY

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

1. Claims 1-6, 13, 15-21, 28, 30-32, 37 and 39 lack novelty under PCT Article 33(2) as being anticipated by Clayton et al. US Application Publication Number 2002/0199007 (hereinafter Clayton).

2. As per claim 1, Clayton discloses a method for establishing a secure connection between two computers, comprising:
a. requesting a connection, wherein the request is in a first protocol (paragraph 0106, 3rd sentence);
b. sending data in response to the request (paragraph 0106, 5th sentence);
c. configuring a second protocol using the data; and establishing the secure connection using the second protocol (paragraph 0107; paragraph 0159, optionally discloses embodiment wherein the secure connection uses other encryption schemes supplied by the VPNSP software).

3. As per claim 2, in addition, the first protocol is HTTPS (paragraph 0106, 3rd sentence).

4. As per claim 3, in addition, the data is sent using the first protocol (paragraph 0106, 5th sentence).

5. As per claim 4, in addition, the request for connection includes a username and password (paragraph 0106, 3rd sentence).

6. As per claim 5, in addition, the data is sent only if the username and password are verified (paragraph 0106, 3rd sentence, property of "logging in").

7. As per claim 6, in addition, the data includes a controller (paragraph 0106, 5th sentence).

8. As per claim 13, in addition, the second protocol is configured automatically using the controller(paragraphs 0107 and 0159).

9. As per claim 15, in addition, the secure connection is established automatically using the controller(paragraphs 0107 and 0159).

10. As per claims 16-21, 28 and 30, the arguments of claims 1-6, 13, 15 are incorporated herein. (supra) In addition, a first computer is operable to request the connection and a second computer is operable to send the data (paragraphs 0106-0107).

11. As per claims 31, 32, 37 and 39, the arguments of claims 1-6, 13, 15 are incorporated herein. (supra) In addition, the

BEST AVAILABLE COPY

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

protocol is configured on a first computer and the secure connection is established between a first computer and a second computer using the protocol (paragraphs 0106-0107).

1. Claims 8-12, 14, 23-27, 29, 34-36 and 38 lack an inventive step under PCT 33(3) as being obvious over Clayton in view of Polcha et al. US Application Publication no. 2003/0217126 (hereinafter Polcha).

2. As per claims 8-11 and 14, the arguments under PCT 33(3) as being obvious over Clayton are incorporated herein. (supra) Clayton does not expressly disclose the use of a credential. Polcha discloses a system and method of automatically configuring a remote client machine to establish a VPN via PPTP by downloading then running an executable file on to the client machine (paragraphs 0044 and 0108). Embedded or included in the executable file is data that was received from an information collection module, which collects information about the remote user and the remote user's computer; such information include credential values such as username and password (paragraphs 0056 and 0063); furthermore the credential is dynamically generated and the second protocol is configured automatically (paragraphs 0045, 0061 and 0103). Moreover, using a credential attached to the executable file enables automatic authentication to proceed by means of the various protocols to establish the VPN (paragraph 0108). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to include the use of a credential to set up the secure connection. One would be motivated to do so to enable automatic secure connection using the standard protocols available to create the VPN including PPTP, IPSec or L2TP (Polcha, paragraphs 0108-0112). The aforementioned cover the limitations of claims 8-11 and 14.

3. As per claim 12, the arguments under PCT 33(3) as being obvious over Clayton in view of Polcha are incorporated herein. (supra) In addition, Clayton discloses the controller is downloaded to clients on an as needed basis (paragraph 0131). Since, a client's session are the only times when a client requires the controller, any corresponding information to set up the session to establish the VPN tunnel is valid for the duration of the secure connection. Hence, the feature of a credential being valid only for the duration of a secure connection is an obvious enhancement. The aforementioned cover the limitations of claim 12.

4. As per claims 23-27, 29, 34-36 and 38, they are system and apparatus claims corresponding to claims 8-12 and 14, and they do not teach or define above the information claimed in claims 8-12 and 14. Therefore, claims 23-27, 29, 34-36 and 38 are obvious over Clayton in view of Polcha for the same reasons set forth in the arguments of claims 8-12 and 14.

5. Claims 7, 22 and 33 lack an inventive step under PCT 33(3) as being obvious over Clayton in view of Polcha, and further in view of Capps et al. USPN 6,735,691 (hereinafter Capps).

6. As per claim 7, the arguments under PCT 33(3) as being obvious over Clayton in view of Polcha are incorporated herein. (supra) Neither Clayton nor Polcha disclose the controller is an Active X controller. Capps discloses a system and method for automating migration of configuration information to a remote client wherein a configuration manager is downloaded and run on a client machine, the configuration manager being an Active X module (col. 8:23-43, especially lines 39-43). As well known in the art, an Active X control is a popular Microsoft controller similar to a JAVA applet that enables the sharing of information between computers. Hence, it would be obvious to one ordinary skill in the art at the time the invention was made for the controller to be an Active X controller. One would be motivated to do so because of the ubiquity of Windows OS and the flexibility of using Active X on the Windows platform: Active X has full access to the Windows OS whereas JAVA applets do not. The aforementioned cover the limitations of claim 7.

7. As per claim 22 and 33, they are system and apparatus claims corresponding to claim 7 and they do not teach or define above the information claimed in claim 7. Therefore, claims 22 and 33 are rejected as being obvious over Clayton in view of Polcha and Capps for the same reasons set forth in the argument of claim 7.

Claims 1-39 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

BEST AVAILABLE COPY

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

BEST AVAILABLE COPY

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.

C57

PATENT COOPERATION TREATY

PCT

REC'D 03 MAR 2005
WIPO PCT

Corrected

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference ROCK1100-WO	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US03/32268	International filing date *(day/month/year)* 10 October 2003 (10.10.2003)	Priority date *(day/month/year)* 10 October 2002 (10.10.2002)
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/32; G06F 15/16 and US CL.: 713/200		
Applicant ROCKSTEADY NETWORKS,INC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of ___ sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 May 2004 (10.05.2004)	04 January 2005 (04.01.2005)
Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. (571) 272-3795

Form PCT/IPEA/409 (cover sheet)(July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US03/32268

I. Basis of the report

1. With regard to the elements of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-23 as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the claims:
pages 24-34, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the drawings:
pages 1-8, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages NONE

☐ the claims, Nos. NONE

☐ the drawings, sheets/fig NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

FORTINET EX1002 Page 488

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US03/32268

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims 1-75	YES
	Claims NONE	NO
Inventive Step (IS)	Claims 1-75	YES
	Claims NONE	NO
Industrial Applicability (IA)	Claims 1-75	YES
	Claims NONE	NO

2. CITATIONS AND EXPLANATIONS

Claims 1-75 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest providing a network access wherein a user on a first network interface is directed to a second network interface for provisioning based on a user profile recited in independent claims 1, 23, 32, 54, 63 and 69.

Dependent claims 2-22, 24-31, 33-53, 55-62, 64-68 and 70-75 also meet the criteria set out in PCT Article 33(2)-(3) by virtue of their dependencies.

Claims 1-75 meet the criteria set out in PCT Article 33(4) for industrial applicability because the subject matter claimed can be made or used in industry.

NEW CITATIONS

C58

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 23 JUL 2004
WIPO PCT

Applicant's or agent's file reference ROCK1120-WO	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US03/32912	International filing date (day/month/year) 16 October 2003 (16.10.2003)	Priority date (day/month/year) 16 October 2002 (16.10.2002)
International Patent Classification (IPC) or national classification and IPC IPC(7): G06F 13/00, 11/30 and US Cl.: 709/225, 226, 232, 229, 231		
Applicant ROCKSTEADY NETWORKS, INC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of ___ sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
14 May 2004 (14.05.2004)	28 June 2004 (28.06.2004)
Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Rupal Dhania Telephone No. 703 305-9700

Form PCT/IPEA/409 (cover sheet)(July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US03/32912

I. Basis of the report

1. With regard to the elements of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-20 as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the claims:
pages 21-27, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the drawings:
pages 1-8, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages NONE

☐ the claims, Nos. NONE

☐ the drawings, sheets/fig NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

FORTINET EX1002 Page 491

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims 1-60	YES
	Claims NONE	NO
Inventive Step (IS)	Claims 1-60	YES
	Claims NONE	NO
Industrial Applicability (IA)	Claims 1-60	YES
	Claims NONE	NO

2. CITATIONS AND EXPLANATIONS

After further consideration, claims 1 - 60 meet the criteria set out in PCT Article 33(2)-(3), because the prior art (specifically Morris et al. (U.S. Pat. No. 6,336,133)) does not teach or fairly suggest updating the at least one bandwidth limit for at least one user from the set of users.

NEW CITATIONS

C59

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference ROCK1130-WO	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2004/029249	International filing date *(day/month/year)* 20 August 2004 (20.08.2004)	Priority date *(day/month/year)* 20 August 2003 (20.08.2003)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant ROCKSTEADY NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 21 February 2006 (21.02.2006)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 740 14 35	Authorized officer Philippe Becamel Telephone No. +41 22 338 70 90

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

REC'D 19 DEC 2005

From the
INTERNATIONAL SEARCHING AUTHORITY

WIPO PCT

PCT

To:
ARIYEH AKMAL
SPRINKLE IP LAW GROUP
P.O. BOX 684767
AUSTIN, TX 78768-4767

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing (*day/month/year*)	15 DEC 2005
Applicant's or agent's file reference ROCK1130-WO	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/US04/29249	20 August 2004 (20.08.2004)	20 August 2003 (20.08.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): H04L 9/00,9/32 and US Cl.: 726/3,5,15

Applicant

ROCKSTEADY NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	28 November 2005 (28.11.2005)	Gilberto Barron Telephone No. 1

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 7-12, 14, 22-27, 29, 33-36 and 38	YES
	Claims 1-6, 13, 15-21, 28, 30-32, 37 and 39	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-39	NO
Industrial applicability (IA)	Claims 1-39	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Form PCT/ISA/237 (Box No. V) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/29249

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

1. Claims 1-6, 13, 15-21, 28, 30-32, 37 and 39 lack novelty under PCT Article 33(2) as being anticipated by Clayton et al. US Application Publication Number 2002/0199007 (hereinafter Clayton).

2. As per claim 1, Clayton discloses a method for establishing a secure connection between two computers, comprising:
a. requesting a connection, wherein the request is in a first protocol (paragraph 0106, 3rd sentence);
b. sending data in response to the request (paragraph 0106, 5th sentence);
c. configuring a second protocol using the data; and establishing the secure connection using the second protocol (paragraph 0107; paragraph 0159, optionally discloses embodiment wherein the secure connection uses other encryption schemes supplied by the VPNSP software).

3. As per claim 2, in addition, the first protocol is HTTPS (paragraph 0106, 3rd sentence).

4. As per claim 3, in addition, the data is sent using the first protocol (paragraph 0106, 5th sentence).

5. As per claim 4, in addition, the request for connection includes a username and password (paragraph 0106, 3rd sentence).

6. As per claim 5, in addition, the data is sent only if the username and password are verified (paragraph 0106, 3rd sentence, property of "logging in").

7. As per claim 6, in addition, the data includes a controller (paragraph 0106, 5th sentence).

8. As per claim 13, in addition, the second protocol is configured automatically using the controller(paragraphs 0107 and 0159).

9. As per claim 15, in addition, the secure connection is established automatically using the controller(paragraphs 0107 and 0159).

10. As per claims 16-21, 28 and 30, the arguments of claims 1-6, 13, 15 are incorporated herein. (supra) In addition, a first computer is operable to request the connection and a second computer is operable to send the data (paragraphs 0106-0107).

11. As per claims 31, 32, 37 and 39, the arguments of claims 1-6, 13, 15 are incorporated herein. (supra) In addition, the

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

protocol is configured on a first computer and the secure connection is established between a first computer and a second computer using the protocol (paragraphs 0106-0107).

1. Claims 8-12, 14, 23-27, 29, 34-36 and 38 lack an inventive step under PCT 33(3) as being obvious over Clayton in view of Polcha et al. US Application Publication no. 2003/0217126 (hereinafter Polcha).

2. As per claims 8-11 and 14, the arguments under PCT 33(3) as being obvious over Clayton are incorporated herein. (supra) Clayton does not expressly disclose the use of a credential. Polcha discloses a system and method of automatically configuring a remote client machine to establish a VPN via PPTP by downloading then running an executable file on to the client machine (paragraphs 0044 and 0108). Embedded or included in the executable file is data that was received from an information collection module, which collects information about the remote user and the remote user's computer; such information include credential values such as username and password (paragraphs 0056 and 0063); furthermore the credential is dynamically generated and the second protocol is configured automatically (paragraphs 0045, 0061 and 0103). Moreover, using a credential attached to the executable file enables automatic authentication to proceed by means of the various protocols to establish the VPN (paragraph 0108). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to include the use of a credential to set up the secure connection. One would be motivated to do so to enable automatic secure connection using the standard protocols available to create the VPN including PPTP, IPSec or L2TP (Polcha, paragraphs 0108-0112). The aforementioned cover the limitations of claims 8-11 and 14.

3. As per claim 12, the arguments under PCT 33(3) as being obvious over Clayton in view of Polcha are incorporated herein. (supra) In addition, Clayton discloses the controller is downloaded to clients on an as needed basis (paragraph 0131). Since, a client's session are the only times when a client requires the controller, any corresponding information to set up the session to establish the VPN tunnel is valid for the duration of the secure connection. Hence, the feature of a credential being valid only for the duration of a secure connection is an obvious enhancement. The aforementioned cover the limitations of claim 12.

4. As per claims 23-27, 29, 34-36 and 38, they are system and apparatus claims corresponding to claims 8-12 and 14, and they do not teach or define above the information claimed in claims 8-12 and 14. Therefore, claims 23-27, 29, 34-36 and 38 are obvious over Clayton in view of Polcha for the same reasons set forth in the arguments of claims 8-12 and 14.

5. Claims 7, 22 and 33 lack an inventive step under PCT 33(3) as being obvious over Clayton in view of Polcha, and further in view of Capps et al. USPN 6,735,691 (hereinafter Capps).

6. As per claim 7, the arguments under PCT 33(3) as being obvious over Clayton in view of Polcha are incorporated herein. (supra) Neither Clayton nor Polcha disclose the controller is an Active X controller. Capps discloses a system and method for automating migration of configuration information to a remote client wherein a configuration manager is downloaded and run on a client machine, the configuration manager being an Active X module (col. 8:23-43, especially lines 39-43). As well known in the art, an Active X control is a popular Microsoft controller similar to a JAVA applet that enables the sharing of information between computers. Hence, it would be obvious to one ordinary skill in the art at the time the invention was made for the controller to be an Active X controller. One would be motivated to do so because of the ubiquity of Windows OS and the flexibility of using Active X on the Windows platform: Active X has full access to the Windows OS whereas JAVA applets do not. The aforementioned cover the limitations of claim 7.

7. As per claim 22 and 33, they are system and apparatus claims corresponding to claim 7 and they do not teach or define above the information claimed in claim 7. Therefore, claims 22 and 33 are rejected as being obvious over Clayton in view of Polcha and Capps for the same reasons set forth in the argument of claim 7.

Claims 1-39 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/092,488	04/22/2011	Patrick Turley	ROCK1150-3

CONFIRMATION NO. 6667

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

PUBLICATION NOTICE

OC000000049726176

Title:DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Publication No.US-2011-0219444-A1
Publication Date:09/08/2011

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A242	US 8032933	10-04-2011	Turley et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C120	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 08/26/2011, 9 pgs.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	11135285
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	07-OCT-2011
Filing Date:	22-APR-2011
Time Stamp:	15:03:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_100711.pdf	149855 caef68f67ed396a84b416bfcc79bf05d2ed0f038	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	4

Warnings:					
Information:					
2	Non Patent Literature	ROCK_Ref_C120.pdf	470927 a0db4dbe12ecb1f8470f55a912500a4e90a6da2f	no	9
Warnings:					
Information:					
		Total Files Size (in bytes):	620782		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2431**	Examiner **Not Yet Assigned**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on October 7, 2011.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust
Patent Agent
Reg. No. 51,032

Dated: October 7, 2011

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing or 371 (c) Date:	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	243	20080098464	04-24-2008	Mizrah	
	244	5835727	11-10-1998	Wong et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B1				
	B2				

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT				Application Number	13/092,488
				Filing or 371 (c) Date:	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	121	ALSHAMSI, ABDELNASIR, et al., "A Technical Comparison of IPSec and SSL," Tokyo University of Technology, July 8, 2004, 10 pages.	
	122	FISHER, DENNIS, "NetScreen to Acquire Neoteris," IT Security & Network Security News, October 6,-2003, 1 page.	
	123	DEMARIA, MIKE, "Faster Than a Speeding VPN--Super Remote Access With Neoteris IVE," Network Computing, 09-09-2002, printed 11-09-2011 from http://www.networkcomputing.com/data-protection/2296249, 3 pages.	
	124	SNYDER, JOEL, "SSL VPN Gateways," Networkworld, 01-12-2004, printed 11-09-2011 from http://www.networkworld.com/reviews/2004/0112revmain.html, 10 pages.	
	125	"NetExtender for SSL-VPN," SonicWALL SSL-VPN NetExtender, April 27, 2006, 30 pages.	
	126	"IPSec vs. SSL VPN: Transition Criteria and Methodology," 2007 Sonicwall, 13 pages.	
	127	FISHER, DENNIS, "Symantec Acquires SSL VPN Vendor," IT Security & Network Security News, 10-20-2003, printed 11-09-2011 from http://www.eweek.com/index2.php?option=content& task=v..." 1 page.	
	128	Notice of Allowance issued in U.S. Patent Application No. 12/617,211, mailed November 10, 2011, 8 pages.	
	129	Notice of Allowance issued in U.S. Patent Application No. 10/683,317, mailed 11-28-2011, 11 pages.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	11571670
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Katharina W. Schuster/Betty Caldwell
Filer Authorized By:	Katharina W. Schuster
Attorney Docket Number:	ROCK1150-3
Receipt Date:	08-DEC-2011
Filing Date:	22-APR-2011
Time Stamp:	13:18:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_12-08-11.pdf	157135 010af2bd113baf304da98e8e462219bd3de8efd7	yes	4

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	4	
Warnings:					
Information:					
2	Non Patent Literature	ION_Ref_C121.pdf	254301 5bdce88fb53b1a841976fcd94c18115ff0f9a8c0	no	10
Warnings:					
Information:					
3	Non Patent Literature	ION_Ref_C122.pdf	67247 8eef4f38e802437198a692aadea8c90d1dc80a21	no	1
Warnings:					
Information:					
4	Non Patent Literature	ION_Ref_C123.pdf	146505 b4f32d56a9d652c7aa69b22bbd220722f397e935	no	3
Warnings:					
Information:					
5	Non Patent Literature	ION_Ref_C124.pdf	435562 b99d6f617f833895981d46bd334eafabb9c4f805	no	10
Warnings:					
Information:					
6	Non Patent Literature	ION_Ref_C125.pdf	2900387 3ed39f1141ff7af731bf6dea82b4f5cd8615d620	no	30
Warnings:					
Information:					
7	Non Patent Literature	ION_Ref_C126.pdf	176554 ecf40c6e7549c227de46936fa52d6b390aaf6afc	no	13
Warnings:					
Information:					
8	Non Patent Literature	ION_Ref_C127.pdf	69460 98c707aa6566c7f88bda954379edfb7671b94207	no	1
Warnings:					
Information:					

9	Non Patent Literature	ROCK_Ref_C128.pdf	413006 d8de4a56acbdca6cd4b119b29ec04383f8693680	no	8
Warnings:					
Information:					
10	Non Patent Literature	ROCK_Ref_C129.pdf	500443 aabd1b4d3de9e4d4f951ca969b9adcea7cfddeee	no	11
Warnings:					
Information:					
			Total Files Size (in bytes):	5120600	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2431**	Examiner **Not Yet Assigned**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on Dec. 8 2011.

Betty Caldwell
Betty Caldwell

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

☐ The statement specified in 37 C.F.R. § 1.97(e); or

☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

Katharina W. Schuster
Reg. No. 50,000

Dated: Dec. 7, 2011

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C130	Office Action for U.S. Patent Application No. 12/753,390, mailed 12/08/2011, 19 pgs.	
	C131	Notice of Allowance for U.S. Patent Application No. 12/617,211, mailed 12/12/2011, 8 pgs.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	11744361
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	03-JAN-2012
Filing Date:	22-APR-2011
Time Stamp:	12:21:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_010312.pdf	128825 1df4f090b69e9e9c7e127ccebc4ee93a9bd6939f	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3

Warnings:					
Information:					
2	Non Patent Literature	ROCK_Ref_C130.pdf	600723 f54e9559558247b9b141a990f43051e505a115ac	no	19
Warnings:					
Information:					
3	Non Patent Literature	ROCK_Ref_C131.pdf	502919 27f31d6cb94b5237471ec14efab5dc449e125544	no	8
Warnings:					
Information:					
		Total Files Size (in bytes):	1232467		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371(c) Date **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2431**	Examiner **Not Yet Assigned**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on January 3, 2012.

Delia Narvaiz

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust

Kevin A. Gust
Patent Agent
Reg. No. 51,032

Dated: December 27, 2011

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	245	US 8108915	01-31-2012	White et al.	
	246	US 8117639	02-14-2012	MacKinnon et al.	
	247	US 20090279567	11-12-2009	Ta et al.	
	248	US 20100064356	03-11-2010	Johnston et al.	
	249	US 20100192213	07-29-2010	Ta et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	12241381
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	07-MAR-2012
Filing Date:	22-APR-2011
Time Stamp:	09:45:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_030712.pdf	129209 c3110e1913f41bc63d72e455e31c87502fec7bd8	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	129209	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **March 7, 2012**.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust
Reg. No. 51,032
Patent Agent

Dated: March 6, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	251	US 20110258687	10-20-2011	White et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	12246615
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	07-MAR-2012
Filing Date:	22-APR-2011
Time Stamp:	15:28:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_030712.pdf	124473 9f266d5bf4d9443a2d1ebfc53a02365b59978850	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	124473	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **March 7, 2012.**

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust

Kevin A. Gust
Reg. No. 51,032
Patent Agent

Dated: March 7, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C132	Notice of Allowance issued for U.S. Patent Application No. 12/753,390, mailed March 16, 2012, 9 pages.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	12510153
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	10-APR-2012
Filing Date:	22-APR-2011
Time Stamp:	16:32:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_041012.pdf	120921 0f38dfaa2c653c94356d52be5881a02ec90f67b4	yes	3

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
Warnings:					
Information:					
2	Non Patent Literature	ROCK_Ref_C132.pdf	142861 f1d54bdb9ef93c91d71a455eabc4895eaba1b36f	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	263782		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **Dynamically Adaptive Network Firewalls and Method, System and Computer Program Product Implementing Same**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **April 10, 2012.**

Delia Narvaiz

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust
Reg. No. 51,032
Patent Agent

Dated: April 9, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	252	US 20120096517	04-19-2012	White et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	12630519
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Kevin Gust/Delia Narvaiz
Filer Authorized By:	Kevin Gust
Attorney Docket Number:	ROCK1150-3
Receipt Date:	25-APR-2012
Filing Date:	22-APR-2011
Time Stamp:	17:39:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_042512.pdf	125721 bd532e62cd7110582fdbd73857d704d69b540a98	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	125721	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **Dynamically Adaptive Network Firewalls and Method, System and Computer Program Product Implementing Same**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on **April 25, 2012.**

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Kevin A. Gust
Reg. No. 51,032
Patent Agent

Dated: April 25, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	253	US 20120117615	05-10-2012	MacKinnon et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C137	Office Action for U.S. Patent Application No. 12/619,560, mailed 05/09/2012, 7 pgs.	
	C138	BAUER, MICK, Designing and Using DMZ Networks to Protect Internet Servers, Linux Journal, March 1, 2001, 6 pgs. at http://linuxjournal.com/article/4415, printed 03/22/2012.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	12901485
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Katharina W. Schuster/Delia Narvaiz
Filer Authorized By:	Katharina W. Schuster
Attorney Docket Number:	ROCK1150-3
Receipt Date:	31-MAY-2012
Filing Date:	22-APR-2011
Time Stamp:	13:40:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_053112.pdf	156207 1d59e801ee66226386fb82573c81b2b4e4a5396b	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	4

Warnings:					
Information:					
2	Non Patent Literature	ROCK_Ref_C137.pdf	274515 e6273bed95fca15fd43a567d3902d71162883f99	no	7
Warnings:					
Information:					
3	Non Patent Literature	ROCK_Ref_C138.pdf	364256 2e76b94aa1948e519cb6db4d4d43cb111c693bbc	no	6
Warnings:					
Information:					
		Total Files Size (in bytes):	794978		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **Dynamically Adaptive Network Firewalls and Method, System and Computer Program Implementing Same**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on May 31 2012.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☒ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Katharina W. Schuster
Reg. No. 50,000

Dated: May 29, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	ROCK1150-3	6667

44654 7590 06/11/2012

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/11/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	13/092,488	TURLEY ET AL.	
	Examiner	Art Unit	
	MINH DINH	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-38* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-3,5-15,17-28 and 30-38* is/are rejected.

8)☒ Claim(s) *4,16 and 29* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 6-8, 18-20 and 31-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 recites "wherein the at least one node further comprises a second node, further comprising associating a second subset of the set of firewall rules with the second node." Since "the at least one node" can be interpreted as one node, it is not clear how it comprises a second node. For prior art rejection purposes, "the at least one node" is interpreted as being "at least two nodes". Claims 18 and 31 are rejected on the same basis as claim 6.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 5-9, 11-15, 17-21, 23-28, 30-34 and 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartal et al. (US 7,146,639 B2) in view of Qian et al. (US 2005/0138416 A1).

6. Regarding claims 1-3, 9, 11-15, 21, 23-28, 34 and 36-38, Bartal discloses a method and device for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising: defining at least one node, wherein the at least one node is associated with two or more network interfaces (fig. 1; fig. 2, elements 300, 250; fig. 5; fig. 9; col. 6, lines 30-39, 57-67; col. 7, lines 1-9); associating a set of firewall rules with the at least one node (col. 9, lines 27-39); receiving a packet at a first node of the at least one node; and accepting or denying the packet based on the set of firewall rules (col. 1, lines 29-31; col. 9, lines 31-39).

Bartal does not disclose reconfiguring the firewall at runtime. Qian discloses utilizing an object model to manage and configure a firewall (Abstract). Specifically, Qian discloses reconfiguring a firewall (i.e., adding, deleting, and/or updating a firewall rule) at runtime using the object model (figures 8 and 10; paragraphs 0057-0064). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bartal method to utilize Qian's object model to reconfigure the firewall at run time. The motivation for doing so would have been to isolate a user and/or an administrator from having to deal with the many possible issues involved in configuring the firewall services (Abstract).

7. Regarding claims 5-8, 17-20 and 30-33, Bartal further discloses associating a first subset of the set of firewall rules with the first node and associating a second subset of the set of firewall rules with the second node (col. 11, lines 40-50).

8. Claims 10, 22 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartal in view of Qian as applied to claims 9, 21 and 34 above, and further in view of Aroya (US 7,634,805). Bartal and Qian do not disclose rewriting a portion of a network packet header associated with the packet. Aroya discloses a method for controlling a data packet through a firewall including rewriting a portion of a network packet header associated with the packet (fig. 2; col. 4, line 45 – col. 5, line 13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Bartal and Qian to rewrite a portion of a network packet header associated with the packet, as taught by Aroya. The motivation for doing so would have been to preserve a routing effect.

Double Patenting

9. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422

F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 1-4, 13-16 and 26-29 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2, 11 and 16 of U.S. Patent No. 8,032,933. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 2, 11 and 16 of U.S. Patent No. '933 contain(s) every element of claims 1-4, 13-16 and 26-29 of the instant application and as such anticipate(s) claims 1-4, 13-16 and 26-29 of the instant application.

11. Claims 1-3, 9, 13-15, 21, 26-28 and 34 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 7, 14 and 19 of U.S. Patent No. 7,160,621. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 7, 14 and 19 of U.S. Patent No. '621 contain(s) every element of claims 1-3, 9, 13-15, 21, 26-28 and

34 of the instant application and as such anticipate(s) claims 1-4, 13-16 and 26-29 of the instant application.

Allowable Subject Matter

12. Claims 4, 16 and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 09:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Minh Dinh/
Primary Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 13/092,488	Applicant(s)/Patent Under Reexamination TURLEY ET AL.	
	Examiner MINH DINH	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,634,805	12-2009	Aroya, Ishai Ben	726/13
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Receipt date: 03/07/2012

Substitute Form for PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	245	US 8108915	01-31-2012	White et al.	
	246	US 8117639	02-14-2012	MacKinnon et al.	
	247	US 20090279567	11-12-2009	Ta et al.	
	248	US 20100064356	03-11-2010	Johnston et al.	
	249	US 20100192213	07-29-2010	Ta et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form for PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
/MD/	251	US 20110258687	10-20-2011	White et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
/MD/	C132	Notice of Allowance issued for U.S. Patent Application No. 12/753,390, mailed March 16, 2012, 9 pages.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

Receipt date: 05/31/2012

Substitute Form PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	253	US 20120117615	05-10-2012	MacKinnon et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

EDR, INC. (800) 352-0050

Receipt date: 05/31/2012

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C137	Office Action for U.S. Patent Application No. 12/619,560, mailed 05/09/2012, 7 pgs.	
	C138	BAUER, MICK, Designing and Using DMZ Networks to Protect Internet Servers, Linux Journal, March 1, 2001, 6 pgs. at http://linuxjournal.com/article/4415, printed 03/22/2012.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

EOR IN RE EX 1102 Page 556

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A242	US 8032933	10-04-2011	Turley et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C120	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 08/26/2011, 9 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered 06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute for PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing or 371 (c) Date:	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	243	20080098464	04-24-2008	Mizrah	
	244	5835727	11-10-1998	Wong et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B1				
	B2				

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute for PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT				Application Number	13/092,488
				Filing or 371 (c) Date:	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	121	ALSHAMSI, ABDELNASIR, et al., "A Technical Comparison of IPSec and SSL," Tokyo University of Technology, July 8, 2004, 10 pages.	
	122	FISHER, DENNIS, "NetScreen to Acquire Neoteris," IT Security & Network Security News, October 6,-2003, 1 page.	
	123	DEMARIA, MIKE, "Faster Than a Speeding VPN--Super Remote Access With Neoteris IVE," Network Computing, 09-09-2002, printed 11-09-2011 from http://www.networkcomputing.com/data-protection/2296249, 3 pages.	
	124	SNYDER, JOEL, "SSL VPN Gateways," Networkworld, 01-12-2004, printed 11-09-2011 from http://www.networkworld.com/reviews/2004/0112revmain.html, 10 pages.	
	125	"NetExtender for SSL-VPN," SonicWALL SSL-VPN NetExtender, April 27, 2006, 30 pages.	
	126	"IPSec vs. SSL VPN: Transition Criteria and Methodology," 2007 Sonicwall, 13 pages.	
	127	FISHER, DENNIS, "Symantec Acquires SSL VPN Vendor," IT Security & Network Security News, 10-20-2003, printed 11-09-2011 from http://www.eweek.com/index2.php?option=content& task=v..." 1 page.	
	128	Notice of Allowance issued in U.S. Patent Application No. 12/617,211, mailed November 10, 2011, 8 pages.	
	129	Notice of Allowance issued in U.S. Patent Application No. 10/683,317, mailed 11-28-2011, 11 pages.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 6667

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/092,488	04/22/2011	726	2432	ROCK1150-3

APPLICANTS

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

**** CONTINUING DATA ***************************

This application is a CON of 12/579,566 10/15/2009 PAT 8,032,933
which is a CON of 11/076,719 03/10/2005 PAT 7,610,621
which claims benefit of 60/551,698 03/10/2004 *
(*)Data provided by applicant is not consistent with PTO records.

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
05/05/2011

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /MINH DINH/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		TX	3	38	3

ADDRESS

Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705
UNITED STATES

TITLE

DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

FILING FEE RECEIVED		
930	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Substitute Form PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
/MD/	252	US 20120096517	04-19-2012	White et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

Substitute Form PTO/SB/08A

AUG 2 9 2011 PATENT & TRADEMARK OFFICE AP21

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 1 of 12

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A1	US 5673393	09-30-1997	Marshall et al.	
	A2	US 5706427	01-06-1998	Tabuki	
	A3	US 5748901	05-05-1998	Afek et al.	
	A4	US 5901148	05-04-1999	Bowen et al.	
	A5	US 5936542	08-10-1999	Kleinrock et al.	
	A6	US 5987134	11-16-1999	Shin et al.	
	A7	US 5996013	11-30-1999	Delp et al.	
	A8	US 6085241	07-04-2000	Otis	
	A9	US 6108782	08-22-2000	Fletcher et al.	
	A10	US 6130892	10-10-2000	Short et al.	
	A11	US 6131116	10-10-2000	Riggins et al.	
	A12	US 6157953	12-05-2000	Chang et al.	
	A13	US 6173331	01-09-2001	Shimonishi	
	A14	US 6176883	01-23-2001	Holloway et al.	
	A15	US 6185567	02-06-2001	Ratnaraj et al.	
	A16	US 6194992	02-27-2001	Short et al.	
	A17	US 6212558	04-03-2001	Antur et al.	
	A18	US 6233607	05-15-2001	Taylor et al.	
	A19	US 6243815	06-05-2001	Antur et al.	
	A20	US 6295294	09-25-2001	Odlyzko	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B1	EP 0 587 522 A2	03-16-1994	Int'l Business Mach. Corp.	
	B2	WO 01/077787 A3	10-18-2001	Siebel Systems, US	
	B3	WO 02/09458 A2	01-31-2002	Bluesocket, Inc., US	
	B4	WO 02/023825 A1	03-21-2002	WP Media Inc.	
	B5	WO 02/041587 A2	05-23-2002	Bluesocket, Inc., US	
	B6	WO 02/077820 A1	10-03-2002	Bluesocket, Inc., US	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	2	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A21	US 6321339	11-20-2001	French et al.	
	A22	US 6324648	11-27-2001	Grantges, Jr.	
	A23	US 6404743	06-11-2002	Meandzija	
	A24	US 6421319	07-16-2002	Iwasaki	
	A25	US 6463474	10-08-2002	Fuh et al.	
	A26	US 6473793	10-29-2002	Dillon et al.	
	A27	US 6473801	10-29-2002	Basel	
	A28	US 6535879	03-18-2003	Behera	
	A29	US 6539431	03-25-2003	Sitaraman et al.	
	A30	US 20010039576	11-08-2001	Kanada	
	A31	US 20020013844	01-31-2002	Garrett et al.	
	A32	US 20020021665	02-21-2002	Bhagavath et al.	
	A33	US 20020023160	02-21-2002	Garrett et al.	
	A34	US 20020035699	03-21-2002	Crosbie	
	A35	US 20020042883	04-11-2002	Roux et al.	
	A36	US 20020046264	04-18-2002	Dillon et al.	
	A37	US 20020052950	05-02-2002	Pillai et al.	
	A38	US 20020055968	05-09-2002	Wishoff et al.	
	A39	US 20020059408	05-16-2002	Pattabhiraman et al.	
	A40	US 20020085719	07-04-2002	Crosbie	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	B7	WO 03/021890 A1	03-13-2003	The Boeing Co., US	
	B8	WO 03/098461 A1	11-27-2003	Polcha et al.	
	B9	WO 04/034229 A2	04-22-2004	Rocksteady Networks, Inc.	
	B10	WO 04/036371 A2	04-29-2004	Rocksteady Networks, Inc.	
	B11	WO 05/020035 A2	03-03-2005	Rocksteady Networks, Inc.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	3	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A41	US 20020087713	07-04-2002	Cunningham	
	A42	US 20020091944	07-11-2002	Anderson et al.	
	A43	US 20020112183	08-15-2002	Baird, III et al.	
	A44	US 20020120741	08-29-2002	Webb et al.	
	A45	US 20020124078	09-05-2002	Conrad	
	A46	US 20020124103	09-05-2002	Maruyama et al.	
	A47	US 20020129143	09-12-2002	McKinnon, III et al.	
	A48	US 20020133581	09-19-2002	Schwartz et al.	
	A49	US 20020133589	09-19-2002	Gubbi et al.	
	A50	US 20020136226	09-26-2002	Christoffel et al.	
	A51	US 20020138762	09-26-2002	Horne	
	A52	US 20020143964	10-03-2002	Guo et al.	
	A53	US 20020152284	10-17-2002	Cambray et al.	
	A54	US 20020162030	10-31-2002	Brezak et al.	
	A55	US 20020164952	11-07-2002	Singhal et al.	
	A56	US 20020165990	11-07-2002	Singhal et al.	
	A57	US 20020169867	11-14-2002	Mann et al.	
	A58	US 20020174227	11-21-2002	Hartsell et al.	
	A59	US 20020178282	11-28-2002	Mysore et al.	
	A60	US 20030043846	03-06-2003	Purpura et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	4	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A61	US 20030087629	05-08-2003	Juitt et al.	
	A62	US 5953506	09-14-1999	Kalra et al.	
	A63	US 6336133	01-01-2002	Morris et al.	
	A64	US 6502131	12-31-2002	Vaid et al.	
	A65	US 5878231	03-02-1999	Baehr et al.	
	A66	US 6088451	07-11-2000	He et al.	
	A67	US 6275693	08-14-2001	Lin et al.	
	A68	US 20020112186	08-15-2002	Ford et al.	
	A69	US 20020123335	09-05-2002	Luna et al.	
	A70	US 20020138763	09-26-2002	Delany et al.	
	A71	US 6205552	03-20-2001	Fudge	
	A72	US 6477143	11-05-2002	Ginossar	
	A73	US 6092200	07-18-2000	Muniyappa et al.	
	A74	US 6516417	02-04-2003	Pegrum et al.	
	A75	US 20030135753	07-17-2003	Batra et al.	
	A76	US 6735691	05-11-2004	Capps et al.	
	A77	US 20020199007	12-01-2002	Clayton et al.	
	A78	US 20030149751	08-07-2003	Bellinger et al.	
	A79	US 20030159072	08-21-2003	Bellinger et al.	
	A80	US 20030217126	11-20-2003	Polcha et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	5	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A81	US 20040049586	03-11-2004	Ocepek et al.	
	A82	US 20050193103	09-01-2005	Drabik, John	
	A83	US 5896499 A	04-20-1999	McKelvey	
	A84	US 6804783	10-12-2004	Wesinger et al.	
	A85	US 7181017	02-20-2007	Nagel et al.	
	A86	US 20020075844	06-01-2002	Hagen	
	A87	US 20040199635	10-07-2004	Ta et al.	
	A88	US 20050204168	09-15-2005	Johnston et al.	
	A89	US 20030212800	11-01-2003	Jones et al.	
	A90	US 6757740	06-01-2004	Parekh et al.	
	A91	US 20020029260	03-01-2002	Dobbins et al.	
	A92	US 20030069956	04-01-2003	Gieske et al.	
	A93	US 20030163603	08-01-2003	Fry et al.	
	A94	US 20030177477	09-01-2003	Fuchs	
	A95	US 20040268234	12-01-2004	Sampathkumar et al.	
	A96	US 6708212	03-16-2004	Porras et al.	
	A97	US 7272646	09-18-2007	Cooper et al.	
	A98	US 6785252	08-31-2004	Zimmerman et al.	
	A99	US 6823385	11-23-2004	McKinnon et al.	
	A100	US 6917622	07-12-2005	McKinnon et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	6	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A101	US 20010038639	11-08-2001	McKinnon et al.	
	A102	US 20010038640	11-08-2001	McKinnon et al.	
	A103	US 20010038645	11-08-2001	McKinnon et al.	
	A104	US 20010039582	11-08-2001	McKinnon et al	
	A105	US 7013331	03-14-2006	Das	
	A106	US 20030055994	03-20-2003	Herrmann et al.	
	A107	US 7143283	11-28-2006	Chen et al.	
	A108	US 7146639	12-05-2006	Bartal et al.	
	A109	US 6636894	10/21/2003	Short et al	
	A110	US 6789110	09-07-2004	Short et al.	
	A111	US 7120934	10-10-2006	Ishikawa	
	A112	US 7185368	02-27-2007	Copeland III	
	A113	US 7266754	09-04-2007	Shah	
	A114	US 7454792	11-18-2008	Cantrell et al.	
	A115	US 20030061506	03-27-2003	Cooper	
	A116	US 20030154399	08-14-2003	Zuk	
	A117	US 20040015719	01-22-2004	Lee	
	A118	US 20040047356	03-11-2004	Bauer	
	A119	US 20040085906	09-19-2008	Ohtani	
	A120	US 20040093513	05-13-2004	Cantrell	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	7	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A121	US 20040172557	09-02-2004	Nakae et al.	
	A122	US 20050044422	02-24-2005	Cantrell	
	A123	US 20050091303	04-28-2005	Suzuki	
	A124	US 20050149721	07-07-2005	Lu	
	A125	US 20060168229	07-27-2006	Shim, et al.	
	A126	US 6732179	05-04-2004	Brown et al.	
	A127	US 6678733	01-13-2004	Brown et al.	
	A128	US 7324947	01-29-2008	Jordan et al	
	A129	US 7325042	01-29-2008	Soscia et al.	
	A130	US 7406530	07-29-2008	Brown et al.	
	A131	US 7420956	09-02-2008	Karaoguz et al.	
	A132	US 20020131404	09-19-2002	Mehta et al.	
	A133	US 20030041104	02-27-2003	Wingard et al.	
	A134	US 20030070170	04-10-2003	Lennon	
	A135	US 20030078784	04-24-2003	Jordan et al.	
	A136	US 20030126608	07-03-2003	Safadi et al.	
	A137	US 20040064836	04-01-2004	Ludvig et al.	
	A138	US 20040073941	04-15-2004	Ludvig et al.	
	A139	US 20040103426	05-27-2004	Ludvig et al.	
	A140	US 20040122956	06-24-2004	Myers et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	8	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A141	US 20040179822	09-16-2004	Tsumagari et al.	
	A142	US 20040181816	09-16-2004	Kim et al.	
	A143	US 20040210633	10-21-2004	Brown et al.	
	A144	US 20050195854	09-08-2005	Agmon et al.	
	A145	US 20060184618	08-17-2006	Kurup et al.	
	A146	US 20070073718	03-29-2007	Ramer et al.	
	A147	US 20070186113	08-09-2007	Cuberson et al.	
	A148	US 20070208936	09-06-2007	Ramos Robles	
	A149	US 20070268878	11-22-2007	Clements	
	A150	US 20080066096	03-13-2008	Wollmershauser et al.	
	A151	US 20080120661	05-22-2008	Ludvig et al.	
	A152	US 20080147840	06-19-2008	Roelens et al.	
	A153	US 20080276305	11-06-2008	Chan et al.	
	A154	US 20060173992	08-03-2006	Weber et al.	
	A155	US 20030046370	03-06-2003	Courtney	
	A156	US 20050021686	01-27-2005	Jai et al.	
	A157	US 20030059038	03-27-2003	Meyerson et al.	
	A158	US 20030172167	09-11-2003	Judge et al.	
	A159	US 20040177276	09-05-2004	MacKinnon et al.	
	A160	US 20050044350	02-24-2005	White et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	9	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A161	US 20050204022	09-15-2005	Johnston et al.	
	A162	US 20050204031	09-05-2005	Johnston et al.	
	A163	US 20050204050	09-15-2005	Turley	
	A164	US 20050204402	09-15-2005	Turley et al.	
	A165	US 20060036723	02-16-2006	Yip et al.	
	A166	US 20050138416	06-23-2005	Qian et al.	
	A167	US 20050204169	09-15-2005	Tonnesen	
	A168	US 20020090089	07-11-2002	Branigan	
	A169	US 6199113	03-06-2001	Alegre et al.	
	A170	US 7509625	03-24-2009	Johnston et al.	
	A171	US 6219706	04-17-2001	Fan et al.	
	A172	US 7624438	11-24-2009	White	
	A173	US 7587512	09-08-2009	Ta et al.	
	A174	US 7610621	10-27-2009	Turley et al.	
	A175	US 7590728	09-15-2009	Tonnesen et al.	
	A176	US 20020138631	09-26-2002	Friedel et al.	
	A177	US 7665130	02-16-2010	Johnston et al.	
	A178	US 6226752	05-01-2001	Gupta et al.	
	A179	US 6631416	10-07-2003	Bendinelli et al.	
	A180	US 6763468	07-13-2004	Gupta et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	10	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A181	US 7085854	08-01-2006	Keane et al.	
	A182	US 7143435	11-28-2006	Droms et al.	
	A183	US 7181542	02-20-2007	Tuomenoksa et al.	
	A184	US 7181766	02-20-2007	Bendinelli et al.	
	A185	US 7194554	03-20-2007	Short et al.	
	A186	US 7290288	10-30-2007	Gregg et al.	
	A187	US 7316029	01-01-2008	Parker et al.	
	A188	US 7324551	01-29-2008	Stammers	
	A189	US 7448075	11-04-2008	Morand et al.	
	A190	US 20020023210	02-21-2002	Tuomenoksa et al.	
	A191	US 20020026503	02-28-2002	Bendinelli et al.	
	A192	US 20020026531	02-28-2002	Keane et al.	
	A193	US 20020029276	03-07-2002	Bendinelli et al.	
	A194	US 20020053031	05-02-2002	Bendinelli et al.	
	A195	US 20020056008	05-09-2002	Keane et al.	
	A196	US 20020091859	07-11-2002	Tuomenoksa et al.	
	A197	US 20020099829	07-25-2002	Richards et al.	
	A198	US 20030115247	06-19-2003	Simpson et al.	
	A199	US 20030182420	09-25-2003	Jones et al.	
	A200	US 20040083295	04-29-2004	Amara et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	11	of	12	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A201	US 20040215957	10-28-2004	Moineau et al.	
	A202	US 20050021975	01-27-2005	Liu	
	A203	US 7310613	12-18-2007	Briel et al.	
	A204	US 20030110073	06-12-2003	Briel et al.	
	A205	US 20100192213	07-29-2010	Ta et al.	
	A206	US 20040268149	12-30-2004	Aaron	
	A207	US 20030212900	11-13-2003	Liu et al.	
	A208	US 20020133586	09-12-2002	Shanklin et al.	
	A209	US 7386888	06-10-2008	Liang et al.	
	A210	US 6266774	07-24-2001	Sampath et al.	
	A211	US 6502135	12-31-2002	Munger et al.	
	A212	US 6839759	01-04-2005	Larson et al.	
	A213	US 7188180	03-06-2007	Larson et al.	
	A214	US 7418504	08-26-2008	Larson et al.	
	A215	US 7490151	02-10-2009	Munger et al.	
	A216	US 20040064351	04-01-2004	Mikurak	
	A217	US 20040064560	04-01-2004	Zhang et al.	
	A218	US 6834341	12-21-2004	Bahl et al.	
	A219	US 20050066200	03-24-2005	Bahl et al.	
	A220	US 20050138358	06-23-2005	Bahl et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Substitute Form PTO/SB/08A

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 12 of 12

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	A221	US 20060168454	07-27-2006	Venkatachary et al.	
	A222	US 7092727	08-15-2006	Li et al.	
	A223	US 7444669	10-28-2008	Bahl et al.	
	A224	US 7185358	02-27-2007	Schreiber et al.	
	A225	US 7085385	08-01-2006	Frantz et al.	
	A226	US 6907530	06-14-2005	Wang	
	A227	US 5623601	04-22-1997	Vu	
	A228	US 20030123442	07-03-2003	Drucker et al.	
	240	US 6996625	02-07-2006	Kaplan et al.	
	241	US 20040107290	06-03-2004	Kaplan et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

USPAP IAP21 AUG 29 2011 PATENT & TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 11

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C1	LINGBLOM, MARIE, "Bluesocket's New Gateway Based on Open Standards – WGX-4000 Switch Wireless Gateway, CRN, Burlington, MA, found at www.crn.channelsupersearch.com, 4-21-2003, 2 pgs.	No Copy
	C2	"Boingo Wireless Service Installed at LaGuardia Airport," 06/17/2003, Copyright 2003 M2Communications Ltd., found at www.findarticles.com, 12-08-2003, 1 pg.	
	C3	"West Point Unwired: the Military Academy at West Point Continues to Lead the Way in High-Tech Curriculum with Wireless Classroom Networking," Communication News, June 2003, Copyright 2003 M2 Communications Ltd., found at www.findarticles.com, 5 pgs., printed 12/8/03.	
	C4	MOLTA, DAVE, "Wireless Hotspots Heat Up," Mobile & Wireless Technology, pp.1-8, 05/15/2003, Copyright 2003 M2Communications Ltd., found at www.networkcomputing.com, printed 12/08/2003, 8 pgs..	
	C5	JACKSON, WILLIAM, "Wireless at West Point: Officers of the Future Use IT in Class Now, in the Field Later (Technology Report)," 04/21/2003, GCN, pp.1-3, www.gcn.com.	
	C6	LINGBLOM, MARIE, "Cranite Develops SMB Strategy, CRN, San Jose, CA, June 23, 2003, 2 pgs.	
	C7	DORNAN, ANDY "Wireless LANs: Freedom vs. Security?" Network Magazine, July 2003, pps. 36-39, www.networkmagazine.com.	
	C8	O'SHEA, DAN, "PCTEL looks past patent suit toward fusion of Wi-Fi, PC" Telephony.online, 06/02/2003, pp. 1-2, found at www.telephonyonline.com, Primedia Business Magazines and Media, printed 12/08/2003.	
	C9	O'SHEA, DAN, "Boingo to Launch Initiative Aimed at Carrier Market" Telephony.online, 03/10/2003, 1 pg., found at www.telephonyonline.com, Primedia Business Magazines and Media, printed 12/08/2003.	
	C10	International Search Report for International Patent Application No. PCT/US03/32912, completed 03/22/2004, mailed 04/08/2004, 6 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	2	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C11	International Search Report for International Patent Application No. PCT/US03/32268, completed 10/17/2004, mailed 10/29/2004, 6 pgs.	
	C12	FAN, CHEN, et al, "Distributed Real Time Intrusion Detection System for 3G," Proceedings of ICCC2004, 2004, pp. 1566-70.	
	C13	YU, ZHAO-xu et al., "Fuzzy Logic Based Adaptive Congestion Control Scheme for High-Speed Network," Vol. 33, No. 4, Information and Control, August 2004, pp. 389-93 (with English abstract).	
	C14	HAMANO, TAKAFUMI et al., "A Redirection-Based Defense Mechanism Against Flood-Type Attacks in Large Scale ISP Networks," 10th Asia-Pacific Conf. on Comm. and 5th Int'l Symposium on Multi-Dimensional Mobile Comm., 2004, pp. 543-547, IEEE #07803-8601-09/04.	
	C15	SAROLAHTI, PASI, "Congestion Control on Spurious TCP Retransmssion Timeouts," Globecom 2003, pp. 682-686, IEEE #0-7803-7974-8.	
	C16	ESTEVEZ-TAPIADOR, JUAN M., et al., "Measuring Normality in HTTP Traffic for Anomaly-Based Intrusion Detection," Computer Networks 45 (2004), pp. 175-193, available at www.sciencedirect.com, El Sevier 2004 #13891286.	
	C17	XING, XU-JIA, et al., "A Survey of Computer Vulnerability Assessment," Chinese Journal of Computers, Vol. 27, No. 1, Jan. 2004, pp. 1-11 (with English abstract).	
	C18	WEN et al. "Development of a Snort-Based Security Network Management and Real-Time Intrusion Detection System," Journal of Beijing Normal Univ. (Natural Science), Vol. 40, No. 1, February 2004, pp. 40-43 (with English abstract).	
	C19	THOTTETHODI, METHUNE, et al., "Exploiting Global Knowledge to Achieve Self-Tuned Congestion Control for k-Ary n-Cube Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 15, No. 3, March 2004, pp. 257-272, IEEE #1045-9219/04.	
	C20	TRABELSI, ZOUHEIR, et al., "Malicious Sniffing Systems Detection Platform," 2004 IEEE, pp. 201-207, IEEE #0-7695-2068-5/04.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	3	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C21	GUANGZHI, QU, et al., "A Framework for Network Vulnerability Analysis," Proceedings of the IASTED Int'l Conf., Comm., Internet & Information Tech., November 18-20, 2004, St. Thomas, US Virgin Islands, pp. 289-294.	
	C22	ALBUQUERQUE, CELIO, et al., "Network Border Patrol: Preventing Congestion Collapse and Promoting Fairness in the Internet," IEEE/ACM Transactions on Networking, Vol. 12, No. 1, February 2004, pp. 173-186, IEEE #1063-6692/04.	
	C23	WIRBEL, LORING, "Security Stampede Could Flatten IPSec," Network Magazine, January 2004, p. 12, available at www.networkmagazine.com.	
	C24	MACLEOD, CALUM, "Freeing the Shackles with Secure Remote Working," Comtec, October 2003, pp. 66-67.	
	C25	FISHER, DENNIS, "SSL Simplifies VPN Security," IT Week, 11/10/2003, pg. 40, available at www.eweek.com/security.	
	C26	CONRY-MURRAY, ANDREW, "SSL VPNs: Remote Access for the Masses," Network Magazine, October 2003, pp. 26-32, available at www.networkmagazine.com.	
	C27	"Permeo Supports Microsoft Network Access Protection for Simplified Secure Remote Access; Permeo's Base5 Support of Microsoft Technology Provides "Zero Touch" Policy Enforcement", 04/25/2005, 2 pgs., Newswire, found at www.nerac.com. #NDN-121-0552-8254-9.	
	C28	"Permeo Drives Out Operational Costs, Simplifies Secure Remote Access, 03/25/2005, 2 pgs., Newswire, found at www.nerac.com. #NDN-121-0549-5967-5.	
	C29	"Netilla Lauches SSL VPN for Citrix. (Industry Briefs) (Virtual Private Networks) (Brief Article)," 09/20/2004, 2 pgs., Computer Reseller News, found at www.nerac.com. #NDN-218-0991-7652-9.	
	C30	"Netilla Lauches Secure Gateway Appliance Family of Application-Specific SSL VPN Products; Initial SGA-C Model Provides Secure Remote Access to Citrix MetaFrame Presentation Server Installations..." 09/13/2004, 3 pgs., PR Newswire, found at www.nerac.com. #NDN-218-0987-0667-2.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	4	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C31	"Secure Remote Access.(Network Security) (VPN Gateway 4400 Series) (Brief Article)," March 1, 2004, 2 pgs., Communication News, Vol. 41, found at www.nerac.com. #NDN-218-0925-2711-6.	
	C32	"Fortinet and Aventail Deliver Joint Solution for Clientless Remote Access with High-Performance Antivirus Protection; Integrated SSL VPN and Antivirus Offering Provides Clientless Remote Access with Complete Content Security", 01/05/2004, 3 pgs., PR Newswire, found at www.nerac.com. #NDN-218-0845-8319-2	
	C33	HAMBLEN, MATT, "Cisco Targets SSL VPN Vendors, Adds Support for Clientless Security Protocol: Installed Base of VPN Devices May Give it an Edge, Despite Late Entry," 11/17/2003, 3 pgs., Computerworld, Vol. 37, No. 46, found at www.nerac.com. #NDN-218-0841-5076-0.	
	C34	HAMZEH, K., et al., "Point-to-Point Tunneling Protocol--PPTP RFC 2637" Network Working Groups, July 1999, pp. 1-54, Microsoft Corporation.	
	C35	International Search Report and Written Opinion for International Patent Application No. PCT/US04/29249, completed 11/28/2005, mailed 12/15/2005, 10 pgs.	
	C36	PFLEEGER, CHARLES P., Computer Network Security, Security in Computing, 1989, pp. 364-415, Ch. 10, PTR Prentice-Hall, Inc., Englewood Cliffs, NJ.	
	C37	Office Action for U.S. Patent Application No. 10/922,041, mailed 07/13/2007, 20 pgs.	
	C38	STONE, DAVID, "Securing Wireless LANs with VPN", Intel Information Technology White Paper, Intel Corp., May 2006, 8 pgs. Order N#313185-001US.	
	C39	Office Action for U.S. Patent Application No. 10/683,317, mailed 10/09/2007, 20 pgs.	
	C40	Office Action for U.S. Patent Application No. 10/687,002, mailed 10/18/2007, 10 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	5	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C41	Office Action for U.S. Patent Application No. 11/078,223, mailed 10/31/2007, 8 pgs.	
	C42	Office Action for U.S. Patent Application No. 11/076,652, mailed 01/25/2008, 9 pgs.	
	C43	Office Action for U.S. Patent Application No. 10/687,002, mailed 04/17/2008, 12 pgs.	
	C44	Office Action for U.S. Patent Application No. 10/683,317, mailed 06/09/2008, 15 pgs.	
	C45	Office Action for U.S. Patent Application No. 11/076,672, mailed 07/09/2008, 12 pgs.	
	C46	Office Action for U.S. Patent Application No. 11/076,652, mailed 07/22/2008, 8 pgs.	
	C47	Office Action for U.S. Patent Application No. 11/076,591, mailed 08/13/2008, 10 pgs.	
	C48	Office Action for U.S. Patent Application No. 11/076,719, mailed 09/04/2008, 7 pgs.	
	C49	SBC TECHNOLOGY RESOURCES, INC., XNMP-XML Network Management Protocol and Interface, 07-19-2002, pp.1-9, http://www.ietf.org/proceedings/02jul/slides	
	C50	Shim, Choon B., " XNMP for IP Telephony Management," Enterprise Networks & Servers, June 2, 2006, 7 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	6	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C51	Office Action for U.S. Patent Application No. 11/076,652, mailed 12/11/2008, 8 pgs.	
	C52	Office Action for U.S. Patent Application No. 10/687,002, mailed 01/07/2009, 14 pgs.	
	C53	Office Action for U.S. Patent Application No. 11/076,672, mailed 02/03/2009, 10 pgs.	
	C54	Oh, et al., "Interaction Translation Methods for XML/SNMP Gateway," July 11, 2003, retrieved from http://web-archive.org/web/20030711162412/http://dpnm.postech.ac.kr/papers/DSOM/02/xml-snmp-gateway/xml-snmp-gateway.pdf, pgs. 1-12.	
	C55	Office Action for U.S. Patent Application No. 10/683,317, mailed 02/11/2009, 17 pgs.	
	C56	Office Action for U.S. Patent Application No. 11/076,591, mailed 02/13/2009, 26 pgs.	
	C57	International Preliminary Report on Patentability for International Patent Application No. PCT/US03/032268 completed 1/4/2005, 3 pgs.	
	C58	International Preliminary Report on Patentability for International Patent Application No. PCT/US03/032912 completed 06/28/2004, 3 pgs.	
	C59	International Preliminary Report on Patentability (Ch. I) of the International Searching Authority for International Patent Application No. PCT/US04/029249 issued 02/21/2006, 6 pgs.	
	C60	Office Action for U.S. Patent Application No. 11/076,719, mailed 03/17/2009, 8 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	7	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C61	Office Action for U.S. Patent Application No. 10/922,041, mailed 12/06/2005, 10 pgs.	
	C62	Office Action for U.S. Patent Application No. 10/922,041, mailed 03/30/2006, 18 pgs.	
	C63	Office Action for U.S. Patent Application No. 10/922,041, mailed 08/11/2006, 19 pgs.	
	C64	Office Action for U.S. Patent Application No. 10/922,041, mailed 01/30/2007, 20 pgs.	
	C65	Office Action for U.S. Patent Application No. 10/683,317, mailed 04/05/2007, 6 pgs.	
	C66	Office Action for U.S. Patent Application No. 10/687,002, mailed 05/02/2007, 10 pgs.	
	C67	Office Action for U.S. Patent Application No. 10/922,041, mailed 05/08/2009, 13 pgs.	
	C68	Office Action for U.S. Patent Application No. 11/076,672, mailed 07/21/2009, 11 pgs.	
	C69	Notice of Allowability for U.S. Patent Application No. 11/076,646, mailed 07/24/2009, 7 pgs.	
	C70	CRANDELL ET AL., "A Secure and Transparent Firewall Web Proxy," October 2003, USENIX, Retrieved from the internet on 7/15/09: <URL: http://www.usenix.org/event/lisa03/tech/full_papers/crandell/crandell.pdf>	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 8 of 11

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
	C71	SOMMERLAD, "Reverse Proxy Patterns," 2003 Retrieved from the Internet on 7/15/09, 27 pages; <URL: http://www.modsecurity.org/archive/ReverseProxy-book-1.pdf>	
	C72	Office Action for U.S. Patent Application No. 11/076,591, mailed 08/06/2009, 29 pgs.	
	C73	Office Action for U.S. Patent Application No. 10/683,317, mailed 08/18/2009, 17 pgs.	
	C74	RASHTI et al, "A Multi-Dimensional Packet Classifier for NP-Based Firewalls," Proceedings of the 2004 Int'l Symposium on Applications and the Internet, January 2004, 5 pages, from the internet, printed 08/12/2009: <URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1266123&isnumber=28312>.	
	C75	WILLIAMSON, Matthew, "Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code," Proceedings of the 18th Annual Computer Security Applications Conference, 2002 IEEE, 8 pages.	
	C76	WILLIAMSON, et al, "Virus Throttling," Virus Bulletin Research Feature 1, March 2003, 4 pgs.	
	C77	Office Action for U.S. Patent Application No. 11/076,672, mailed 01/07/2010, 9 pgs.	
	C78	Office Action for U.S. Patent Application No. 11/076,591, mailed 02/02/2010, 34 pgs.	
	C80	Office Action for U.S. Patent Application No. 11/076,591, mailed 07/20/2010, 33 pgs.	
	C81	Office Action for U.S. Patent Application No. 10/683,317, mailed 07/23/2010, 9 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	9	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C82	Office Action for U.S. Patent Application No. 12/506,140, mailed 09/01/2010, 11 pgs.	
	C90	"Discussion of Conceptual Difference Between Cisco IOS Classic and Zone-Based Firewalls," October 2007, Cisco Systems, Inc., San Jose, CA, 4 pgs.	
	C91	Cisco IOS Firewall Zone-Based Policy Firewall, Release 12.4(6)T, Technical Discussion, February 2006, 77 pgs., Cisco Systems, Inc., San Jose, CA.	
	C92	Zone-Based Policy Firewall Design and Application Guide, Document ID: 98628, 09/13/2007, 49 pgs., Cisco Systems, Inc., San Jose, CA	
	C93	SP MAJ, W MAKAIRANONDH, D VEAL, "An Evaluation of Firewall Configuration Methods," IJSCSNS International Journal of Computer Science and Network Security, Vol. 10, No. 8, August 2010, 7 pgs.	
	C94	Using VPN with Zone-Based Policy Firewall, May 2009, Cisco Systems, Inc., San Jose, CA, 10 pgs.	
	C95	Cisco IOS Firewall Classic and Zone-Based Virtual Firewall Application Configuration Example, Document ID: 100595, February 12, 2008, 20 pgs., Cisco Systems, Inc., San Jose, CA.	
	C96	Class-Based Policy Provisioning: Introducing Class-Based Policy Language (CPL), August 2008, 36 pgs., Cisco Systems, Inc., San Jose, CA.	
	C97	Cisco IOS Zone Based Firewall Example, at http://www.linickx.com/archives/2945/cisco-ios-zon..., printed 12/07/2010, 6 pgs., LINICKX.com.	
	C98	Zone-Based Policy Firewall, Published 02/22/2006, Updated 06/19/2006, 46 pgs., Cisco Systems, Inc., San Jose, CA.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	10	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C99	Applying Zone-based Firewall Policies in Cisco Security Manager, Published March 2009, Revised September 2009, Cisco Systems, Inc., San Jose, CA.	
	C100	"FreeBSD Handbook, Chapter 30 Firewalls," 2003, found at www.freebsd.org/doc/handbook/firewalls-ipfw.html, printed 12/27/2010, 13 pgs.	
	C101	WATTERS, Paul, "Solaris 8 Administrator's Guide, Chapter 4, Network Configuration," O'Reilly & Associates, Inc., January 2002, 17 pgs.	
	C102	SPITZNER, Lance, "Configuring network interface cards; getting your interfaces to talk," March 23, 2004, 4 pgs.	
	C103	GITE, Vivek, "Redhat/CentOS/Fedora Linux Open Port," September 13, 2007, found at www.cyberciti.biz/faq/howto-rhel-linux-open-port-using-iptables/ printed 01/03/2011, 7 pgs.	
	C105	Office Action for U.S. Patent Application No. 10/683,317, mailed 01/03/2011, 12 pgs.	
	C106	Office Action for U.S. Patent Application No. 12/617,211, mailed 02/03/2011, 14 pgs.	
	C107	"Managing Firewall Services," User Guide for Cisco Security Manager 3.3.1, October 2009, Ch. 11, 90 pgs., Cisco Systems, Inc., San Jose, CA.	
	C108	"Cisco Common Classification Policy Language," Cisco Router and Security Device Manager 2.4 User's Guide, Ch. 34, 2007, 32 pgs., Cisco Systems, Inc., San Jose, CA.	
	C109	Guide to User Documentation for Cisco Security Manager 4.0, June 18, 2010, Cisco Systems, Inc., San Jose, CA.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2431
				Examiner Name	Not Yet Assigned
Sheet	11	of	11	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C110	Cisco Configuration Professional: Zone-Based Firewall Blocking Peer to Peer Traffic Configuration Example, Document ID: 112237, Updated 12/03/2010, 25 pgs., Cisco Systems, Inc., San Jose, CA	
	C111	Tuning Cisco IOS Classic and Zone-Based Policy Firewall Denial-of-Service Protection, 2006, 10 pgs., Cisco Systems, Inc., San Jose, CA.	
	C112	HOLUSKA, Marty, Using Ciscos IOS Firewalls to Implement a Network Security Policy, Fort Hays State University/INT 490, printed 12/06/2010, 5 pgs., http://quasarint.com/Capstone/zb_policy.php	
	C113	Cisco Feature Navigator, Cisco Systems, Inc., San Jose, CA, printed on 12/02/2010, 4 pgs., at http://tools.cisco.com/ITDIT/CFN/Dispatch.	
	C114	Office Action for U.S. Patent Application No. 12/506,140, mailed 02/18/2011, 13 pgs.	
	C118	Office Action for U.S. Patent Application No. 12/617,211, mailed 07/19/2011, 18 pgs.	
	C119	Office Action for U.S. Patent Application No. 12/506,140, mailed 08/04/2011, 18 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	Art Unit
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012								
	1	✓								
	2	✓								
	3	✓								
	4	O								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	O								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	O								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	**Art Unit**
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012								
	37	✓								
	38	✓								

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C130	Office Action for U.S. Patent Application No. 12/753,390, mailed 12/08/2011, 19 pgs.	
	C131	Notice of Allowance for U.S. Patent Application No. 12/617,211, mailed 12/12/2011, 8 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered 06/01/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S68	28646	713/153-155;726/11-14,22-24;709/224-225,227,229.ccls. and (@ad<"20050310" or @rlad<"20050310")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 13:00
S69	380	S68 and ((firewall gateway proxy) with (model topology object$1oriented (object adj oriented)) same2 (node object))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 13:00
S70	43	S69 and ((dynamic$4 automatic$4 run$1time (run adj time) anytime (any adj time)) with ((configur$5 re$1configur$5 updat$3 manag$5) near3 (rule polic$3)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 13:00
S71	1029	S68 and ((firewall gateway proxy) with (block$3 preventing drop$4) with (packet connection))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 13:25
S72	40	S71 and ((dynamic$4 automatic$4 run$1time (run adj time) anytime (any adj time)) with ((configur$5 re$1configur$5 updat$3 manag$5) near3 (rule polic$3)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 13:25
S73	40	S71 and ((dynamic$4 automatic$4 run$1time (run adj time) anytime (any adj time)) with ((configur$5 re$1configur$5 updat$3 manag$5) near3 (rule polic$3)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 14:35
S74	161	firewall same ((dynamic$4 run$1time (run adj time) real$1time (real adj time) anytime (any adj time)) with ((configur$5 re$1configur$5 updat$3 manag$5) near3 (rule polic$3)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 14:35
S75	76	S74 and (@ad<"20050310" or @rlad<"20050310")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 14:35
S76	74	S75 not S73	US-PGPUB; USPAT;	OR	ON	2012/06/03 14:35

			USOCR; EPO; JPO; DERWENT; IBM_TDB			
S77	28646	713/153-155;726/11-14,22-24;709/224-225,227,229.ccls. and (@ad<"20050310" or @rlad<"20050310")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/06/03 16:48
S78	128	S77 and (firewall same (packet with (rewrit$4 modif$7 pre$1process$3)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/06/03 16:53

EAST Search History (Interference)

<This search history is empty>

6/3/2012 8:09:59 PM
C:\Users\mdinh\Documents\EAST\Workspaces\13092488 Firewall Modeling.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	Art Unit
	MINH DINH	2432

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
713/153-155; 726/11-14,22-24; 709/224-225,227,229 (text search only for all - see search history printout)	06/03/12	MD
Inventor Name Search	06/03/12	MD

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	229	US 7216173	05-08-2007	Clayton et al.	
	230	US 20020165949	11-07-2002	Na et al.	
	231	US 20030069955	04-10-2003	Gieseke et al.	
	232	US 6643260	11-04-2003	Kloth et al.	
	233	US 6789118	09-07-2004	Rao	
	234	US 6798746	09-28-2004	Kloth et al.	
	235	US 6816903	11-09-2004	Rakoshitz et al.	
	236	US 6876668	04-05-2005	Chawla et al.	
	237	US 6976089	12-13-2005	Na et al.	
	238	US 7185073	02-27-2007	Gai et al.	
	239	US 7257833	08-14-2007	Parekh et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	05/29/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

(Substitute Form PTO/SB/08b)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2431
Examiner Name	Not Yet Assigned
Atty Docket Number	ROCK1150-3

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C83	Office Action for U.S. Patent Application No. 12/579,566, mailed 10/06/2010, 7 pgs.	
	C115	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 03/23/2011, 12 pgs.	
	C116	Notice of Allowance for U.S. Patent Application No. 12/579,566, mailed 05/13/2011, 8 pgs.	
	C117	Office Action for U.S. Patent Application No. 10/683,317, mailed 06/08/2011, 15 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered 05/29/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Attorney Docket Number	ROCK1150-3

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	254	US 8224983	07-17-2012	Ta et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature		Date Considered	

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C140	Office Action for U.S. Patent Application No. 13/173,764, mailed 07/17/2012, 15 pgs.	

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	13333438
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Katharina W. Schuster/Delia Narvaiz
Filer Authorized By:	Katharina W. Schuster
Attorney Docket Number:	ROCK1150-3
Receipt Date:	25-JUL-2012
Filing Date:	22-APR-2011
Time Stamp:	11:35:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ROCK1150-3_IDS_072512.pdf	164773 882963fe9531cb6490721b1c35f9ecedda5da6aa	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	5	
Warnings:					
Information:					
2	Non Patent Literature	ROCK_Ref_C140.pdf	497099 d92fda339377509d414d889ff777beb3f0823a14	no	15
Warnings:					
Information:					
		Total Files Size (in bytes):	661872		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Atty. Docket No. (Opt.) **ROCK1150-3**

Applicant **Patrick Turley**	
Application Number **13/092,488**	Filing or 371 (c) Date: **April 22, 2011**
For **DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME**	
Group Art Unit **2432**	Examiner **DINH, Minh**
Confirmation Number: **6667**	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certification of Transmission Under 37 C.F.R. 1.8

I hereby certify that this correspondence is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 via the U.S. Patent and Trademark Office Electronic Filing System (EFS-Web) on July 25, 2012.

Delia Narvaiz

Dear Sir,

Applicant respectfully requests, pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, that the information listed on the attached SB08A/B form(s) be considered and cited in the examination of the above-identified application. A copy of U.S. Patent(s) and U.S. Patent Application Publication(s) listed on the attached SB08A form is not being submitted with this Information Disclosure Statement pursuant to the waiver of 37 C.F.R. § 1.98(a)(2)(i) by the U.S. Patent and Trademark Office. Where applicable, a copy of foreign patent document(s) as well as information listed on the attached SB08B form is enclosed for the convenience of the Examiner.

☐ This Information Disclosure Statement is being submitted within three months of the filing date of a national application other than a continued prosecution application under 37 C.F.R. § 1.53(d).

☐ This Information Disclosure Statement is being submitted within three months of the date of entry of the national stage as set forth in 37 C.F.R. § 1.491 in an international application;

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action on the merits; or

☐ This Information Disclosure Statement is being submitted before the mailing of a First Office Action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

☒ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(b) and before the mailing date of any of a Final Action under 37 C.F.R. § 1.113, a Notice of Allowance under 37 C.F.R. § 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

- ☒ The statement specified in 37 C.F.R. § 1.97(e); or
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

☐ This Information Disclosure Statement is being submitted after the period specified in 37 C.F.R. § 1.97(c) and on or before payment of the issue fee and is accompanied by:

- ☐ The statement specified in 37 C.F.R. § 1.97(e); and
- ☐ The fee set forth in 37 C.F.R. § 1.17(p). Applicant hereby authorizes the Commissioner to deduct the amount of $180 from Deposit Account No. 50-3183 of Sprinkle IP Law Group for the filing fee of this Information Disclosure Statement.

Pursuant to 37 C.F.R. § 1.97(e), Applicant hereby states:

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of the information disclosure statement.

Applicant respectfully submits that the claims of Applicant's above-referenced patent application are patentably distinguishable from the listed information. Furthermore, pursuant to 37 C.F.R. §§ 1.97(g) and (h), no representation is made that a search has been made or that this information is material to patentability of the present application.

Applicant does not believe any fees are due and owing at this time. If Applicant is in error, the Director is hereby authorized to deduct any and all appropriate fees from Deposit Account 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

SPRINKLE IP LAW GROUP
Attorneys for Applicant

Katharina W. Schuster
Reg. No. 50,000

Dated: July 24, 2012

1301 W. 25th Street, Suite 408
Austin, Texas 78705
Tel. (512) 637-9220
Fax. (512) 317-9088

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	13/092,488
Filing Date	2011-04-22
First Named Inventor	TURLEY, PATRICK
Title	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND
Art Unit	2432
Examiner Name	DINH, MINH
Attorney Docket Number	RPXC-31413

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: **25883**

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☐ Applicant/Inventor.

OR

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____.

SIGNATURE of Applicant or Assignee of Record

Signature	/P.M.S/	Date	8/14/12
Name	PAUL M. SARACENI	Telephone	(415) 728-9245
Title and Company	CHIEF IP OFFICER, RPX CORPORATION		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: RPX CORPORATION

Application No./Patent No.: 13/092,488 Filed/Issue Date: 2011-04-22

Titled: DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

RPX CORPORATION , a CORPORATION
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Turley, Patrick To: White, Eric
The document was recorded in the United States Patent and Trademark Office at
Reel 026340, Frame 0542, or for which a copy thereof is attached.

2. From: White, Eric To: ROCKSTEADY TECHNOLOGIES, LLC
The document was recorded in the United States Patent and Trademark Office at
Reel 026340, Frame 0537, or for which a copy thereof is attached.

3. From: White, Eric To: ROCKSTEADY TECHNOLOGIES, LLC
The document was recorded in the United States Patent and Trademark Office at
Reel 028457, Frame 0012, or for which a copy thereof is attached.

☒ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

PAUL M. SARACENI 8/14/12
Signature Date

PAUL M. SARACENI CHIEF IP OFFICER
Printed or Typed Name Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(b)

SUPPLEMENTAL SHEET

U.S. Patent App. No.: 13/092,488
Filed: April 22, 2011
Atty. Dkt. No.: RPXC-31413

4. From: ROCKSTEADY TECHNOLOGIES, LLC

To: RPX CORPORATION

The document was recorded in the United States Patent and Trademark Office at Reel 028774 Frame 0036, or for which a copy thereof is attached.

Electronic Acknowledgement Receipt

EFS ID:	13546304
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	44654
Filer:	Gregory Michael Howison
Filer Authorized By:	
Attorney Docket Number:	ROCK1150-3
Receipt Date:	21-AUG-2012
Filing Date:	22-APR-2011
Time Stamp:	15:04:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	RPX31413poa.pdf	165510 300641b60d4e32c1805b13b26256ad31b009f640	no	1

Warnings:	
Information:	

2	Assignee showing of ownership per 37 CFR 3.73(b).	RPX31413373.pdf	196348 fd47576242d19e97e9c2b821702d08f9e23c4389	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	361858

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/092,488	04/22/2011	Patrick Turley	ROCK1150-3

CONFIRMATION NO. 6667

POWER OF ATTORNEY NOTICE

44654
Sprinkle IP Law Group
1301 W. 25th Street
Suite 408
Austin, TX 78705

OC000000056192797

Date Mailed: 08/29/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/21/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/092,488	04/22/2011	Patrick Turley	RPXC-31413

CONFIRMATION NO. 6667

25883
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

POA ACCEPTANCE LETTER

OC00000056192818

Date Mailed: 08/29/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/21/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	TURLEY, Patrick
Serial No.:	13/092,488
Confirmation No.:	6667
Filed:	April 22, 2011
Group:	2432
Examiner:	DINH, Minh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AND RESPONSE TO OFFICE ACTION

This communication is responsive to the Examiner's Office Action dated June 11, 2012. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:

defining at least one node, wherein the at least one node is associated with two or more network interfaces;

associating a set of firewall rules with the at least one node;

receiving a packet at a first node of the at least one node; and

accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

2. (Currently Amended) A method according to claim 1, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.

3. (Currently Amended) A method according to claim 2, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.

4. (Original) A method according to claim 1, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

5. (Original) A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.

6. (Original) A method according to claim 5, wherein the at least one node further comprises a second node, further comprising associating a second subset of the set of firewall rules with the second node.

7. (Original) A method according to claim 6, wherein the first subset of firewall rules is same as or at least partially different from the second subset of firewall rules.

8. (Original) A method according to claim 6, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.

9. (Original) A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.

10. (Original) A method according to claim 9, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

11. (Original) A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.

12. (Original) A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.

13. (Currently Amended) A device for controlling data through a firewall, comprising:

a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices;

a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction; and

a data controlling computer program comprising data controlling computer program code

stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:

define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces; and

when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules.

14. (Currently Amended) A device according to claim 13, wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.

15. (Original) A device according to claim 14, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

16. (Currently Amended) A device according to claim 13, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction.

17. (Original) A device according to claim 13, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

18. (Original) A device according to claim 17, wherein the at least one node further comprises a second node, and wherein the data controlling computer program code is further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

19. (Original) A device according to claim 18, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

20. (Original) A device according to claim 18, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

21. (Original) A device according to claim 13, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.

22. (Original) A device according to claim 21, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

23. (Original) A device according to claim 13, wherein each of the at least one node is associated with at least two network interfaces.

24. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is connected with at least one physical device.

25. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and

wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces.

26. (Currently Amended) A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:

define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;

associate a set of firewall rules with the at least one node;

receive a packet at a first node of the at least one node; and

accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

27. (Currently Amended) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction.

28. (Original) A data controlling computer program product according to claim 27, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

29. (Currently Amended) A data controlling computer program product according to claim 27, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction.

30. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

31. (Original) A data controlling computer program product according to claim 30, wherein the at least one node further comprises a second node, and wherein the computer instructions are further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

32. (Original) A data controlling computer program product according to claim 31, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

33. (Original) A data controlling computer program product according to claim 31, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

34. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.

35. (Original) A data controlling computer program product according to claim 34, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

36. (Original) A data controlling computer program product according to claim 26, wherein each of the at least one node comprises at least two network interfaces.

37. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is connected with at least one physical device.

38. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is physically connected to every other network

interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.

REMARKS

In response to the Office Action dated June 11, 2012, the Applicant has amended Claims 1-3, 13-14, 16, 26-37 and 29. Thus, Claims 1-38 remain pending in the application. Reconsideration of the claims, as amended, is respectfully requested.

Claims 6-8, 18-20 and 31-33 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter Applicant regards as the invention. More particularly, the Official Action referenced the language, "wherein the at least one node further comprises a second node, further comprising associating a second subset of the set of firewall rules with the second node." The Official Action states since "the at least one node" can be interpreted as one node, it is not clear how it comprises a second node. For prior art rejection purposes, "the at least one node" is interpreted as being "at least two nodes". Applicant respectfully submits that the Official Action's statement that Claims 6-8, 18-20 and 31-33 should interpret the at least one node as at least two nodes as an accurate interpretation of the limitations of these claims. If the Official Action is stating that the at least one node should be interpreted as at least two nodes for all of the claims, Applicant respectfully disagrees with this statement. In the claims that do not include the additional limitation of the at least one node further comprising a second node, the claim language is clearly indicating that the limitation is at least one node. In the claims referenced by the Official Action including the further limitation of the at least one node further comprising a second node, these claims must be interpreted as the at least one node to comprise at least two nodes. However, Applicant disagrees that this language is indefinite because the further limitation of the second node is not inconsistent with the language of at least one node. An apparatus including a second node comprises at least one node. Therefore, the Applicant respectfully submits that Claims 6-8, 18-20 and 31-33 are not indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention, and Applicant respectfully requests withdrawal of the rejection.

Claims 1-4, 13-16 and 26-29 were rejected on the grounds of nonstatutory obviousness-type double patenting as being unpatentable over Claims 2, 11 and 16 of U.S. Patent No.

8,032,933. A Terminal Disclaimer is submitted concurrently with this response with respect to U.S. Patent No. 8,032,933.

Claims 1-3, 9, 13-15, 21, 26-28 and 34 were rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 7, 14 and 19 of U.S. Patent No. 7,160,621. A Terminal Disclaimer is submitted concurrently with this response with respect to U.S. Patent No. 7,160,621.

Claims 1-3, 5-9, 11-15, 17-21, 23-28, 30-34 and 36-38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bartal et al.* in view of *Qian et al.* Claim 1 includes the limitation of "accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction." Thus, the firewall rules that are accepting or denying packets are dynamically self-configurable during runtime without operator interaction. This is distinctly different from what is described with respect to *Bartal* and *Qian*. The Official Action admits that *Bartal* does not disclose reconfiguring the firewall at runtime. In order to disclose this limitation the Official Action recites the *Qian* reference and more particularly the discussions of Figs. 8 and 10 in paragraphs [0057-0064]. However, a review of this portion of the *Qian* reference clearly indicates that all of the changes, revisions and updates that are made within the firewall are done by the user and are not self-configurable during runtime without operator interaction. As clearly recited in paragraph [0065], "the method shown in Claim 10 permits an advanced user to establish a firewall policy for a computer. The advanced user may set the firewall policies in accordance with filtering needs for the computer 102." Thus, the reference makes clear that the discussion referenced by the Official Action is made by the advanced user and is not a self-configuring operation occurring during runtime.

Additionally, the abstract of the *Qian* reference referenced within the Official Action states, "a user or administrator of a computer may utilize the object model to manage and configure the firewall services." Thus, again, it is made clear that the configuration described with respect to the *Qian* reference is made by a user or a system administrator and is not a dynamically self-configurable during runtime process without operator interaction. Therefore, the Applicant respectfully submits that the combination of *Qian* and *Bartal* do not render

obvious the limitations of Claim 1. A Notice of Allowance for Claim 1, and all claims dependent therefrom, is respectfully requested.

Claim 13 has been amended to include the limitation of:

> a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction; and

The Applicant respectfully submits that Claim 13 is distinguishable from the combination of *Bartal* and *Qian* for reasons similar to those discussed with respect to Claim 1 as the *Qian* reference does not describe firewall rules that are dynamically self-configurable during runtime without operator interaction. A Notice of Allowance is respectfully requested.

Claim 26 includes the limitation of:

> accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

Applicant respectfully submits that this language, similar to that of Claim 1, distinguishes Claim 26, and all claims dependent therefrom, from the combination of *Bartal* and *Qian*. A Notice of Allowance is respectfully requested.

Claims 10, 22 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bartal* in view of *Qian* and further in view of *Aroya*. Applicant respectfully submits that these claims, being dependent upon Claims 1, 13 and 26, respectively, are allowable for similar reasons as the *Aroya* reference fails to overcome the shortcomings of *Bartal* and *Qian*. A Notice of Allowance is respectfully requested.

Applicant thanks the Examiner for the indication of allowable subject matter for Claims 4, 16 and 29.

In view of the foregoing amendments and comments, the Applicant respectfully submits that all pending claims are distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/RPXC-31413 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicant(s)

/Brian D. Walker Reg. #37751/
Brian D. Walker
Registration No. 37,751

BDW/mep

P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
September 7, 2012

Electronic Acknowledgement Receipt

EFS ID:	13686084
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	25883
Filer:	Brian D. Walker
Filer Authorized By:	
Attorney Docket Number:	RPXC-31413
Receipt Date:	07-SEP-2012
Filing Date:	22-APR-2011
Time Stamp:	18:12:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RPX31413AMDTerminalDisclaimer.pdf	102225 4b6ad65add28e2ca037fca6ee2951ee112de8eeb	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	12
Warnings:			
Information:			
	Total Files Size (in bytes):	102225	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	13092488
Filing Date	22-Apr-2011
First Named Inventor	Patrick Turley
Attorney Docket Number	RPXC-31413
Title of Invention	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
RPX CORPORATION	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8032933

7160621

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

- (●) Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.
- ( ) I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

- ( ) Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ( ) Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).
- (●) Applicant(s) status remains as SMALL ENTITY.
- ( ) Applicant(s) status remains as other than SMALL ENTITY.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- (●) An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

  Registration Number 37751

- ( ) A sole inventor
- ( ) A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors
- ( ) A joint inventor; all of whom are signing this request
- ( ) The assignee of record of the entire interest that has properly made itself of record pursuant to 37 CFR 3.71

Signature	/Brian Walker/
Name	BRIAN D. WALKER

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	13092488
Filing Date:	22-Apr-2011
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Filer:	Brian D. Walker
Attorney Docket Number:	RPXC-31413

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or terminal disclaimer	2814	1	80	80
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**80**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13092488

Filing Date: 22-Apr-2011

Applicant/Patent under Reexamination: Turley et al.

Electronic Terminal Disclaimer filed on September 7, 2012

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	13686282
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	25883
Filer:	Brian D. Walker
Filer Authorized By:	
Attorney Docket Number:	RPXC-31413
Receipt Date:	07-SEP-2012
Filing Date:	22-APR-2011
Time Stamp:	18:15:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$80
RAM confirmation Number	6087
Deposit Account	200780
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33986 40caddeca9ccc0b4574dc6449cbd706836208d5d	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30341 0eb75272fc70d1a3049f06cc62aa27d8b0f77aef	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64327		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/092,488	04/22/2011	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	09/07/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 38	Minus	** 38	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $125 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/CHRISTINE V.13390459 MOORE/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

25883 7590 12/03/2012

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
12/03/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@dalpat.com

Office Action Summary	Application No.	Applicant(s)	
	13/092,488	TURLEY ET AL.	
	Examiner	Art Unit	
	MINH DINH	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 September 2012*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-38* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-3,5-15,17-28 and 30-38* is/are rejected.

8)☒ Claim(s) *4,16 and 29* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 April 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed on 09/07/2012. Claims 1-3, 13-14, 16, 26-27 and 29 have been amended.

Terminal Disclaimer

2. The terminal disclaimer filed on 09/07/2012 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Patent Numbers 8,032,933 and 7,160,621 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Arguments

3. Applicant's arguments with respect to the rejection of claims 6-8, 18-20 and 31-33 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention have been fully considered but they are not persuasive. The claim term “the at least one node” clearly includes one node, and, therefore, it is not clear how it comprises a second node.

4. Applicant’s arguments with respect to the rejection of claims 1-3, 5-9, 11-15, 17-21, 23-28, 30-34 and 36-38 under 35 U.S.C. 103(a) have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Claim Rejections - 35 USC § 112

5. The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 6-8, 18-20 and 31-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 recites “wherein the at least one node further comprises a second node, further comprising associating a second subset of the set of firewall rules with the second node.” Since “the at least one node” can be interpreted as one node, it is not clear how it comprises a second node. For prior art rejection purposes, “the at least one node” is interpreted as being “at least two nodes”. Claims 18 and 31 are rejected on the same basis as claim 6.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-3, 5-9, 11-15, 17-21, 23-28, 30-34 and 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartal et al. (US 7,146,639 B2) in view of Danford et al. (US 2004/0236963).

9. Regarding claims 1-3, 9, 11-15, 21, 23-28, 34 and 36-38, Bartal discloses a method and device for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising: defining at least one node, wherein the at least one node is associated with two or more network interfaces (fig. 1; fig. 2, elements 300, 250; fig. 5; fig. 9; col. 6, lines 30-39, 57-67; col. 7, lines 1-9); associating a set of firewall rules with the at least one node (col. 9, lines 27-39); receiving a packet at a first node of the at least one node; and accepting or denying the packet based on the set of firewall rules (col. 1, lines 29-31; col. 9, lines 31-39).

Bartal does not disclose reconfiguring the firewall at runtime without operator interaction. Danford discloses reconfiguring a firewall at runtime without operator interaction (i.e., adding, deleting, modifying a firewall rule based on result of anomaly detection) (Abstract; fig. 1, element 120; fig. 2; paragraphs 0014-0017). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Bartal method to reconfigure the firewall at runtime without operator interaction, as taught by Danford. The motivation for doing so would have been to defend against malicious network traffic with minimized false positives and false negatives.

10. Regarding claims 5-8, 17-20 and 30-33, Bartal further discloses associating a first subset of the set of firewall rules with the first node and associating a second subset of the set of firewall rules with the second node (col. 11, lines 40-50).

11. Claims 10, 22 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartal in view of Danford as applied to claims 9, 21 and 34 above, and further in

view of Aroya (US 7,634,805). Bartal and Danford do not disclose rewriting a portion of a network packet header associated with the packet. Aroya discloses a method for controlling a data packet through a firewall including rewriting a portion of a network packet header associated with the packet (fig. 2; col. 4, line 45 – col. 5, line 13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Bartal and Danford to rewrite a portion of a network packet header associated with the packet, as taught by Aroya. The motivation for doing so would have been to preserve a routing effect.

Allowable Subject Matter

12. Claims 4, 16 and 29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 09:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Minh Dinh/
Primary Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 13/092,488	Applicant(s)/Patent Under Reexamination TURLEY ET AL.	
	Examiner MINH DINH	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,836,496	11-2010	Chesla et al.	726/13
*	B	US-7,540,025	05-2009	Tzadikario, Rephael	726/22
*	C	US-2004/0236963	11-2004	Danford et al.	713/201
*	D	US-2002/0083175	06-2002	Afek et al.	709/225
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Receipt date: 07/25/2012

Substitute Form PTO/SB/08a

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Application Number	13/092,488
Filing Date	April 22, 2011
First Named Inventor	Patrick Turley
Group Art Unit	2432
Examiner Name	DINH, Minh
Attorney Docket Number	ROCK1150-3

Sheet 1 of 1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
	254	US 8224983	07-17-2012	Ta et al.	
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			
		US			

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code *(if known)*	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Minh Dinh/	Date Considered	11/27/2012

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

Receipt date: 07/25/2012

Substitute Form PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/092,488
				Filing Date	April 22, 2011
				First Named Inventor	Patrick Turley
				Group Art Unit	2432
				Examiner Name	DINH, Minh
Sheet	1	of	1	Atty Docket Number	ROCK1150-3

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.) date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	C140	Office Action for U.S. Patent Application No. 13/173,764, mailed 07/17/2012, 15 pgs.	

Examiner Signature	/Minh Dinh/	Date Considered	11/27/2012	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /MD/

EOR IN IPR2013-00240 EX1102 Page 040

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	Art Unit
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012	11/27/2012							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	O	O							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	O	O							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							
	26	✓	✓							
	27	✓	✓							
	28	✓	✓							
	29	O	O							
	30	✓	✓							
	31	✓	✓							
	32	✓	✓							
	33	✓	✓							
	34	✓	✓							
	35	✓	✓							
	36	✓	✓							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	**Art Unit**
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012	11/27/2012							
	37	✓	✓							
	38	✓	✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S80	29326	713/153-155;726/11-14,22-24;709/224-225,227,229.ccls. and (@ad<"20050310" or @rlad<"20050310")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/11/27 20:06
S81	1156	S80 and (firewall same (ids (intrusion adj detection)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/11/27 20:07
S82	180	S81 and ((dynamic$4 adapt$5) with (block$3 filter$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/11/27 20:09
S83	24	S81 and ((dynamic$4 adapt$5) with (block$3 filter$3) same (malicious anomal$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/11/27 20:10

EAST Search History (Interference)

<This search history is empty>

11/27/2012 9:54:14 PM
C:\Users\mdinh\Documents\EAST\Workspaces\13092488 Firewall Modeling.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	Art Unit
	MINH DINH	2432

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
713/153-155; 726/11-14,22-24; 709/224-225,227,229 (text search only for all - see search history printout)	06/03/12	MD
Inventor Name Search	06/03/12	MD
713/153-155; 726/11-14,22-24; 709/224-225,227,229 (text search only for all - see search history printout)	11/27/12	MD
Inventor Name Search	11/27/12	MD

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	TURLEY, Patrick
Serial No.:	13/092,488
Confirmation No.:	6667
Filed:	April 22, 2011
Group:	2432
Examiner:	DINH, Minh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AFTER FINAL

This communication is responsive to the Examiner's Office Action dated December 3, 2012. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:

defining at least one node, wherein the at least one node is associated with two or more network interfaces;

associating a set of firewall rules with the at least one node;

receiving a packet at a first node of the at least one node; and

accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.

2. (Cancelled)

3. (Previously Presented) A method according to claim 2, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.

4. (Original) A method according to claim 1, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

5. (Original) A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.

6. (Currently Amended) A method according to claim 5, wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node.

7. (Original) A method according to claim 6, wherein the first subset of firewall rules is same as or at least partially different from the second subset of firewall rules.

8. (Original) A method according to claim 6, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.

9. (Original) A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.

10. (Original) A method according to claim 9, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

11. (Original) A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.

12. (Original) A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.

13. (Currently Amended) A device for controlling data through a firewall, comprising:

a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices;

a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction; and

a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:

define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces; [[and]]

when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules[[.]]; and

wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.

14. (Cancelled)

15. (Original) A device according to claim 14, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

16. (Previously Presented) A device according to claim 13, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction.

17. (Original) A device according to claim 13, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

18. (Currently Amended) A device according to claim 17, wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

19. (Original) A device according to claim 18, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

20. (Original) A device according to claim 18, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

21. (Original) A device according to claim 13, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.

22. (Original) A device according to claim 21, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

23. (Original) A device according to claim 13, wherein each of the at least one node is associated with at least two network interfaces.

24. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is connected with at least one physical device.

25. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and

wherein physical connection between the plurality of network interfaces comprises indirect

physical connection between the plurality of network interfaces.

26. (Currently Amended) A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:

define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;

associate a set of firewall rules with the at least one node, wherein the set of firewall rules further comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction;

receive a packet at a first node of the at least one node; and

accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

27. (Previously Presented A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction.

28. (Original) A data controlling computer program product according to claim 27, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

29. (Cancelled)

30. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

31. (Currently Amended) A data controlling computer program product according to claim 30, wherein the at least one node further comprises at least two nodes including a second node, and wherein the computer instructions are further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

32. (Original) A data controlling computer program product according to claim 31, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

33. (Original) A data controlling computer program product according to claim 31, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

34. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.

35. (Original) A data controlling computer program product according to claim 34, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

36. (Original) A data controlling computer program product according to claim 26, wherein each of the at least one node comprises at least two network interfaces.

37. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is connected with at least one physical device.

38. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is physically connected to every other network

interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.

REMARKS

In response to the Office Action dated December 3, 2012, the Applicant has amended Claims 1, 6, 13, 18, 26 and 31 and cancelled Claims 2, 14 and 29. Thus, Claims 1, 3-13, 15-28 and 30-38 remain pending in the application. Reconsideration of the claims, as amended, is respectfully requested.

Claims 6-8, 18-20, 31-33 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter, which Applicant regards as the invention. Applicant has amended the claims, where necessary, to more particularly point out and distinctly claim the subject matter of the invention. Withdrawal of the rejection is respectfully requested.

Claims 1-3, 5-9, 11-15, 17-21, 23-28, 30-34 and 36 and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bartal* in view of *Danford*. With respect to Claim 1, Applicant has rolled the previous limitations of Claim 2 into Claim 1. Applicant, in reviewing the previous Office Action, finds no discussion of the limitations of Claim 2 with respect to the cited references. Thus, Claim 1 now more particularly recites the limitation of, "wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction." While the recited *Danford* reference describes setting a period of time for applying a blocking measure to an intrusion within a firewall, nothing with respect to *Danford* describes dynamically updating the set of firewall rules. The rules described with respect to *Danford* remain constant. The blocking measures are applied and not applied in accordance with the flow chart structure described within the *Danford* reference. Therefore, Applicant respectfully submits that Claim 1, as amended, is distinguished from the combination of *Bartal* and *Danford*. Thus, Applicant respectfully submits that Claim 1, and all claims dependent therefrom, are distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Claim 13 has been amended to more particularly include the limitation of, "wherein the data controlling computer code is further executable to dynamically update the set of firewall rules during runtime without operator interaction." As previously discussed with respect to Claim 1, the dynamic updating of the set of firewall rules is not described with respect to the

Danford reference and Applicant finds no discussion of this limitation within the previous Office Action. Therefore, the Applicant respectfully submits that Claim 13, as amended, is distinguishable from the art of record, and a Notice of Allowance is respectfully requested.

Claim 26, has been amended to include the previous limitations of Claim 29. In view of the indication of allowable subject matter for Claim 29, Applicant respectfully submits that Claim 26, as amended, is distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Claims 10, 22 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Bartal* in view of *Danford* and further in view of *Aroya*. Applicant respectfully submits that these claims, being dependent upon Claims 1, 13 and 26, respectively, are allowable for similar reasons as the *Aroya* reference fails to overcome the shortcomings of *Bartal* and *Danford*. A Notice of Allowance is respectfully requested.

In view of the foregoing amendments and comments, the Applicant respectfully submits that all pending claims are distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/RPXC-31413 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicant(s)

/Brian D. Walker Reg. #37751/
Brian D. Walker
Registration No. 37,751

BDW/mep
P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
December 4, 2012

Electronic Acknowledgement Receipt

EFS ID:	14382032
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	25883
Filer:	Brian D. Walker
Filer Authorized By:	
Attorney Docket Number:	RPXC-31413
Receipt Date:	06-DEC-2012
Filing Date:	22-APR-2011
Time Stamp:	12:35:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RPX31413AMDAF.pdf	106416 fbb8aee7da26daaca75fa2bcb6b57883b67c6ce2	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	10
Warnings:			
Information:			
	Total Files Size (in bytes):	106416	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/092,488	04/22/2011	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 12/06/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 35	Minus	** 38	= 0	X $31 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/VIOLA ROGERS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

25883 7590 12/28/2012

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
12/28/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@dalpat.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/092,488	**Applicant(s)** TURLEY ET AL.
	Examiner MINH DINH	**Art Unit** 2432

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 06 December 2012 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance;

   (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.

   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☐ will not be entered, or (b) ☒ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:

    _____.

12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

STATUS OF CLAIMS

14. The status of the claim(s) is (or will be) as follows:

    Claim(s) allowed: 26-28 and 30-38.
    Claim(s) objected to: .
    Claim(s) rejected: 1,3-13 and 15-25.
    Claim(s) withdrawn from consideration: .

/Minh Dinh/
Primary Examiner, Art Unit 2432

Applicant argues that while Danford (2004/0236963) describes setting a period of time for applying a blocking measure to an intrusion, Danford does not describe dynamically updating the firewall rules (Remarks, page 9, third paragraph). Danford discloses that when an anomaly is detected, a firewall rule (i.e., a blocking measure is to be interpreted as enforcement of a defensive rule for discarding traffice from a particular source address to a particular destination address) is enforced for a duration of time. Danford further discloses that the duration of time can be extended if the anomaly is still evident (par. 0007-0008, 0015).

OK TO ENTER: /MD/

12/14/2012

RPXC-31413 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	TURLEY, Patrick
Serial No.:	13/092,488
Confirmation No.:	6667
Filed:	April 22, 2011
Group:	2432
Examiner:	DINH, Minh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AFTER FINAL

This communication is responsive to the Examiner's Office Action dated December 3, 2012. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	TURLEY, Patrick
Serial No.:	13/092,488
Confirmation No.:	6667
Filed:	April 22, 2011
Group:	2432
Examiner:	DINH, Minh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AFTER FINAL

This communication is responsive to the Examiner's Office Action dated December 3, 2012, and the Advisory Action of December 28, 2012. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:

defining at least one node, wherein the at least one node is associated with two or more network interfaces;

associating a set of firewall rules with the at least one node;

receiving a packet at a first node of the at least one node; and

accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, ~~wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.~~ wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

2. (Cancelled)

3. (Previously Presented) A method according to claim 2, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.

4. (Cancelled)

5. (Original) A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.

6. (Previously Presented) A method according to claim 5, wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node.

7. (Original) A method according to claim 6, wherein the first subset of firewall rules is same as or at least partially different from the second subset of firewall rules.

8. (Original) A method according to claim 6, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.

9. (Original) A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.

10. (Original) A method according to claim 9, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

11. (Original) A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.

12. (Original) A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.

13. (Currently Amended) A device for controlling data through a firewall, comprising:

a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices;

a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction; [[and]]

a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:

define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces; and

when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules~~; and~~.

~~wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.~~

14. (Cancelled)

15. (Original) A device according to claim 14, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

16. (Cancelled)

17. (Original) A device according to claim 13, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

18. (Previously Presented) A device according to claim 17, wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

19. (Original) A device according to claim 18, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

20. (Original) A device according to claim 18, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

21. (Original) A device according to claim 13, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.

22. (Original) A device according to claim 21, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

23. (Original) A device according to claim 13, wherein each of the at least one node is associated with at least two network interfaces.

24. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is connected with at least one physical device.

25. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and

wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces.

26. (Previously Presented) A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:

define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;

associate a set of firewall rules with the at least one node, wherein the set of firewall rules further comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction;

receive a packet at a first node of the at least one node; and

accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

27. (Previously Presented A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction.

28. (Original) A data controlling computer program product according to claim 27, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

29. (Cancelled)

30. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

31. (Previously Presented) A data controlling computer program product according to claim 30, wherein the at least one node further comprises at least two nodes including a second node, and wherein the computer instructions are further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

32. (Original) A data controlling computer program product according to claim 31, wherein the first subset of the set of firewall rules is same as or different from the second subset of the set of firewall rules.

33. (Original) A data controlling computer program product according to claim 31, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

34. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.

35. (Original) A data controlling computer program product according to claim 34, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

36. (Original) A data controlling computer program product according to claim 26, wherein each of the at least one node comprises at least two network interfaces.

37. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is connected with at least one physical device.

38. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is physically connected to every other network interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.

39. (New) A method according to claim 1, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.

40. (New) A device according to claim 13, wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.

REMARKS

In response to the Office Action dated December 3, 2012, and the Advisory Action of December 28, 2012, the Applicant has amended Claims 1 and 13 to include the previous subject matter of Claims 4 and 16 as referenced in the December 3 Office Action. In view of the indication of allowable subject matter for Claims 4 and 16, Applicant respectfully submits that Claims 1 and 13, as amended, are now in condition for allowance. A Notice of Allowance for these claims, and all claims dependent therefrom, is respectfully requested. Applicant thanks the Examiner for the indication of allowable subject matter in Claims 26-28 and 30-38.

In view of the foregoing amendments and comments, the Applicant respectfully submits that all pending claims are distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/RPXC-31413 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicant(s)

/Brian D. Walker Reg. #37751/
Brian D. Walker
Registration No. 37,751

BDW/mep

P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
January 3, 2013

Electronic Acknowledgement Receipt

EFS ID:	14609069
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	25883
Filer:	Brian D. Walker
Filer Authorized By:	
Attorney Docket Number:	RPXC-31413
Receipt Date:	03-JAN-2013
Filing Date:	22-APR-2011
Time Stamp:	16:31:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RPX31413AMDAfterAdvisory.pdf	87708 917aa9ad62ede7168cfc0150281affba3b9611cf	yes	9

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment After Final	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	9
Warnings:			
Information:			
	Total Files Size (in bytes):	87708	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REMARKS

In response to the Office Action dated December 3, 2012, and the Advisory Action of December 28, 2012, the Applicant has amended Claims 1 and 13 to include the previous subject matter of Claims 4 and 16 as referenced in the December 3 Office Action. In view of the indication of allowable subject matter for Claims 4 and 16, Applicant respectfully submits that Claims 1 and 13, as amended, are now in condition for allowance. A Notice of Allowance for these claims, and all claims dependent therefrom, is respectfully requested. Applicant thanks the Examiner for the indication of allowable subject matter in Claims 26-28 and 30-38.

In view of the foregoing amendments and comments, the Applicant respectfully submits that all pending claims are distinguishable from the art of record and a Notice of Allowance is respectfully requested.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/RPXC-31413 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicant(s)

/Brian D. Walker Reg. #37751/
Brian D. Walker
Registration No. 37,751

BDW/mep

P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
January 3, 2013

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/092,488	04/22/2011	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/03/2013	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 35	Minus	** 38	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/PEGGY YARBOROUGH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

25883 7590 01/15/2013
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DINH, MINH	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 01/15/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

TITLE OF INVENTION: DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$885	$300	$0	$1185	04/15/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

25883 7590 01/15/2013
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

TITLE OF INVENTION: DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$885	$300	$0	$1185	04/15/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
DINH, MINH	2432	726-013000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

25883 7590 01/15/2013

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 01/15/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	13/092,488	TURLEY ET AL.	
	Examiner	Art Unit	
	MINH DINH	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the after-final amendment filed on 01/03/2013*.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are *1,3,5-13,15,17-28 and 30-40*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/Minh Dinh/
Primary Examiner, Art Unit 2432

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	13/092,488	TURLEY ET AL.	
	Examiner	Art Unit	
	MINH DINH	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *MINH DINH*. (3)_____.

(2) *BRIAN WALKER*. (4)_____.

Date of Interview: *08 January 2013*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *3 and 15*.

Identification of prior art discussed: _____.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Claims 3 and 15 depend upon canceled claims. Mr. Walker authorized Examiner's amendment to correct the issue .

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Minh Dinh/ Primary Examiner, Art Unit 2432	

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brian Walker on 01/08/2013.

The application has been amended as follows:

3. (Currently Amended) A method according to claim [[2]]1, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.

15. (Currently Amended) A device according to claim [[14]]13, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

2. The following is an examiner's statement of reasons for allowance: the prior art fail to teach "wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical

structure comprises defined places for dynamically updating the set of firewall rules during runtime."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 09:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Minh Dinh/
Primary Examiner, Art Unit 2432

OK TO ENTER: /MD/

01/09/2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	TURLEY, Patrick
Serial No.:	13/092,488
Confirmation No.:	6667
Filed:	April 22, 2011
Group:	2432
Examiner:	DINH, Minh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AFTER FINAL

This communication is responsive to the Examiner's Office Action dated December 3, 2012, and the Advisory Action of December 28, 2012. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S84	29438	713/153-155;726/11-14,22-24;709/224-225,227,229.ccls. and (@ad<"20050310" or @rlad<"20050310")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:12
S85	1164	S84 and (firewall same (ids (intrusion adj detection)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:12
S86	24	S85 and ((dynamic$4 adapt$5) with (block$3 filter$3) same (malicious anomal$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:12
S87	3	S85 and (((run adj time) run$1time) with (block$3 filter$3) same (malicious anomal$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:14
S88	0	S86 and (rule with (hierarchical tree graph) same (updat$3 modif$7 add$3 delet$3 remov$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:30
S89	17	S85 and (rule with (hierarchical tree graph) same (updat$3 modif$7 add$3 delet$3 remov$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/07 10:31

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S90	0	(firewall and (node device) and interface and rule and receiv$3 and packet and (accept$3 deny$3) and dynamically and configurable and runtime and chain and path and hierarchical and space and updat$3).clm.	US-PGPUB; UPAD	OR	ON	2013/01/07 11:56

1/9/2013 11:14:20 PM
C:\Users\mdinh\Documents\EAST\Workspaces\13092488 Firewall Modeling.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	**Art Unit**
	MINH DINH	2432

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
713/153-155; 726/11-14,22-24; 709/224-225,227,229 (text search only for all - see search history printout)	06/03/12	MD
Inventor Name Search	06/03/12	MD
713/153-155; 726/11-14,22-24; 709/224-225,227,229 (text search only for all - see search history printout)	11/27/12	MD
Inventor Name Search	11/27/12	MD
Update EAST search	01/07/13	MD
Inventor Name Search	01/07/13	MD

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
	PG-PUB and UPAD text search, see interference search printout	01/07/13	MD

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	**Art Unit**
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012	11/27/2012	01/09/2013						
1	1	✓	✓	=						
	2	✓	✓	-						
2	3	✓	✓	=						
	4	O	O	-						
3	5	✓	✓	=						
4	6	✓	✓	=						
5	7	✓	✓	=						
6	8	✓	✓	=						
7	9	✓	✓	=						
8	10	✓	✓	=						
9	11	✓	✓	=						
10	12	✓	✓	=						
12	13	✓	✓	=						
	14	✓	✓	-						
13	15	✓	✓	=						
	16	O	O	-						
14	17	✓	✓	=						
15	18	✓	✓	=						
16	19	✓	✓	=						
17	20	✓	✓	=						
18	21	✓	✓	=						
19	22	✓	✓	=						
20	23	✓	✓	=						
21	24	✓	✓	=						
22	25	✓	✓	=						
24	26	✓	✓	=						
25	27	✓	✓	=						
26	28	✓	✓	=						
	29	O	O	-						
27	30	✓	✓	=						
28	31	✓	✓	=						
29	32	✓	✓	=						
30	33	✓	✓	=						
31	34	✓	✓	=						
32	35	✓	✓	=						
33	36	✓	✓	=						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13092488	TURLEY ET AL.
	Examiner	**Art Unit**
	MINH DINH	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/03/2012	11/27/2012	01/09/2013						
34	37	✓	✓	=						
35	38	✓	✓	=						
11	39			=						
23	40			=						

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
13092488	TURLEY ET AL.
Examiner	**Art Unit**
MINH DINH	2432

ORIGINAL		INTERNATIONAL CLASSIFICATION														
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED									
726	11	H	0	4	L	29 / 00 (2006.01.01)										

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	14	17	30	33										
	2	15	18	31	34										
2	3	16	19	32	35										
	4	17	20	33	36										
3	5	18	21	34	37										
4	6	19	22	35	38										
5	7	20	23	11	39										
6	8	21	24	23	40										
7	9	22	25												
8	10	24	26												
9	11	25	27												
10	12	26	28												
12	13		29												
	14	27	30												
13	15	28	31												
	16	29	32												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	35	
/MINH DINH/ Primary Examiner.Art Unit 2432	01/09/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

25883 7590 01/15/2013
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

TITLE OF INVENTION: DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$885	$300	$0	$1185	04/15/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
DINH, MINH	2432	726-013000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 HOWISON & ARNOTT,
2 L.L.P.
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: RPX CORPORATION

(B) RESIDENCE: (CITY and STATE OR COUNTRY): SAN FRANCISCO, CALIFORNIA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 200780 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☒ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Timothy F. Bliss Reg. #50925/ Date January 16, 2013

Typed or printed name TIMOTHY F. BLISS Registration No. 50,925

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Patrick Turley
Serial No.:	13/092,488
Filed:	April 22, 2011
Confirmation No.	6667
Notice of Allowance Mailed:	January 15, 2013
Group:	2432
Examiner:	Minh Dinh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT UNDER RULE 312

The above-identified application has been carefully reviewed prior to the payment of the Issue Fee. It is requested that the following amendments be entered under the provisions of Rule 312.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims beginning on page 3 of this paper.

Remarks begin on page 10 of this paper.

In the Specification

Please replace paragraphs [0001] and [0048] with the following amended paragraphs:

[0001] This application is a continuation of~~, and claims a benefit of priority under 35 U.S.C. 120 of the filing date of~~ U.S. patent application Ser. No. 12/579,566, filed Oct. 15, 2009, now ~~allowed~~ U.S. Pat. No. 8,032,933, issued on Oct. 4, 2011, entitled "DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME," which ~~claims priority from~~ is a continuation of U.S. patent application Ser. No. 11/076,719, filed Mar. 10, 2005, issued on Oct. 27, 2009 as U.S. Pat. No. 7,610,621, entitled "SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING," which claims priority from Provisional Application No. 60/551,698, filed Mar. 10, 2004, entitled "SYSTEM AND METHOD FOR BEHAVIOR-BASED FIREWALL MODELING." This application also relates to U.S. patent application Ser. No. 10/683,317, filed Oct. 10, 2003, ~~pending~~ now U.S. Pat. No. 8,117,639, issued on Feb. 14, 2012, entitled "SYSTEM AND METHOD FOR PROVIDING ACCESS CONTROL," and Provisional Application No. 60/551,703, entitled "SYSTEM AND METHOD FOR PROVIDING A CENTRALIZED DESCRIPTION/ CONFIGURATION OF CLIENT DEVICES ON A NETWORK ACCESS GATEWAY," filed Mar. 10, 2004. All applications referenced herein are hereby fully incorporated by reference.

[0048] The arriving (:A) sub-tree (represented at 202) prepares packets to enter the matrix. This is where packets are marked, de-NATed (if Network Address Translation has occurred), ~~de-MAQUERADEd~~ de-MASQUERADEd and redirected. Since the purpose of this sub-tree is packet "conditioning", its rules only change network packets, and do not drop or accept them. Along with the :D sub-tree (see below), these rules implement the behaviors of nodes.

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:

defining at least one node, wherein the at least one node is associated with two or more network interfaces;

associating a set of firewall rules with the at least one node;

receiving a packet at a first node of the at least one node; and

accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.

2. (Cancelled)

3. (Previously Presented) A method according to claim 1, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.

4. (Cancelled)

5. (Original) A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.

6. (Previously Presented) A method according to claim 5, wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node.

7. (Currently Amended) A method according to claim 6, wherein the first subset of firewall rules is the same as or at least partially different from the second subset of firewall rules.

8. (Original) A method according to claim 6, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.

9. (Original) A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.

10. (Original) A method according to claim 9, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

11. (Original) A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.

12. (Original) A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.

13. (Previously Presented) A device for controlling data through a firewall, comprising:

a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices;

a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places

for dynamically updating the set of firewall rules during runtime without operator interaction;

a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:

define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces; and

when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules.

14. (Cancelled)

15. (Original) A device according to claim 13, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

16. (Cancelled)

17. (Original) A device according to claim 13, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

18. (Previously Presented) A device according to claim 17, wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

19. (Currently Amended) A device according to claim 18, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.

20. (Original) A device according to claim 18, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

21. (Original) A device according to claim 13, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.

22. (Original) A device according to claim 21, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

23. (Original) A device according to claim 13, wherein each of the at least one node is associated with at least two network interfaces.

24. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is connected with at least one physical device.

25. (Original) A device according to claim 13, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and

wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces.

26. (Previously Presented) A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:

define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;

associate a set of firewall rules with the at least one node, wherein the set of firewall rules further comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction;

receive a packet at a first node of the at least one node; and

accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.

27. (Previously Presented) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction.

28. (Original) A data controlling computer program product according to claim 27, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

29. (Cancelled)

30. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:

associate a first subset of the set of firewall rules with the first node; and

if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.

31. (Previously Presented) A data controlling computer program product according to claim 30, wherein the at least one node further comprises at least two nodes including a second node, and wherein the computer instructions are further executable to:

associate a second subset of the set of firewall rules with the second node; and

if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

32. (Currently Amended) A data controlling computer program product according to claim 31, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.

33. (Original) A data controlling computer program product according to claim 31, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.

34. (Original) A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.

35. (Original) A data controlling computer program product according to claim 34, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.

36. (Original) A data controlling computer program product according to claim 26, wherein each of the at least one node comprises at least two network interfaces.

37. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is connected with at least one physical device.

38. (Original) A data controlling computer program product according to claim 26, wherein each of the two or more network interfaces is physically connected to every other network interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.

39. (Previously Presented) A method according to claim 1, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.

40. (Previously Presented) A device according to claim 13, wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.

Remarks

Subsequent to the receipt of a Notice of Allowance, this application was carefully reviewed prior to payment of the Issue Fee. The errors noted during this review have been corrected by this Amendment Under Rule 312. It is respectfully submitted that the foregoing amendments do not affect the merits of the application and are proper subject matter for an Amendment Under Rule 312.

Entry of this Amendment is respectfully requested.

Respectfully submitted,
HOWISON & ARNOTT, L.L.P.
Attorneys for Applicant(s)

/Timothy F. Bliss Reg. #50925/
Timothy F. Bliss
Registration No. 50,925

TFB/mep
P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
January 16, 2013

Electronic Patent Application Fee Transmittal

Application Number:	13092488
Filing Date:	22-Apr-2011
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Filer:	Timothy Frank Bliss/beth pierotti
Attorney Docket Number:	RPXC-31413

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1770	1770
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2070**

Electronic Acknowledgement Receipt

EFS ID:	14719522
Application Number:	13092488
International Application Number:	
Confirmation Number:	6667
Title of Invention:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME
First Named Inventor/Applicant Name:	Patrick Turley
Customer Number:	25883
Filer:	Timothy Frank Bliss
Filer Authorized By:	
Attorney Docket Number:	RPXC-31413
Receipt Date:	16-JAN-2013
Filing Date:	22-APR-2011
Time Stamp:	18:36:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2070
RAM confirmation Number	7753
Deposit Account	200780
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Issue Fee Payment (PTO-85B)	rpx31413issfee.pdf	573588 ecad301524f7cef44377a53158e56ebcfcd0517c	no	1
Warnings:					
Information:					
2		rpx31413AMD312.pdf	90597 4bb645ed48107837 7ccecbd7a8aa31c1074e8462	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Specification	2	2
	Claims	3	9
	Applicant Arguments/Remarks Made in an Amendment	10	10

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32356 3aba706a8096a06b63efbe5676c9d5b7abbbcaff	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	696541		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

OK TO ENTER: /MD/

01/23/2013

RPXC-31413 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Patrick Turley
Serial No.:	13/092,488
Filed:	April 22, 2011
Confirmation No.	6667
Notice of Allowance Mailed:	January 15, 2013
Group:	2432
Examiner:	Minh Dinh
For:	DYNAMICALLY ADAPTIVE NETWORK FIREWALLS AND METHOD, SYSTEM AND COMPUTER PROGRAM PRODUCT IMPLEMENTING SAME

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT UNDER RULE 312

The above-identified application has been carefully reviewed prior to the payment of the Issue Fee. It is requested that the following amendments be entered under the provisions of Rule 312.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims beginning on page 3 of this paper.

Remarks begin on page 10 of this paper.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	04/22/2011	Patrick Turley	RPXC-31413	6667

25883 7590 01/29/2013

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
01/29/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@dalpat.com

Response to Rule 312 Communication	Application No.	Applicant(s)
	13/092,488	TURLEY ET AL.
	Examiner	Art Unit
	MINH DINH	2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

1. ☒ The amendment filed on *16 January 2013* under 37 CFR 1.312 has been considered, and has been:

   a) ☒ entered.

   b) ☐ entered as directed to matters of form not affecting the scope of the invention.

   c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
   Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

   d) ☐ disapproved. See explanation below.

   e) ☐ entered in part. See explanation below.

/Minh Dinh/
Primary Examiner, Art Unit 2432

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/092,488	03/12/2013	8397282	RPXC-31413	6667

25883 7590 02/20/2013

HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Patrick Turley, Austin, TX;
Eric White, Austin, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.