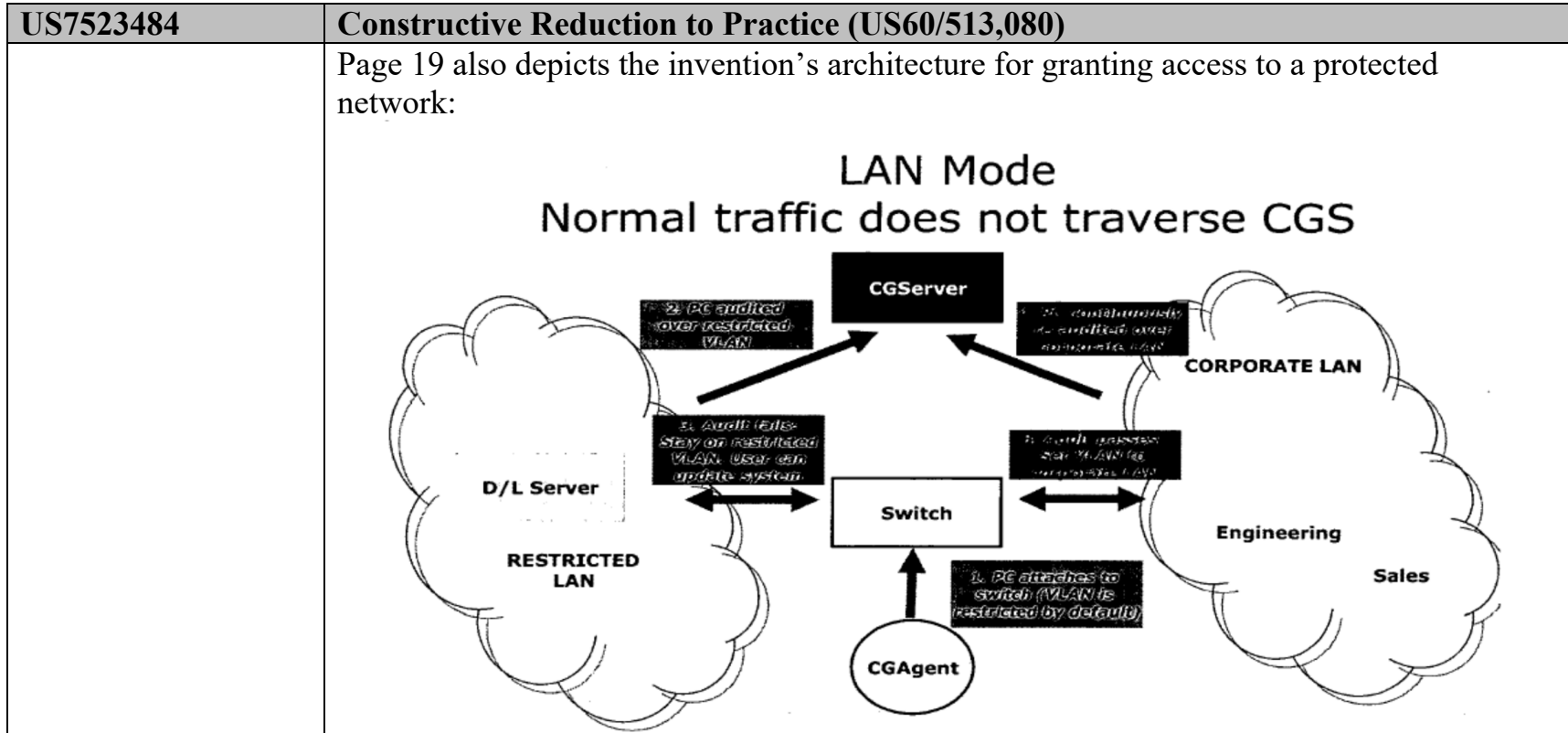


US7523484	Constructive Reduction to Practice (US60/513,080)
[28.0] A method of granting access to a protected network, the method comprising:	Many portions of the provisional verify that the invention was directed to the claimed “method of granting access to a protected network” by their references to “corporate network” and the like. Examples include the very title itself and page 3: 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. The provisional also provides that the network is “protected” through “protected VLANs [that] support ACLs,” which allow “full or limited access to the corporate network based on the policy” or method of granting access. <u>Page 14</u> 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.

EX2010

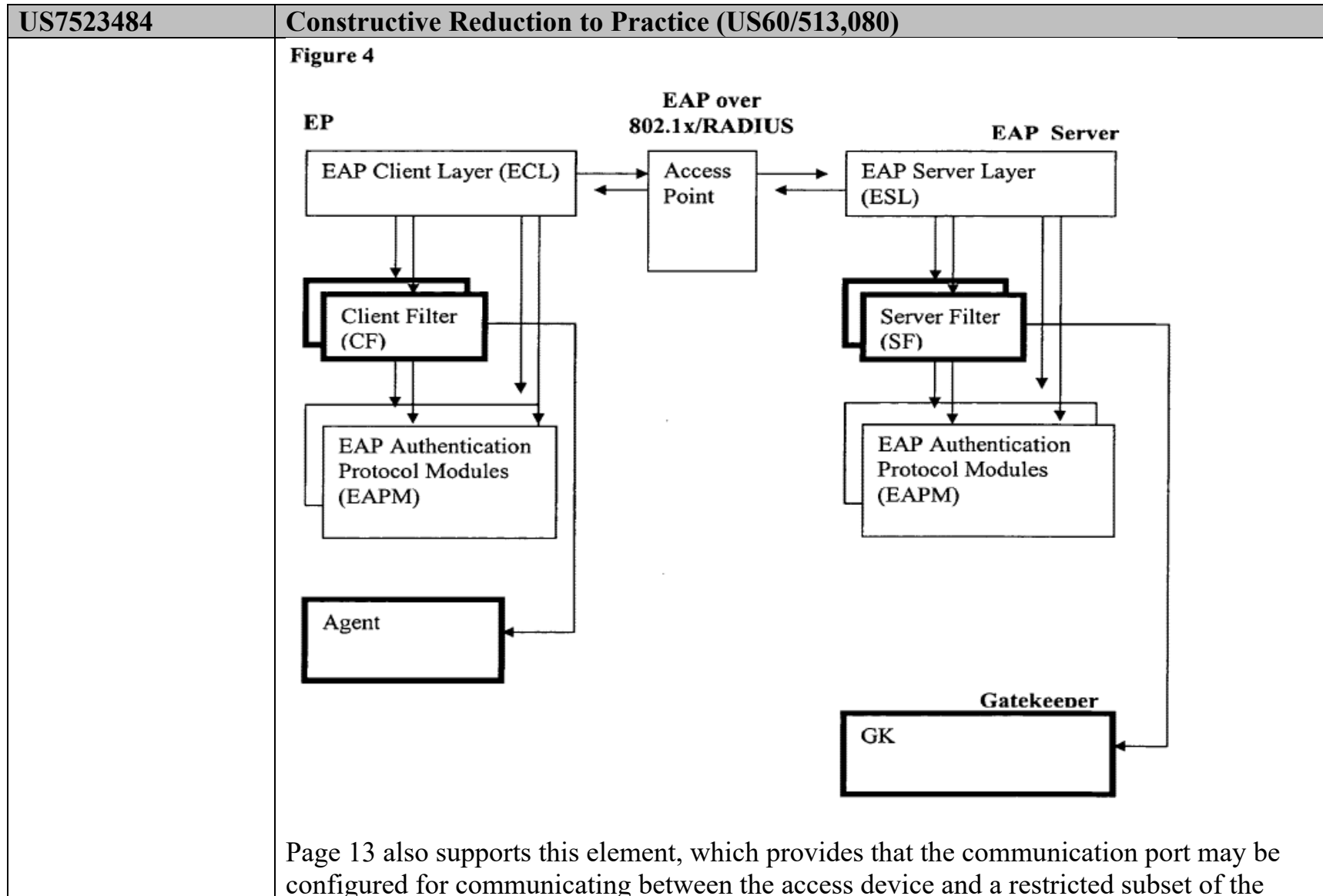
exhibitstickers.com



US7523484	Constructive Reduction to Practice (US60/513,080)
[28.1] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	The provisional provides for receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper. E.g., page 3 provides for an access device (e.g., an EP, which may be a PC or ND), an access point (AP) such as a switch where “an EP connects...to one of the switch’s ports”, and a gatekeeper (GK):

US7523484	Constructive Reduction to Practice (US60/513,080)
	1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b. ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port. Figure 4 and page 9 also supports this element, which provides that the request for access to a less-restricted subset of the protected network from an access device, the request

US7523484	Constructive Reduction to Practice (US60/513,080)
	being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper, as the figure demonstrates that an Agent running on the EP communicates with the GK through the access point:



US7523484	Constructive Reduction to Practice (US60/513,080)
	protected network, the restricted subset including a gatekeeper to be satisfied before an access device is granted access to a less-restricted subset of a protected network, as the “EP is isolated from the company network until it successfully passes an audit with the GK.” That is, access to the company network is restricted by default, and any communications between the EP and the GK prior to a successful audit must take place on a restricted subset of the protected network: <u>Page 13</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. Page 14 also provides that the GK may “control many different ports and APs [] from a different network,” which a POSITA would understand to include a restricted subset of the protected network.

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 14</u> 12 2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP 3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. 5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods. Details of exemplary enforcement modes of the invention are given in the attached Appendix.
[28.1] applying a security policy to the access device, responsive to the request;	Several portions of the provisional support this. Page 3 describes “policies which specify the audit criteria and types of access.” These “policies” support the claimed “security policy”, analyzing the device against “audit criteria” supports this limitation.

US7523484	Constructive Reduction to Practice (US60/513,080)
	1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Page 8 also describes the application of a “security policy” in response to a request, as the provisional provides for both applying “security policies” to the analysis of responsive data from the access device through the “authentication with the authentication server [] AND an audit with the software agent with the GK”:

Page 8

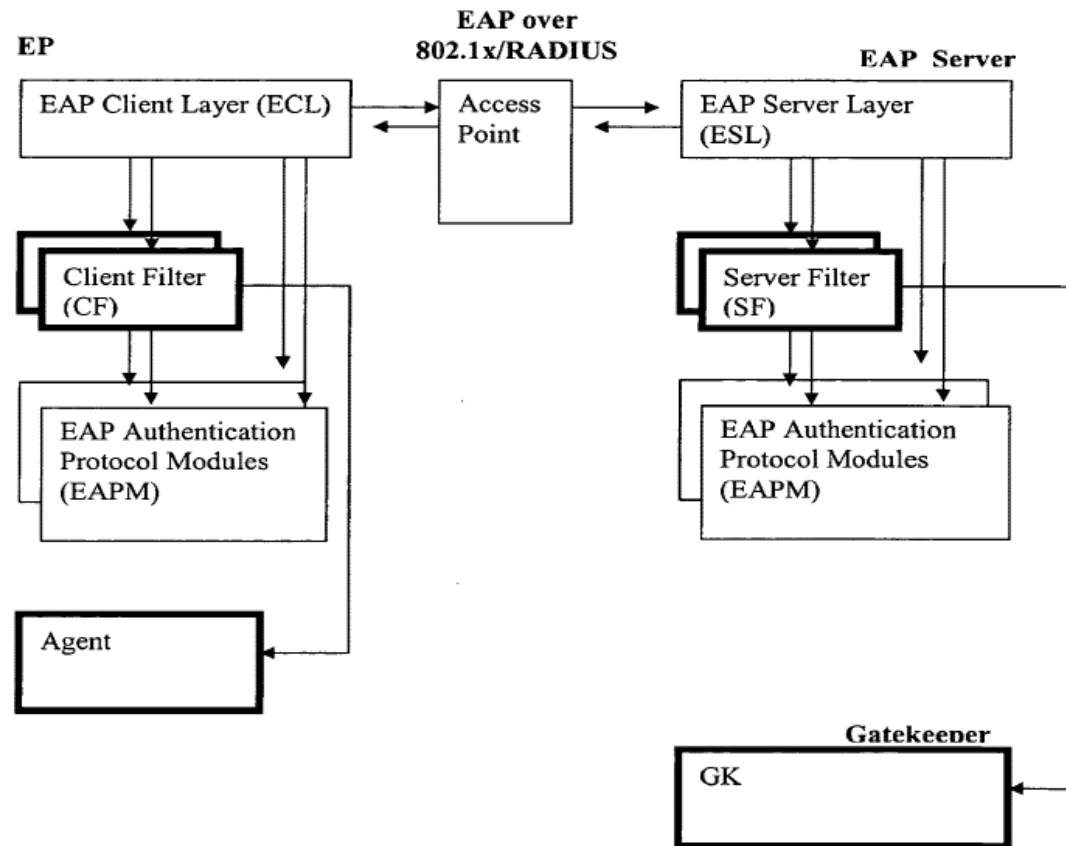
Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

Similarly, Figure 4 also demonstrates the application of a security policy through EAPMs and client and server filters (CF and SF) in response to a request from the agent or access device.

Page 9
Figure 4



The CF and SF APIs have APIs which correspond to the EAPM APIs. Therefore, the ECL or ESL can call the CF and SF instances corresponding to a particular authentication method as shown in Figures 5a and 5b. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM.

US7523484	Constructive Reduction to Practice (US60/513,080)
[28.2] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied; and	The provisional discloses reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied. For example, pages 13-14 provide that the “EP is isolated from the company network until it successfully passes an audit with the GK.” That is, access to the company network is restricted by default, and the AP must be reconfigured in order to grant access. Page 14 also provides that this may be done by configuring a communication port on the AP, as “full or limited access to the corporate policy can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.” Furthermore, page 14 describes the invention as not “requiring normal network traffic to traverse the [gatekeeper]”—and thus reconfiguring “the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper.”

Pages 13-14

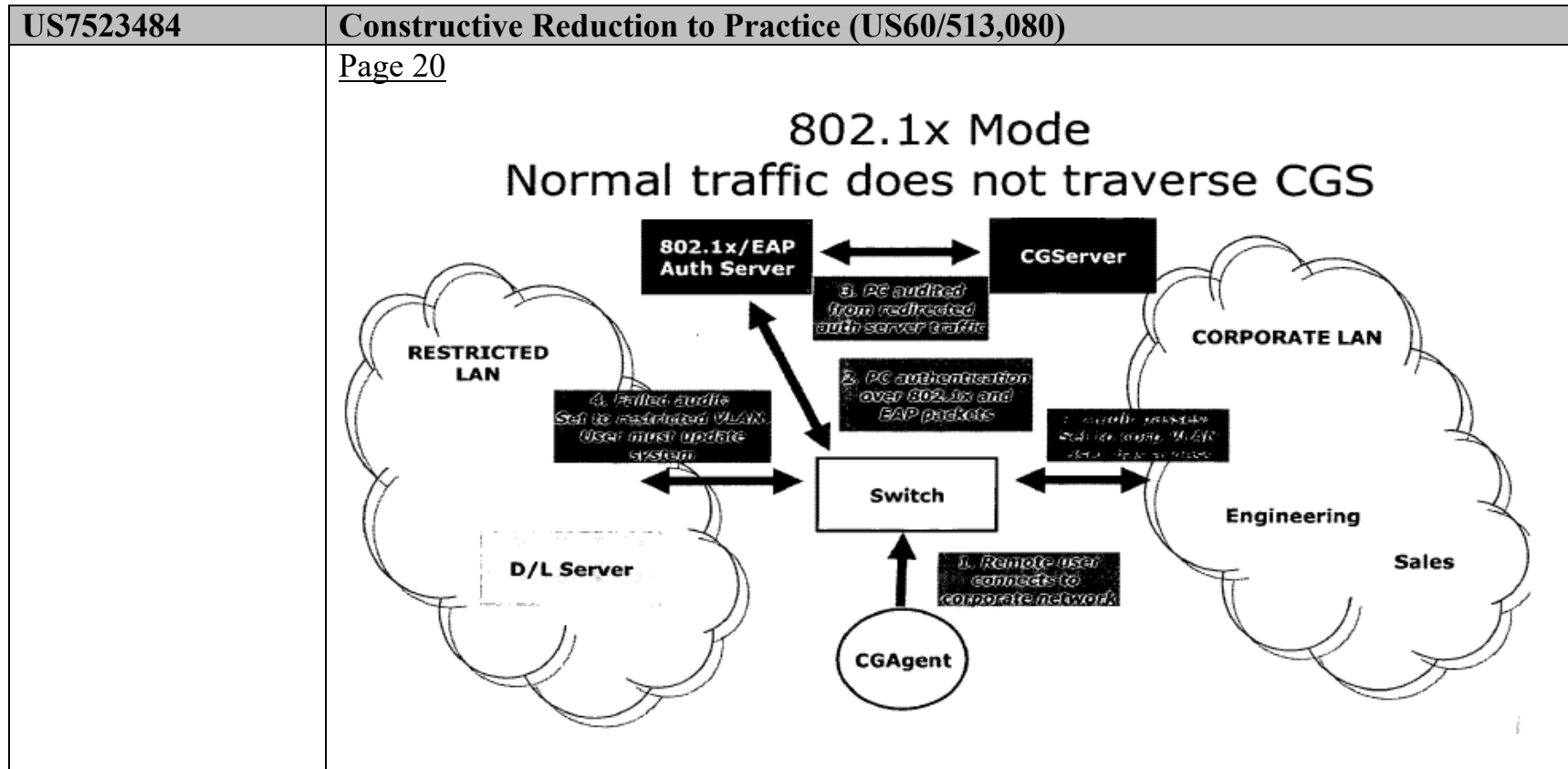
If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK.

After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.

....

3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.

Similarly, the figure on page 20 demonstrates that data is communicated between the access device and the less-restricted subset of the protected network (“Corporate LAN”) without passing the data through the gatekeeper (“CGServer”), but rather the “communication port” or “Switch”:



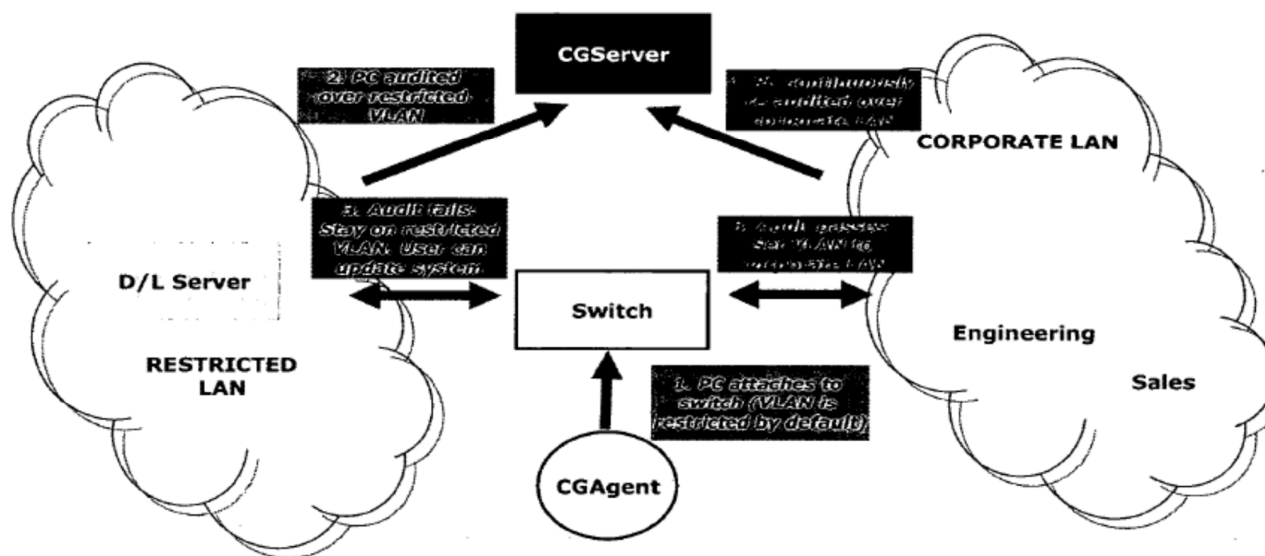
US7523484	Constructive Reduction to Practice (US60/513,080)
[28.3] communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.	The provisional provides for communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset. The excerpt from page 13 describes how after the access point is reconfigured to grant access, “‘keep alives’ and updates regarding changes to previous audit information are exchanged.” These “‘keep alives’” are communications between the GK and agent to monitor security status, as provided by the figures on page 21, which demonstrates continued “audit[ing]” and “re-audi[ing]” after a failed audit on the less-restricted subset of the network (“Restricted VLAN”): <u>Page 13</u> If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 21</u> Audit Mode Client Side Enforcement <pre> graph TD CGServer[CG Server] <--> VPN[VPN/NAS/Switch] VPN <--> DLS[D/L Server] VPN <--> EngSales[Engineering Sales] CGAgent((CGAgent)) <--> VPN CGAgent <--> DLS CGAgent <--> EngSales subgraph RESTRICTED_LAN [RESTRICTED LAN] DLS end subgraph CORPORATE_LAN [CORPORATE LAN] EngSales end </pre> The diagram illustrates the Audit Mode Client Side Enforcement architecture. It features a central VPN/NAS/Switch connected to a CG Server and a CGAgent. The CGAgent is also connected to a D/L Server and a Engineering Sales group. The D/L Server is part of the RESTRICTED LAN, and the Engineering Sales group is part of the CORPORATE LAN. The process flow is as follows: 1. User connects to network 2. System audited and re-audited 3. Failed audit: Agent restricts access 4. Audit success: Agent allows access
[38]	See [28]. The provisional supports the limitation of updating the access device if requirements of the security policy are not satisfied. For example, the figures on Pages 19 and 20 provide that when an “audit fails...[u]ser can update system” and that after a “failed audit...[u]ser must update system.”

Page 19

LAN Mode

Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20 802.1x Mode Normal traffic does not traverse CGS <pre> graph TD Switch --- RESTRICTED_LAN Switch --- CORPORATE_LAN CGAgent --- Switch AuthServer[802.1x/EAP Auth Server] <--> CGServer AuthServer <--> Switch Switch <--> CGServer subgraph RESTRICTED_LAN DLServer[D/L Server] end subgraph CORPORATE_LAN Engineering Sales end style RESTRICTED_LAN fill:none,stroke-dasharray: 5 5 style CORPORATE_LAN fill:none,stroke-dasharray: 5 5 </pre> 1. Remote user connects to corporate network 2. PC authentication over 802.1x and EAP packets 3. PC audited from redirected auth server traffic 4. Failed audit, set to restricted VLAN. User must update system
[39]	See [28]. The provisional provides that the security policy includes an audit of the access device. For example, page 3 provides that access to a corporate network for an access device is “based on audit criteria”:

Page 3

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Similarly, page 8 provides for “an audit with the software agent” on the access device.

Page 8

Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

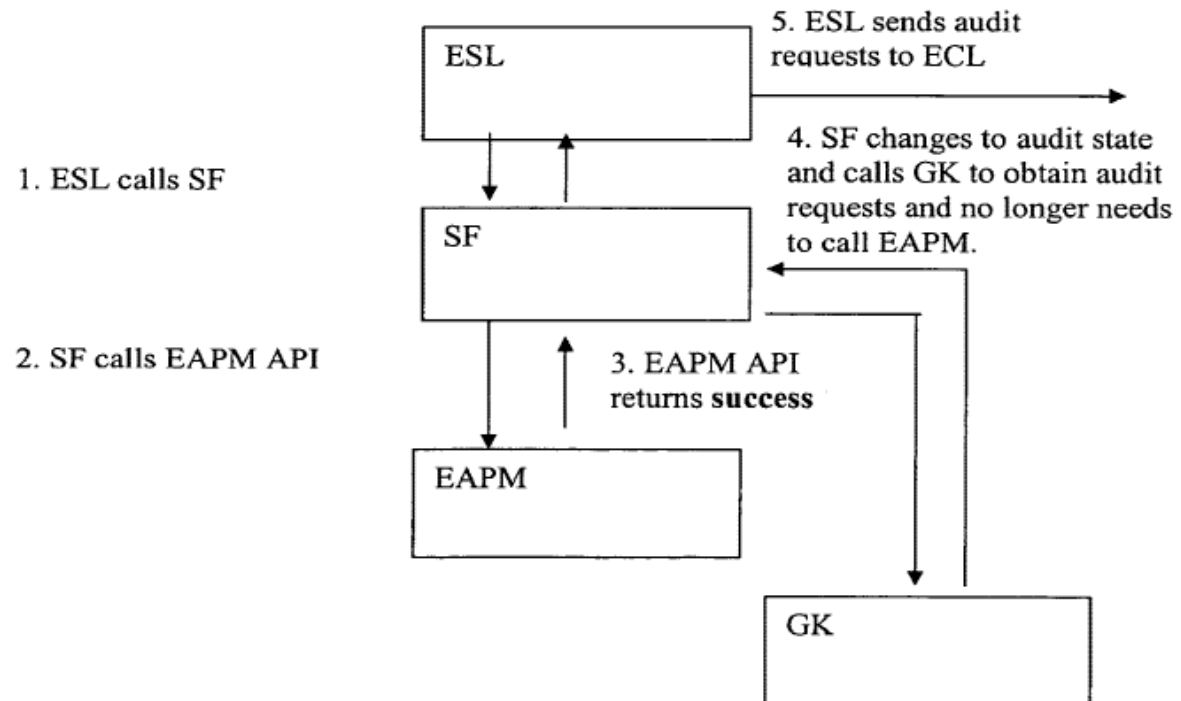
US7523484	Constructive Reduction to Practice (US60/513,080)
	Finally, pages 11-12 and figures 6 and 7a both provide for the application of a security policy through an audit on the access device or agent, which “returns information about the local system” and “call the agent and GK” to perform this exchange.

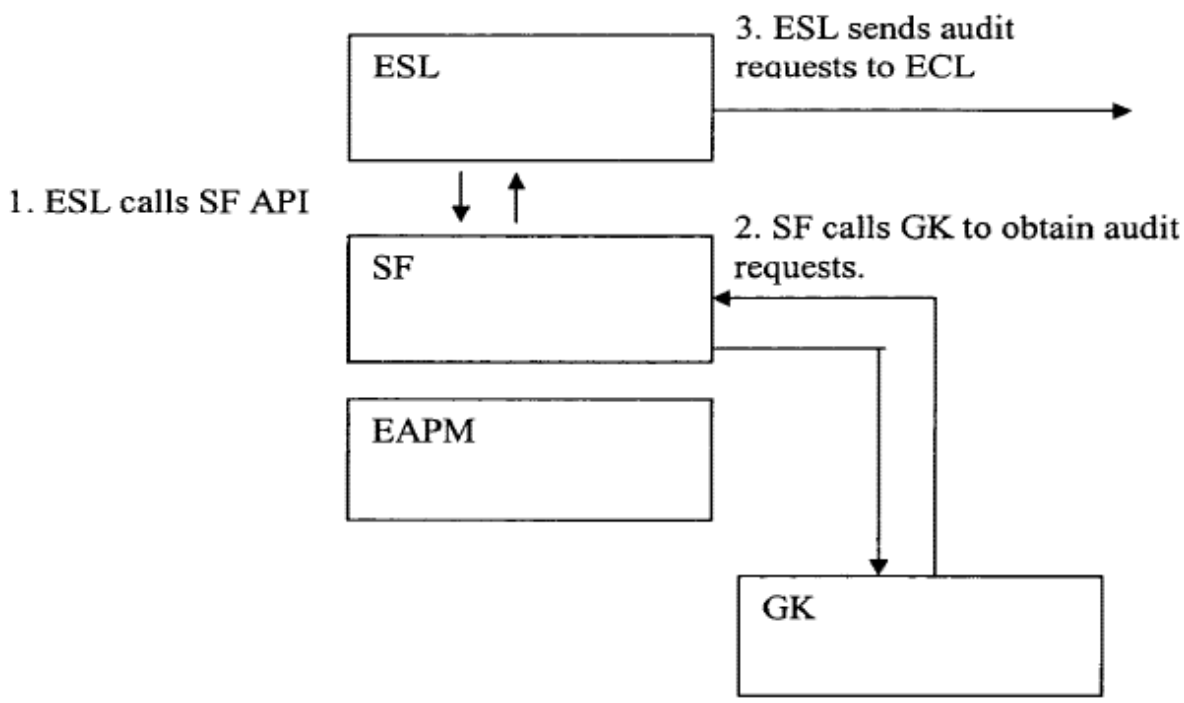
Pages 11-12

If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests.

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

Figure 6: Server Changing to Audit State



US7523484	Constructive Reduction to Practice (US60/513,080)
	During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. Figure 7a: Server in Audit State  <pre>sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>ESL: Note right of SF: 2. SF calls GK to obtain audit requests. SF->>GK: GK->>SF: Note right of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre> The diagram illustrates the sequence of operations during an audit state. It features four main components: ESL (top), SF (middle), EAPM (bottom left), and GK (bottom right). The process begins with ESL calling the SF API, indicated by a downward arrow from ESL to SF and an upward arrow from SF to ESL. Next, SF calls GK to obtain audit requests, shown by a downward arrow from SF to GK and an upward arrow from GK to SF. Finally, ESL sends audit requests to ECL, represented by a horizontal arrow pointing to the right from ESL. The EAPM component is shown but has no active connections in this specific sequence.

US7523484	Constructive Reduction to Practice (US60/513,080)
[41.0] A method of granting access to a protected network, the method comprising:	<i>See</i> claim [28.0].
[41.1] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper;	<i>See</i> [28.1].

US7523484	Constructive Reduction to Practice (US60/513,080)
[41.2] applying a security policy to the access device, responsive to the request;	<i>See</i> [28.2].
[41.3] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied; and	<i>See</i> [28.3].
[41.4] updating the access device if requirements of the security policy are not satisfied.	<i>See</i> [28] and [38].

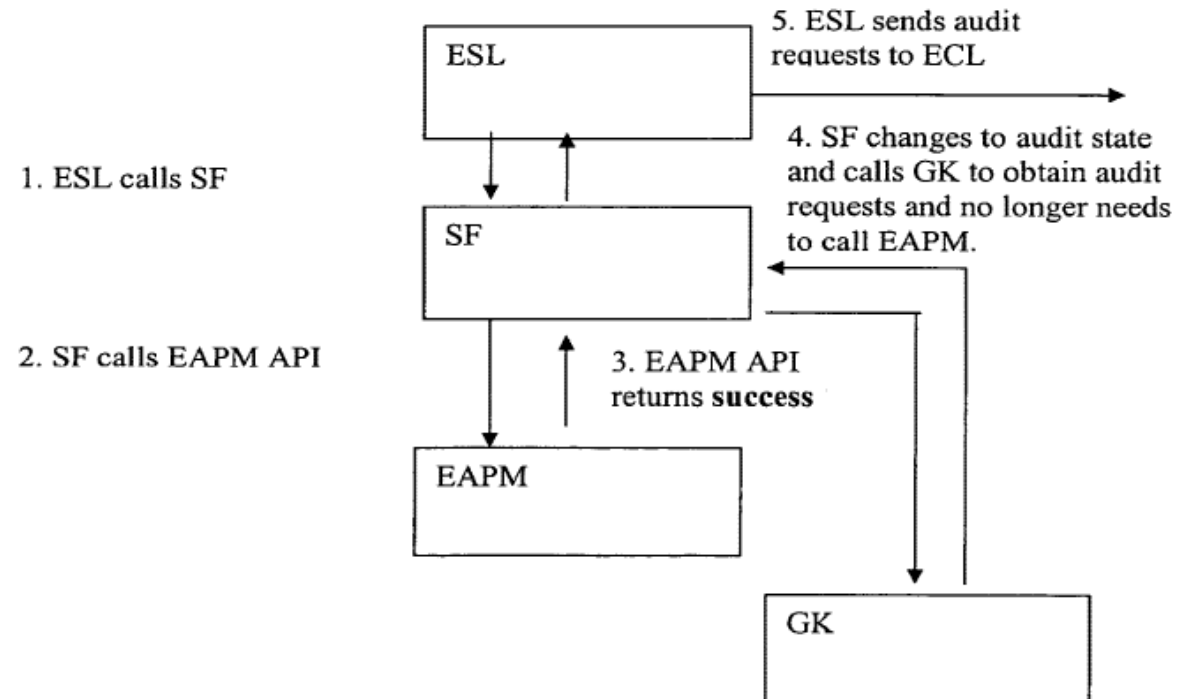
US7523484	Constructive Reduction to Practice (US60/513,080)
[42]	<i>See</i> [41] and [39], which provide “the security policy includes an audit of the access device.”
[43]	<i>See</i> [41]. The provisional discloses communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy. For instance, pages 11-13 and figures 6, 7a, and 7b both detail communication between the GK and agent on the access device to obtain “the necessary audit information” or “information about the local system” to determine if the device passes the audit or “satisfies the requirements of the security policy”.

Pages 11-13

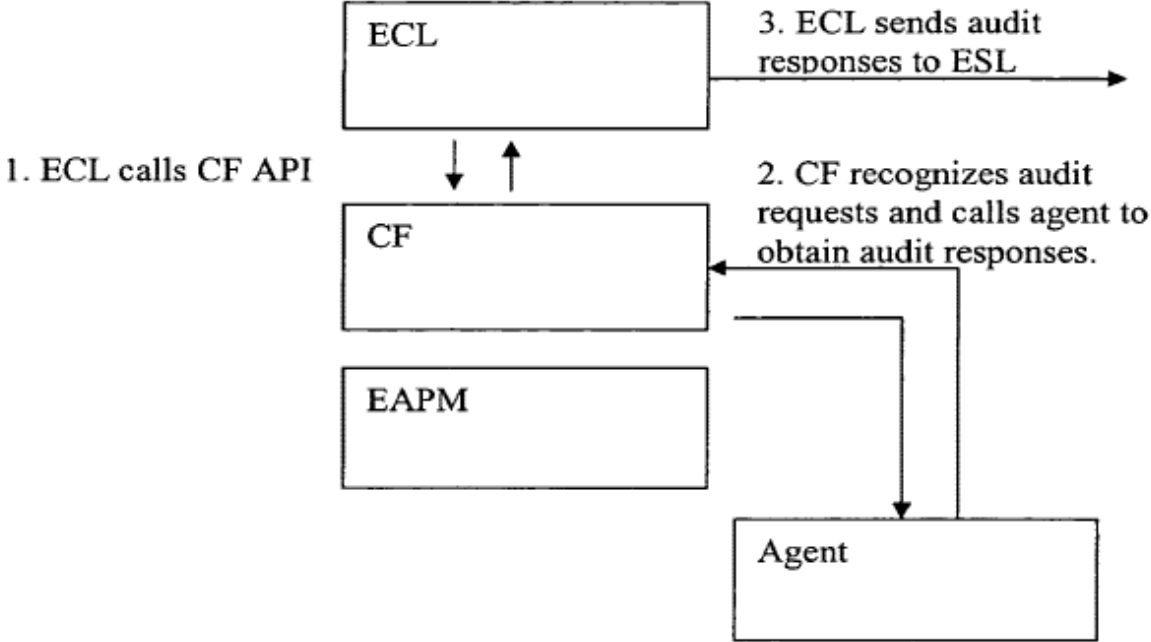
If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests.

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

Figure 6: Server Changing to Audit State



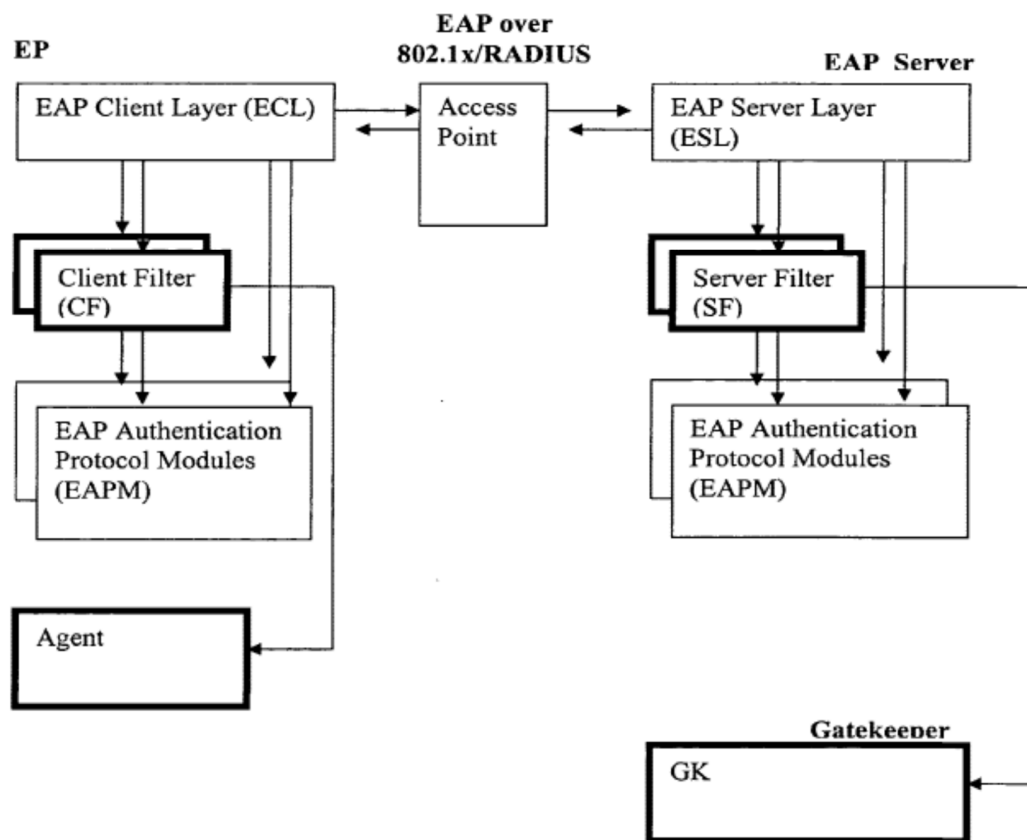
US7523484	Constructive Reduction to Practice (US60/513,080) During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. Figure 7a: Server in Audit State <pre>sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>ESL: Note left of SF: 2. SF calls GK to obtain audit requests. SF->>GK: Note right of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre>
------------------	---

US7523484	Constructive Reduction to Practice (US60/513,080)
	Figure 7b: Client Responding to Audit Requests  <pre>graph TD; ECL[ECL] -- "1. ECL calls CF API" --> CF[CF]; CF --> ECL; CF -- "2. CF recognizes audit requests and calls agent to obtain audit responses." --> Agent[Agent]; Agent -- "3. ECL sends audit responses to ESL" --> ECL;</pre> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well.

US7523484	Constructive Reduction to Practice (US60/513,080)
[53]	<i>See</i> [41] and [23]. The provisional describes “authenticating a user of the access device.” The provisional recognizes that authentication relies on “authentication credentials, such as user name and password or a digital certificate.” Page 6. In light this, a POSITA would understand that in the present invention, “the security policy audit is based at least in part on the information concerning an identity of a user of the device.” Figures 4, 5a & 5b and page 20 depict the exchange of authentication information, including “information concerning an identity of a user of the device.”

Page 9

Figure 4



Page 10

8

Figure 5a: Client in Authentication State

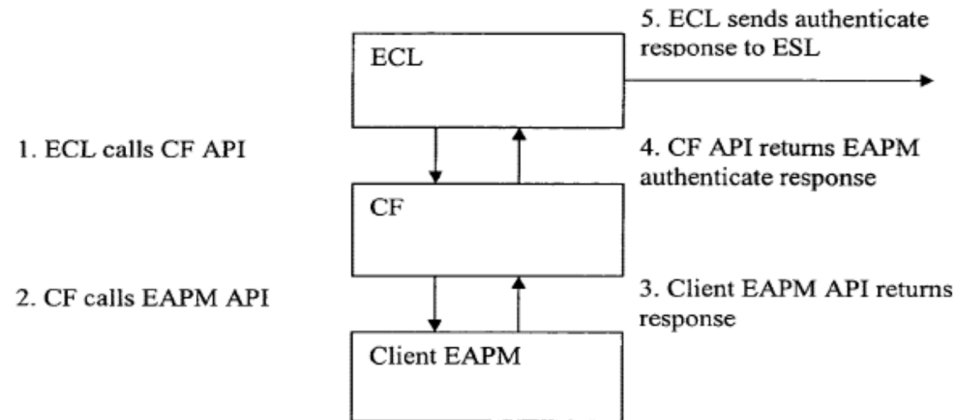
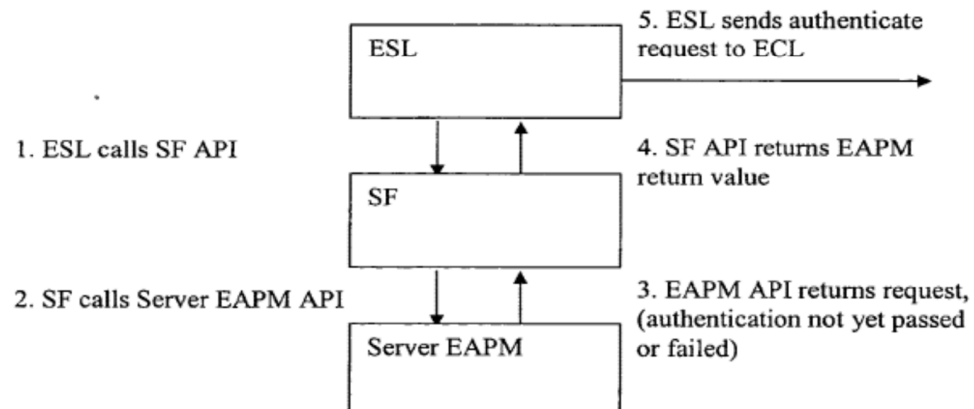
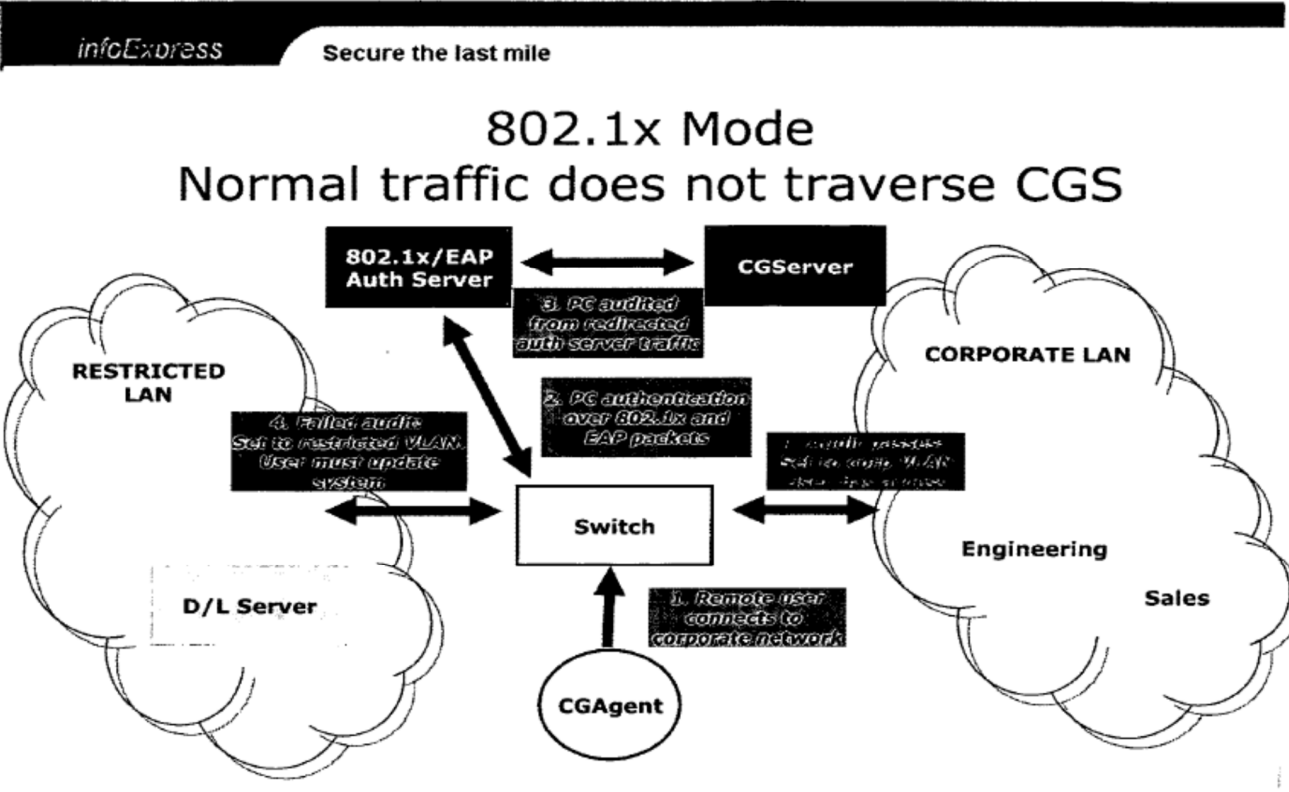


Figure 5b: Server in Authentication State



US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20  The diagram illustrates the 802.1x Mode network architecture. It features a central Switch connected to three main components: a CGAgent (represented by a circle), an 802.1x/EAP Auth Server, and a CGServer. The 802.1x/EAP Auth Server and CGServer are connected via a bidirectional arrow. The 802.1x/EAP Auth Server is also connected to the Switch via a bidirectional arrow. The CGAgent is connected to the Switch via a bidirectional arrow. The Switch is connected to two network clouds: the RESTRICTED LAN on the left and the CORPORATE LAN on the right. The RESTRICTED LAN contains a D/L Server. The CORPORATE LAN contains two sub-networks: Engineering and Sales. The diagram includes four numbered steps: 1. Remote user connects to corporate network; 2. PC authentication over 802.1x and EAP packets; 3. PC audited from redirected auth server traffic; 4. Failed audit. Set to restricted VLAN. User must update system. The infoExpress logo and the text "Secure the last mile" are at the top. The title "802.1x Mode" and subtitle "Normal traffic does not traverse CGS" are centered. The copyright notice "(c) 2003 InfoExpress, Inc." and the number "5" are at the bottom.

US7523484	Constructive Reduction to Practice (US60/513,080)
[56.0] A method of granting access to a protected network, the method comprising:	<i>See</i> [28.0], which describes “a method of granting access to a protected network.”
[56.1] receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper and being	<i>See</i> [28.1], which describes “receiving a request for access to a less-restricted subset of the protected network from an access device, the request being received through a communication port of an access point, the communication port configured for communicating between the access device and a restricted subset of the protected network, the restricted subset including a gatekeeper.” The provisional also supports the limitation of “being characterized by an access control list, the access to the restricted subset of the protected network being responsive to a VLAN configured to communicate with the protected network subject to the access control list.” For example, page 3 provides that the ACL filters and specifies “what traffic is permitted through a port.”

US7523484	Constructive Reduction to Practice (US60/513,080)
characterized by an access control list, the access to the restricted subset of the protected network being responsive to a VLAN configured to communicate with the protected network subject to the access control list;	1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch’s ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b. ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Pages 13-14 also provide that the VLAN is configured to communicate with the protected network subject to the ACL, as the “access to the network is modified appropriately by changing the VLAN used for the EP” and “full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.” <u>Pages 13-14</u> After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
[56.2] applying a security policy to the access device, responsive to the request; and	See [28.2], which provides “applying a security policy to the access device, responsive to the request.”

US7523484	Constructive Reduction to Practice (US60/513,080)
[56.3] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied.	<i>See</i> [28.3], which provides “reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied.”
[57.0] A method of granting access to a protected network, the method comprising:	<i>See</i> [23.0], which discloses “a method of granting access to a protected network.”

US7523484	Constructive Reduction to Practice (US60/513,080)
[57.1] receiving a first communication from an access device at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network, the restricted subset including a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network;	<i>See</i> [28.1], which disclose “the restricted subset including a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network.” The provisional further discloses receiving a first communication from an access device at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network. For instance, page 3 provides for the PC or ND, i.e., “access device” and an AP or access point, which includes a “switch” and “switch’s port” or “communication port” between a less-restricted subset of the protected network and the protected “corporate network”. The access device sends both authentication data and audit data that is passed through the communication port to the gatekeeper (GK), where the gatekeeper must be on the restricted subset of the protected network because prior to being authenticated and passing the audit, where the access device is limited to only access the protected network.

Page 3

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 8 and Figure 4 further provide that the first communication from the agent occurs at a communication port, the communication port being configured to pass the first communication to a restricted subset of the protected network, as the “auditing protocol takes place between the EP agent software and the GK”. The “AP may be programmed to prohibit access...to the corporate network until...an audit with the software agent with the GK passes.” That is, access to the corporate network is restricted by default, and the first communication from the agent to the gatekeeper must take place on a restricted subset of the protected network.

Page 8

Invention

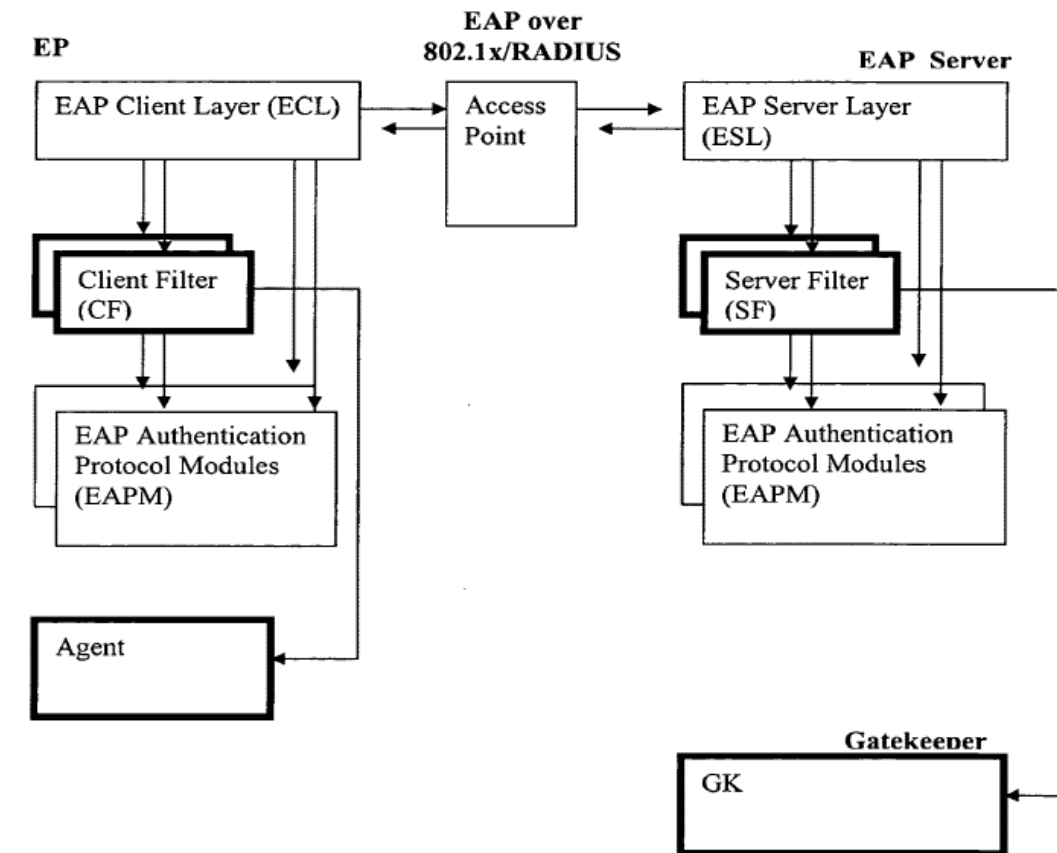
According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

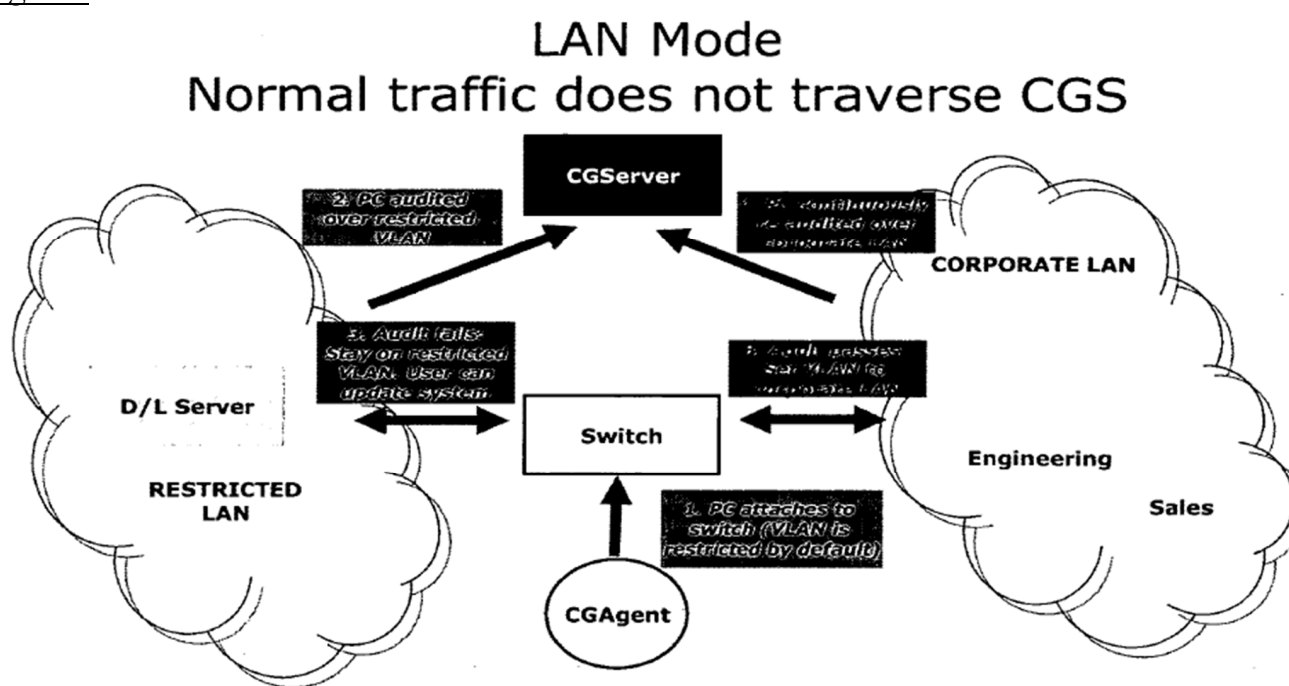
According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

Page 9

Figure 4



The CF and SF APIs have APIs which correspond to the EAPM APIs. Therefore, the ECL or ESL can call the CF and SF instances corresponding to a particular authentication method as shown in Figures 5a and 5b. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM.

US7523484	Constructive Reduction to Practice (US60/513,080)
	The figure on page 19 shows the CGAgent, residing on an access device (PC), connecting to the switch (step 1) on a the restricted VLAN (step 2). The PC is then audited by the CGServer with the audit data being set using the restricted VLAN (restricted subset of the protected network which includes the gatekeeper) from the PC through the switch to the CGServer (gatekeeper). If the audit of the PC passes, the VLAN for the PC is set to the corporate LAN (less-restricted subset). <u>Page 19</u>  LAN Mode Normal traffic does not traverse CGS The diagram illustrates the LAN Mode architecture and traffic flow. It features two main network segments: the RESTRICTED LAN on the left and the CORPORATE LAN on the right. The RESTRICTED LAN contains a D/L Server. The CORPORATE LAN contains Engineering and Sales departments. A central Switch connects these two LANs. Above the switch is the CGServer, and below it is the CGAgent. The process flow is as follows: 1. PC attaches to switch (VLAN is restricted by default): The CGAgent connects to the Switch. 2. Audit passes, set VLAN to corporate LAN: The CGServer receives audit data from the Switch and updates the VLAN. 3. Audit fails, stay on restricted VLAN. User can update system: The CGServer sends a message back to the Switch if the audit fails. 4. PC audited over restricted VLAN: The CGServer audits the PC through the Switch. 5. Configuration of restricted VLAN determined by CGS: The CGServer manages the restricted VLAN configuration.

US7523484	Constructive Reduction to Practice (US60/513,080)
[57.2] receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network;	<i>See</i> [57.1]. The provisional discloses receiving a command from the gatekeeper, the command being responsive to the received first communication and being configured to reconfigure the communication port to communicate data to the less-restricted subset of the protected network. For example, the GK requests audit information from the agent or device which returns information about the local system. Based on these audit responses, the “EP is isolated from the company network until it successfully passes an audit with the GK.” That is, access to the company network is restricted by default, and the GK must command reconfiguration of the communication port in order to grant access. The provisional discloses that this reconfiguration involves sending a command from the GK to the switch changing the VLAN for the access device’s switch port to the less-restricted VLAN. <u>Page 13</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well.

Page 14

2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

The figure on page 19 shows the CGAgent, residing on an access device (PC), connecting to the switch (step 1) on a the restricted VLAN (step 2). The PC is then audited by the CGServer with the audit data being set using the restricted VLAN (restricted subset of the protected network which includes the gatekeeper) from the PC through the switch to the CGserver (gatekeeper). If the audit of the PC passes, the VLAN for the PC is set to the corporate LAN (less-restricted subset).

As discussed on page 14 (above), a command is sent from the CGServer to the switch to change the VLAN for the port that the access device is connected to on the switch. This command puts the access device's switch port onto the less-restricted VLAN for the PC (access device).

US7523484	Constructive Reduction to Practice (US60/513,080)
	In step 3 of the figure on page 19, if the Audit fails, the device stays on the restricted VLAN. Since the command was not sent, the PC would not be able to access the less-restricted VLAN. <u>Page 19</u> LAN Mode Normal traffic does not traverse CGS <pre> graph TD CGServer[CGServer] <--> Switch[Switch] Switch <--> RESTRICTED_LAN[RESTRICTED LAN] Switch <--> CORPORATE_LAN[CORPORATE LAN] CGAgent((CGAgent)) --> Switch RESTRICTED_LAN --- DLServer[D/L Server] CORPORATE_LAN --- Eng[Engineering] CORPORATE_LAN --- Sales[Sales] CGServer -- "2. PC audited over restricted VLAN" --> Switch Switch -- "3. Audit fails: Stay on restricted VLAN. User can update system" --> CGServer CGServer -- "4. Audit successful: Set VLAN to less-restricted VLAN" --> Switch CGAgent -- "1. PC attaches to switch (VLAN is restricted by default)" --> Switch </pre>

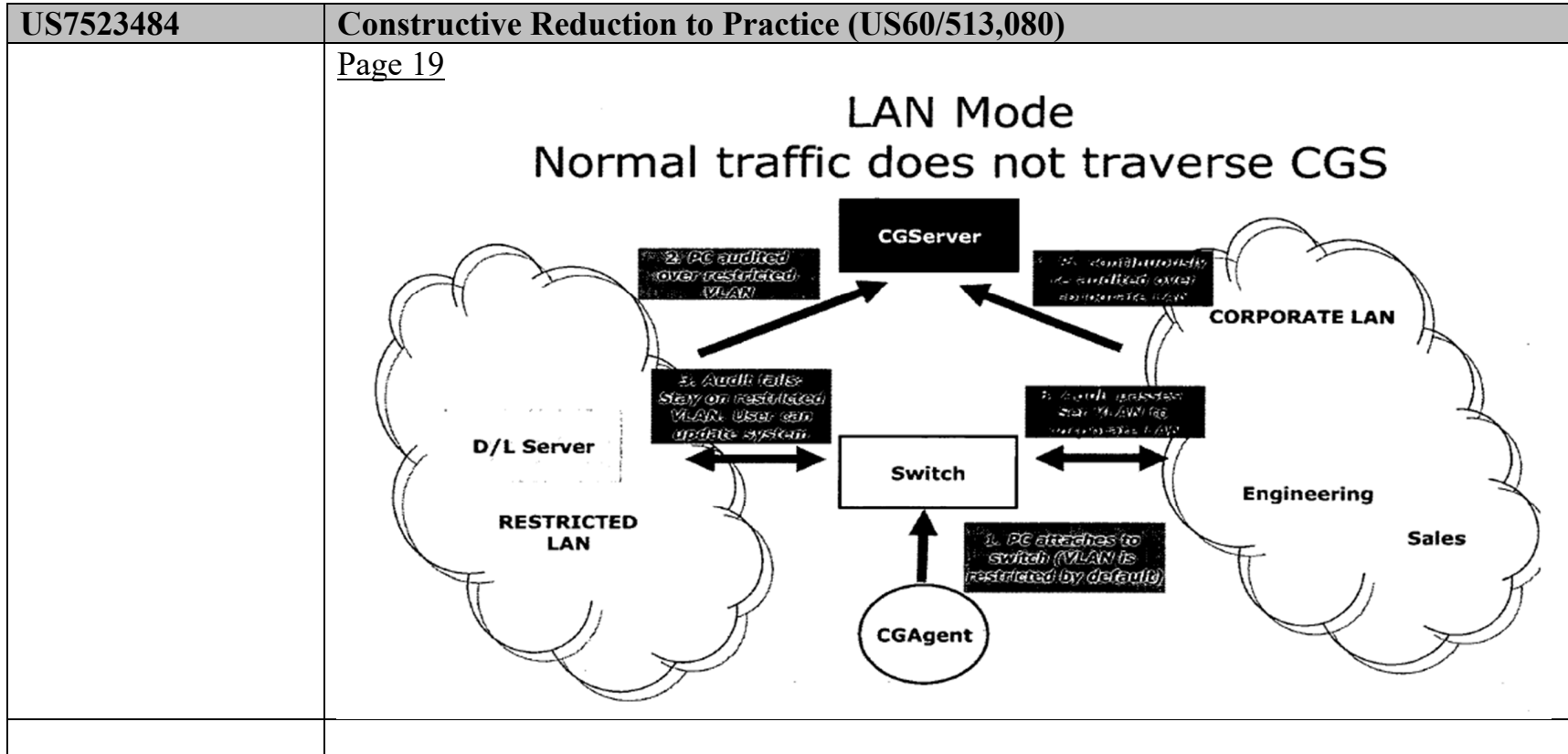
US7523484	Constructive Reduction to Practice (US60/513,080)
[57.3] configuring the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command; and	The provisional provides for configuring the communication port to communicate data to the less-restricted subset of the protected network rather than merely the restricted subset of the protected network, responsive to the received command. <i>See</i> [57.2]. As discussed in [57.2], a command is sent to configure the access device's switch port to be on the less-restricted VLAN. This allows the access device to access the less-restricted subset of the protected network.
[57.4] receiving a second communication from the access device at the communication port, the communication port now being configured to pass the second communication to the less-restricted subset of the protected network.	<i>See</i> [57.2] and [57.3]. The provisional discloses receiving a second communication from the access device at the communication port, the communication port now being configured to pass the second communication to the less-restricted subset of the protected network. Once the command to change the PC's switch port to allow access to the less-restricted VLAN (<i>see</i> claim element 57.2 and 57.3) has been processed by the switch, messages (i.e., the second communication from the access device) sent by the PC to devices within the less-restricted subset (e.g. less-restricted VLAN or subset of the protected network) are passed through the switch (via the reconfigured communication port) to the less-restricted VLAN.

Page 14

2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

The figure on page 19 shows the CGAgent, residing on an access device (PC), connecting to the switch (step 1) on a the restricted VLAN. In step 2, the PC is then audited by the CGServer with the audit data being set using the restricted VLAN (restricted subset of the protected network which includes the gatekeeper) from the PC through the switch to the CGserver (gatekeeper). If the audit of the PC passes, the VLAN for the PC is set to the corporate LAN (less-restricted subset).

Once the PC is on the less-restricted VLAN, the PC is able to communicate via the switch to other devices on the less-restricted VLAN.



US7523484	Constructive Reduction to Practice (US60/513,080)
[58]	<i>See [57].</i> The provisional discloses configuring the communication port includes associating the communication port with a VLAN. As shown in [57.2]-[57.4], when the command is set to the communication device it changes the port to be on the less-restricted VLAN. As discussed in claim 57, initially the port is on the restricted VLAN and the port is then modified to be on the less-restricted VLAN via the reconfiguration command sent to the switch. <u>Pages 14</u> 2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP 3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. 5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

US7523484	Constructive Reduction to Practice (US60/513,080)
[59]	<i>See</i> [57]. The provisional discloses the limitation of a communication port limited to communicating with the restricted subset of the protected network by an access control list when the first communication is received. For example, pages 3 and provide that the ACL is a set of rules specifying “what traffic is permitted through a [communication] port,” which a POSITA would understand to include limiting communication with the restricted subset of the protected network by an ACL “by setting the port to the VLAN whose router interface has the desired ACL.” <u>Page 3</u> ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port.

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 14</u> 2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP 3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. 5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.
[61]	<i>See [57] and [61].</i> Page 3 provides that the communication port is coupled with a network switch, where “[a] switch . . . which is used to connect to the EPs to the corporate network.”

Page 3

1

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20 802.1x Mode Normal traffic does not traverse CGS (c) 2003 InfoExpress, Inc. 5
[62]	See [59]. Page 3 provides that the communication port is coupled with a wireless access point (WAP):

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch’s ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

US7523484	Constructive Reduction to Practice (US60/513,080)
[63]	<i>See</i> [59]. The provisional supports this limitation, as page 3 and Figure 1 provides that it was well known at the time of the invention, and a POSITA would understand to be a part of the invention, that the communication device may include remote access to a virtual private network or “VPN”: <u>Page 4</u> In a typical system, policies are created by a policy manager, which may be connected to the corporate network. The policies are transferred to a GK that sits between the network access server (NAS) used by the EP and the corporate network. This implies that the GK has two NICs, one for the NAS side and one for the corporate network side. Each policy indicates various combinations of applications, configurations, and user identity that are permitted or prohibited for an EP accessing the corporate network. The NAS may be a remote access VPN, dialup server, or any other type of remote access device which is provided to permit EPs to access the corporate network. See Figure 1. The figure on page 21 also demonstrates that the communication device includes remote access across a “VPN”:

US7523484	Constructive Reduction to Practice (US60/513,080)
	Audit Mode Client Side Enforcement The diagram illustrates a network architecture for audit mode client-side enforcement. At the top center is a box labeled 'CG Server'. Below it is a box labeled 'VPN/NAS/Switch'. To the left of the switch is a cloud labeled 'RESTRICTED LAN' containing a box labeled 'D/L Server'. To the right of the switch is a cloud labeled 'CORPORATE LAN' containing the text 'Engineering' and 'Sales'. Below the switch is a circle labeled 'CGAgent'. Arrows indicate connections: a double-headed arrow between the switch and the RESTRICTED LAN; a double-headed arrow between the switch and the CORPORATE LAN; a double-headed arrow between the switch and the CGAgent; and a single-headed arrow pointing from the CGAgent to the CG Server. Four numbered steps are shown in boxes: '1. User connects to network' (between switch and CGAgent), '2. System audited and re-audited' (between switch and CG Server), '3. Failed audit Agent restricts access' (between CGAgent and RESTRICTED LAN), and '4. Audit success Agent allows access' (between CGAgent and CORPORATE LAN).
[65]	See [53] and [57].
	The provisional discloses “authenticating a user of the access device” ([53]).

US7523484	Constructive Reduction to Practice (US60/513,080)
[66]	<i>See</i> [43], [53], [57], and [65]. The provisional discloses “obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy.” The provisional provides that the system is configured to obtain system data from the access device and apply the security policy to determine if the access device satisfies the requirements of the security policy. For example, on page 4, the provisional provides that the “agent tells the GK information about the EP including applications configurations, and user logins,” which is system data from the access device via the agent (e.g. CG Agent) running on the access device. <u>Page 4</u> When the EP tries to access the corporate network, a software agent running on the EP automatically conducts an audit session with the GK. The agent tells the GK information about the EP including applications, configurations, and user logins, which the GK compares against the policies from the policy manager. Page 8 also provides that the auditing protocol “takes place between the EP agent software and the GK,” where the GK “sends requests for more information” and obtains the information from the access device until the audit is completed, or the security policy is applied to determine if the access device satisfied the requirements of the security policy:

Page 8

Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

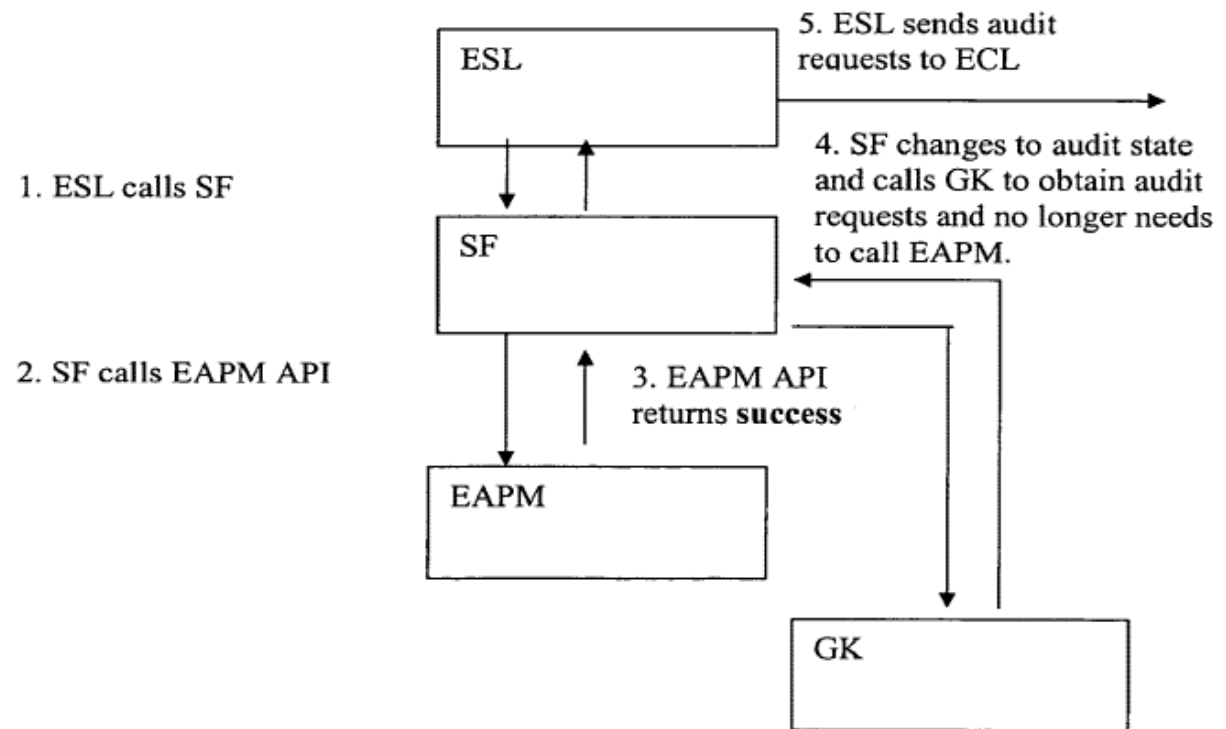
In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

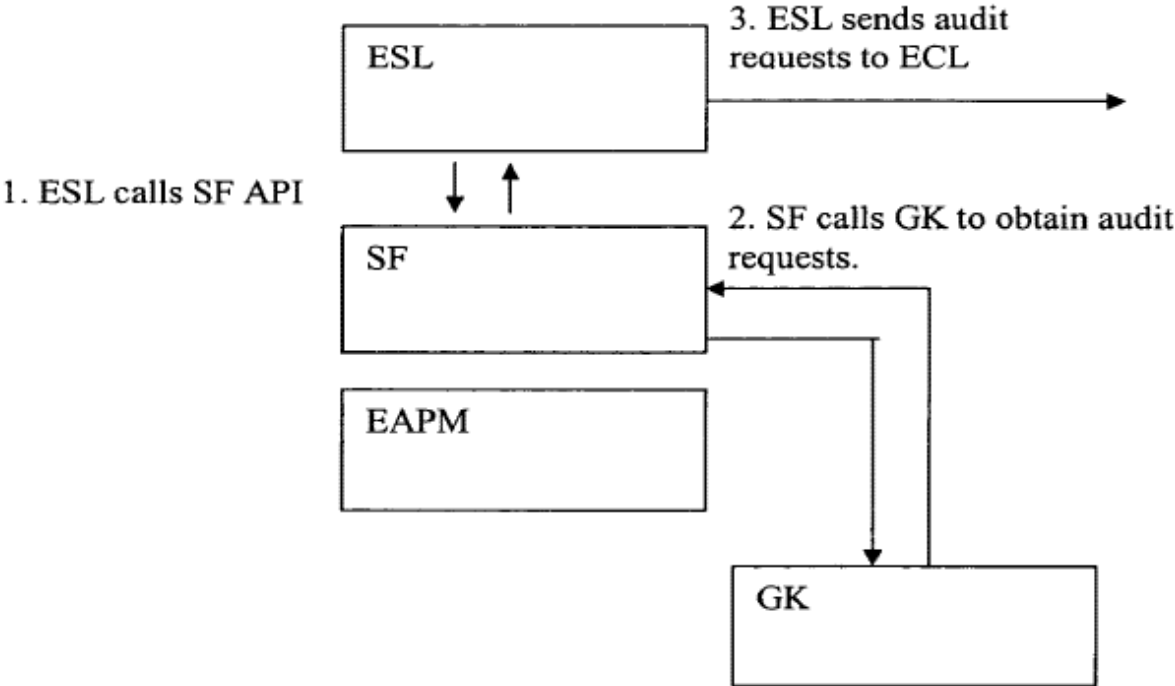
Pages 11-12 and figures 6 and 7a also provide that the audit requests for "system data" are obtained by the GK from the the access device, and the security policy or audit uses this system data to determine if the access device satisfies the requirements of the security policy:

Page 11

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

Figure 6: Server Changing to Audit State



US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 12</u> During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. Figure 7a: Server in Audit State  <pre data-bbox="678 625 1845 1307">sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>ESL: Note right of SF: 2. SF calls GK to obtain audit requests. SF->>GK: Note right of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre>

US7523484	Constructive Reduction to Practice (US60/513,080)
[67]	<i>See</i> [57] and [66]. The provisional discloses “the system data includes antivirus software version data.” Page 11 states, “On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.” A POSITA would understand that the “information about the local system” supports “wherein the system data includes antivirus software version data.” The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server’s ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server’s authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the references to the types of device information that were absent from prior art access control systems (identified as a problem in these systems) —e.g. that regarding

US7523484	Constructive Reduction to Practice (US60/513,080)
	a “virus or trojan running on [the endpoints]” (pages 5-6)—mean that a POSITA would understand that in the present invention too, “the system data includes antivirus software version data.”
[68]	<i>See</i> [57]. The provisional provides for communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, where applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy. For example, page 3 provides for an access device (PC or ND), an access point (AP), and a gatekeeper:

US7523484	Constructive Reduction to Practice (US60/513,080)
	1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b. ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port. Pages 8-9, including Figure 4, also disclose communicating between the gatekeeper (GK) and an agent executing on the access device to obtain system data from the access device

US7523484	Constructive Reduction to Practice (US60/513,080)
	including “audit information,” where applying the security policy (<i>i.e.</i>, “the auditing protocol”) includes using the system data to determine if the access device satisfies the requirements of the security policy. <u>Pages 8-9</u> Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP’s port allowing access for the PC. If the audit fails, the port on the AP is left disabled. According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

