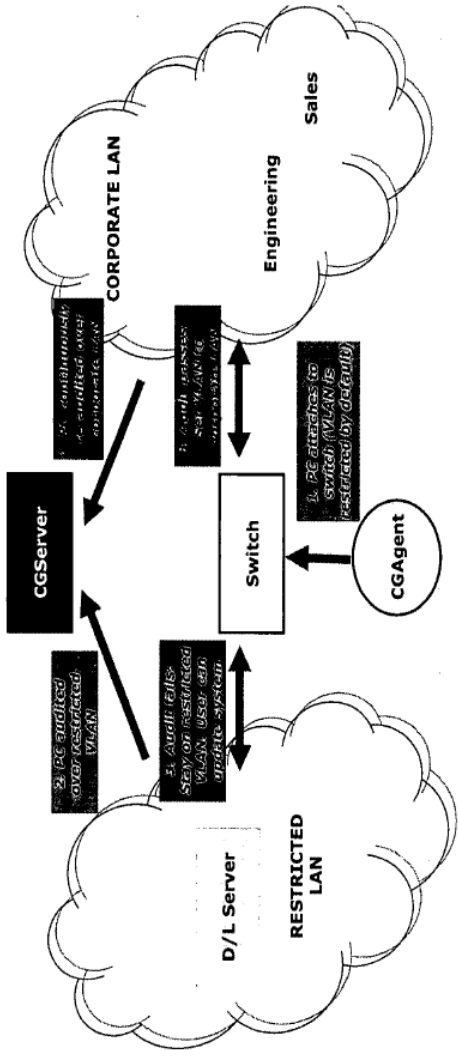


|                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>U.S. Patent No.<br/>8,051,460</b></p>                                                                                | <p><b>Constructive Reduction to Practice — 60-513,080</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p><b>1. (Preamble) A</b><br/>method of granting<br/>access to a<br/>protected network,<br/>the method<br/>comprising:</p> | <p>Many portions of the '080 provisional specification verify that the invention was directed to the claimed “method of granting access to a protected network” by their references to “controlling access” and the like. For example are the very title itself, and the description on page 3:</p> <p style="text-align: center;">1</p> <p style="text-align: center;"><b>GATEKEEPER INVENTION FOR CONTROLLING<br/>ACCESS TO A CORPORATE NETWORK USING 802.1x</b></p> <p>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.</p> <p>Figure 17 (page 19) depicts the invention’s architecture for access control:</p> <div style="text-align: center;"> <p><b>LAN Mode</b></p> <p><b>Normal traffic does not traverse CGS</b></p>  </div> |

**1.1: [a]** receiving a request for access to a less-restricted subset of the protected network from an access device, **[b]** the request received through a communication port of an access point, **[c]** the communication port configured for communicating between the access device and a restricted subset of the protected network, **[d]** the restricted subset including a gatekeeper,

The '080 provisional provides several instances of controlling an endpoint device's access to a "corporate network"—that is, a "less-restricted subset of the protected network from an access device[.]" Therefore, the invention "receiv[es] a request for access to a less-restricted subset of the protected network from [that endpoint/] access device[.]" See, e.g., 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.

Next, page 8 describes a PC endpoint's access to a "corporate network" via an access point and that the device (EP) is able to access the GK on the restricted subset of the network in order to send audit data to the GK:

## 6

### **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 13 describes how after an endpoint fails an audit, it is not granted access to the corporate network/less restricted subset, and is instead afforded “limited network access” and is “isolated from the company network”:

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.

After the audit has been performed, “keep alive” 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.

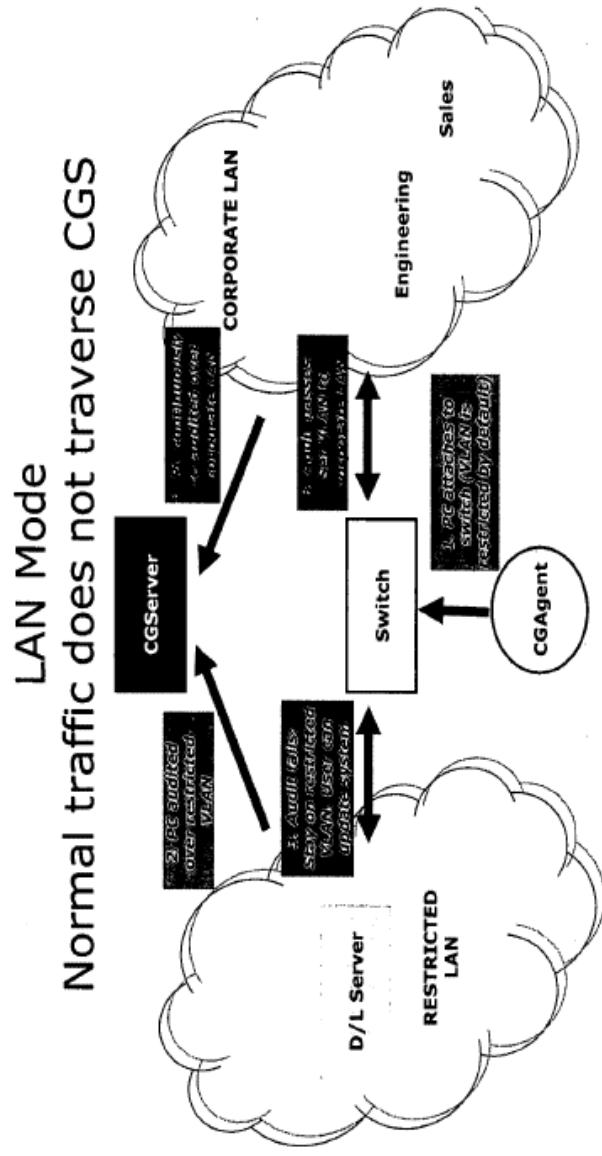
Page 14 describes granting “full or limited access to the corporate network . . . based on the policy”:

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.

This architecture, including the restricted network, is depicted schematically in, for example, appendix page 19:



(c) 2003 InfoExpress, Inc.

The provisional supports “the request [for access being] received through a communication port of an access point[.]” Page 14 describes how “[a]n EP attached *to a port* on the AP can be restricted from accessing the corporate network if it does not meet audit criteria.” Having the endpoint “attached to a port” means that the endpoint’s communications, including its request(s) for access, are received through that communication port.

## 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.

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Several other portions describe or suggest the claimed “communication port” through which the request for access is received. <i>E.g.</i>, page 3 states, “An EP connects to a switch with an Ethernet cable <b><i>to one of the switch’s ports</i></b>. An EP typically connects to a W AP through a wireless network card, commonly through protocols like 802.11 a or 802.11 b.” It is implied that the wireless connection is also through the WAP’s ports:</p> <p>EP – End point which can be a PC or ND.</p> <p>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 802.11 a or 802.11 b.</p> <p>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.</p> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

And also page 8 (“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.”)

## 6

### 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.

Third, the provisional supports “[c] the communication port configured for communicating between the access device and a restricted subset of the protected network, [and] [d] the restricted subset including a gatekeeper, [.]” As noted above with respect to 1.1[b], the provisional discloses communication ports on the access point. These ports are initially “configured for communicating between the access device and a restricted subset of the protected network[.]” For example, page 8 states that “an [access point] may be programmed to prohibit access by the PC to the corporate network[.]” but during this time the endpoint is in communication with the gatekeeper. Thus, because the endpoint has limited access, it “communicat[es] [with] . . . a restricted subset of the protected network[.]” Furthermore, this restricted subset includes a gatekeeper:

6

#### **Invention**

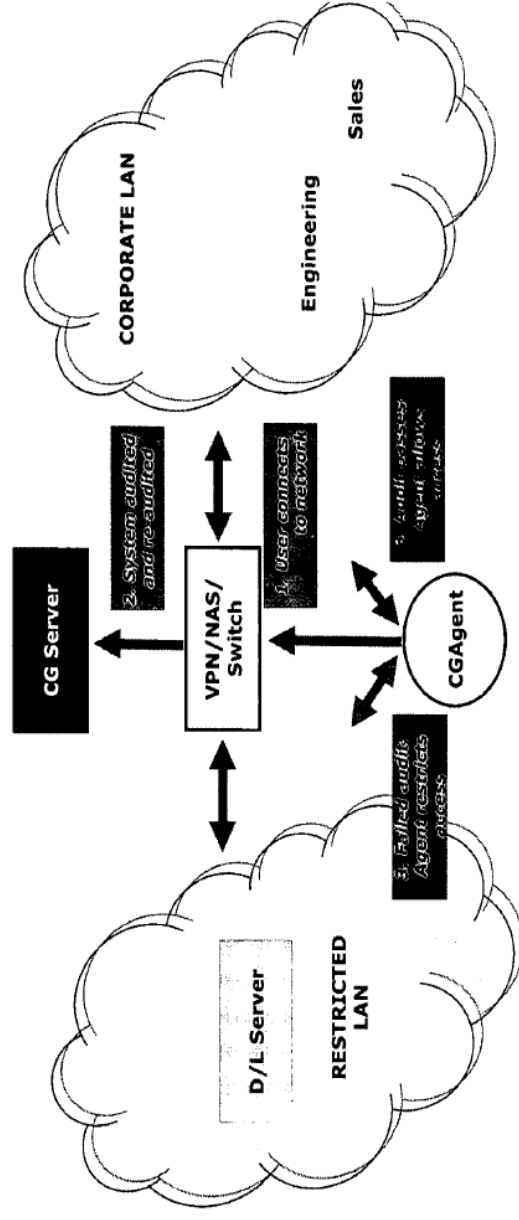
According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. 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.

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Page 13 also describes the endpoint being limited to “communicating [with] a restricted subset of the protected network, the restricted subset including a gatekeeper, [.]”</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The appendix figure on page 21 shows this same arrangement, where the “restricted subset” includes the “restricted LAN” and also a gatekeeper in the form of the “CG Server”:</p> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Audit Mode Client Side Enforcement



(c) 2003 InfoExpress, Inc.

|                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1.2:</b> applying a security policy to the access device in response to the request;</p> <p><b>1.3:</b> using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and</p> | <p>Several portions of the provisional describe “applying a security policy to the access device in response to the request; [and] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device[.]” For example, the description of the invention on page 3 describes “policies which specify the audit criteria”—in other words, security policies.</p> <p style="text-align: center;"><b>1</b></p> <p style="text-align: center;"><b>GATEKEEPER INVENTION FOR CONTROLLING<br/>ACCESS TO A CORPORATE NETWORK USING 802.1x</b></p> <p>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.</p> <p>The specification contains several descriptions of “auditing” the endpoint—that is, “using the gatekeeper to determine if requirements of the security policy are satisfied by the access device[.]” For example, page 8 describes “[an] auditing protocol tak[ing] place between the EP agent software and the [gatekeeper]” where “[t]he gatekeeper sends requests for [audit] information” until it completes the audit.</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Invention**

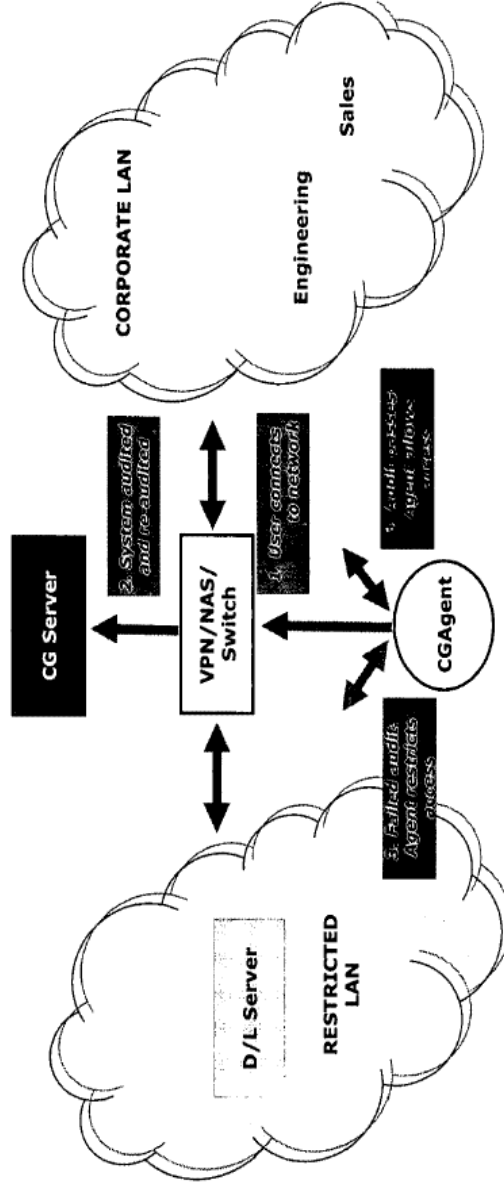
According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. 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.

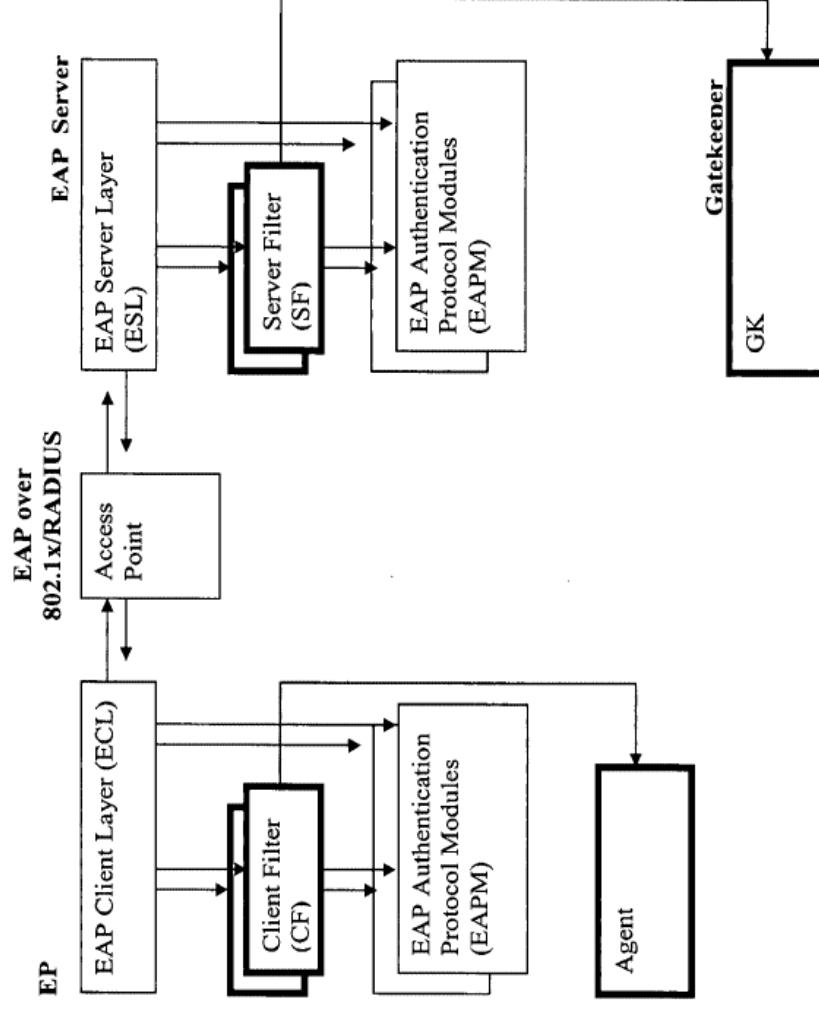
|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Similarly, page 13 describes alternate scenarios, where either the “the audit indicates the client EP is in compliance” or where “the GK determines that the EP has failed the audit”—again showing “applying a security policy to the access device in response to the request; [and] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device[.]”</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The appendix figure on page 21 shows these steps schematically, where (among other actions) the endpoint’s “system [is] audited and re-audited” by the CG Server, that is, the gatekeeper:</p> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Audit Mode Client Side Enforcement



Finally, Figure 4 (page 7) schematically shows a system that can perform these steps, including “using the gatekeeper . . .”

**Figure 4**



|                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1.4:</b> 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, when the requirements of the security policy are satisfied.</p> | <p>Several portions of the provisional support this element. The portion from page 8 states, “If the audit is successful, the server sends a message to the AP which enables the EP’s port allowing access for the PC....” This process of “send[ing] a message to an [access point]” shows “reconfiguring the communication port” thereupon. Additionally, because this reconfiguring “enables the EP’s port allowing access for the PC,” the reconfiguring permits “communicating data between the access device and the less-restricted subset of the protected network.” Finally, because this process happens “[i]f the audit is successful,” the reconfiguring takes place “when the requirements of the security policy are satisfied”</p> <p><b>Invention</b></p> <p>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.</p> <p>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.</p> <p>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.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Page 13 describes how “the SF returns a success response. If the VLAN for the BP is specified in the policy, then the VLAN that should be used for this EP is passed back as well.” “Return[ing] a success response” in conjunction with “pass[ing] back” a VLAN describe “reconfiguring” the communication port on an access point. And we know from the next page (14) that a VLAN is means to providing “full or limited access to the corporate network”—and thus a way to permit “communicating data between the access device and the less-restricted subset of the protected network[.]” Last for this example, the process described can take place when “the audit indicates the client EP is in compliance”—that is “when the requirements of the security policy are satisfied[.]”</p> <p>If the audit indicates the client EP is in compliance, the SF returns a success response.<br/> 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.</p> <p>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.</p> <p>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.</p> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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.

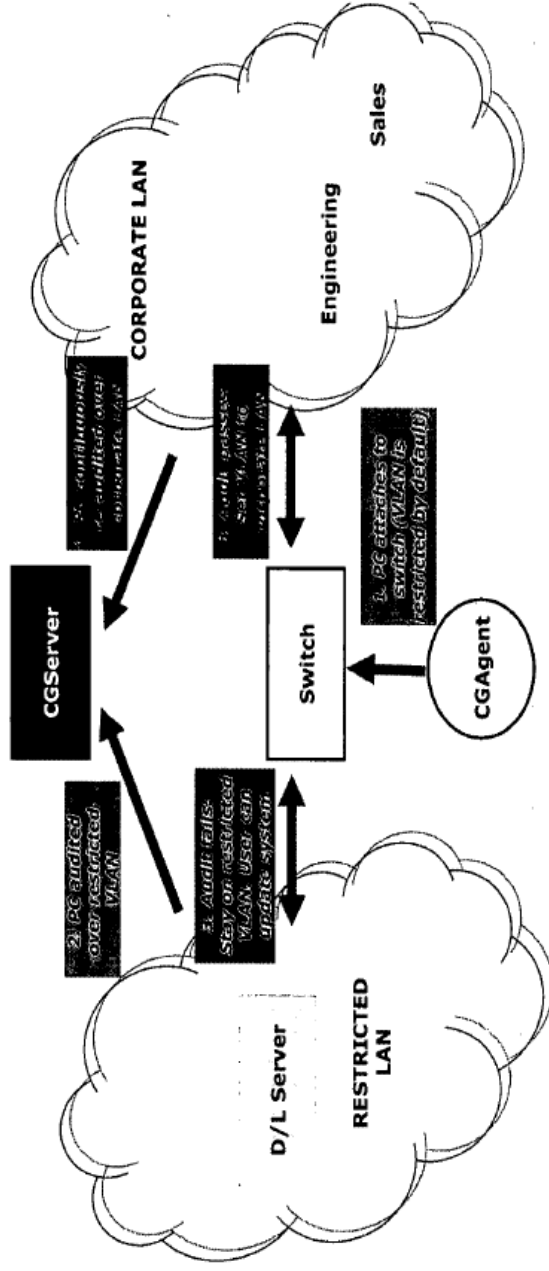
Details of exemplary enforcement modes of the invention are given in the attached Appendix.

Furthermore, page 14 and other portions of the specification describe the invention as not “requiring normal network traffic to traverse the [gatekeeper]”—and thus “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*[.]”

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <div data-bbox="212 1037 240 1073" data-label="Page-Header">12</div> <div data-bbox="277 506 667 1566" data-label="List-Group"><ol style="list-style-type: none"><li>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</li><li>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.</li><li>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.</li><li>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.</li></ol></div> <div data-bbox="699 571 764 1612" data-label="Text"><p>Details of exemplary enforcement modes of the invention are given in the attached Appendix.</p></div> <div data-bbox="834 216 980 1612" data-label="Text"><p>This “out of band” architecture described on page 14 is depicted schematically in the appendix figure on page 19. In the “LAN Mode” the “[n]ormal traffic does not traverse the [server]”—that is the claimed gatekeeper. Instead, the endpoint (as shown by the CG Agent) can communicate directly with the corporate LAN without going through the CG server.</p></div> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## LAN Mode

Normal traffic does not traverse CGS



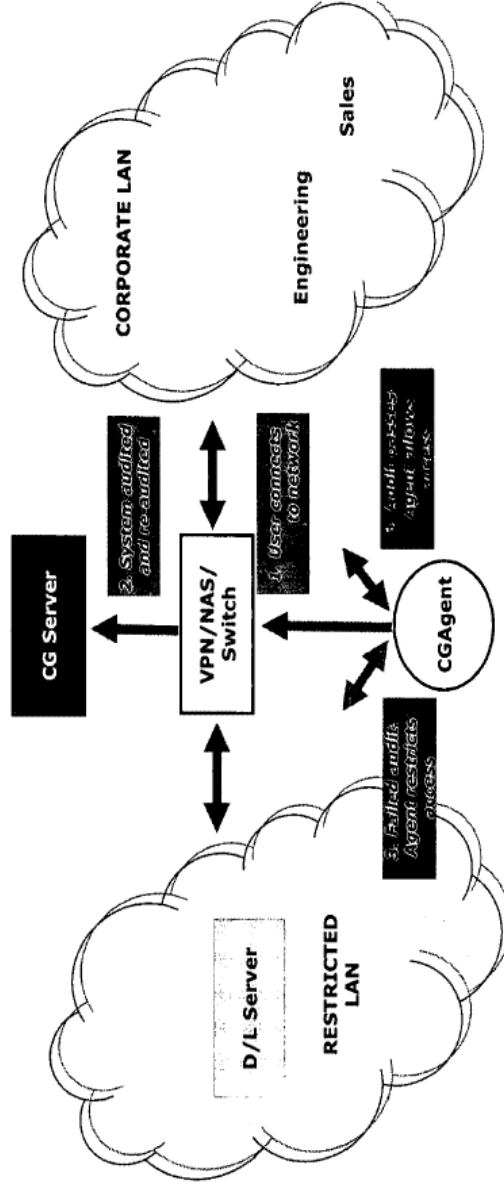
(c) 2003 InfoExpress, Inc.

4

This architecture lies in contrast to prior art “in-line” systems, where all communications necessarily passed through a gatekeeper. See, e.g., pages 4 (“A disadvantage of this type of system is that network traffic between the EP and corporate network *must pass through the GK* to enforce access.”), 5 (Figure 2), 15-16 (depicting “inline mode”).

Furthermore, the appendix figure on page 21 depicts two alternate scenarios—one where the “audit passes” and the “agent allows access” to the corporate LAN (that is, the “less restricted subset of the network”), and another where the “audit fails” and the “agent restricts access” to the “restricted LAN.” It is apparent that this shows the “out of band” architecture described above.

## Audit Mode Client Side Enforcement



2.

See claim 1.

At least three excerpts of the provisional describe “further comprising authenticating a user of the access device.” Page 8 states “an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes . . .” The reference to “authentication” supports “the security policy includ[ing] authentication of the user of the device[.]”

6

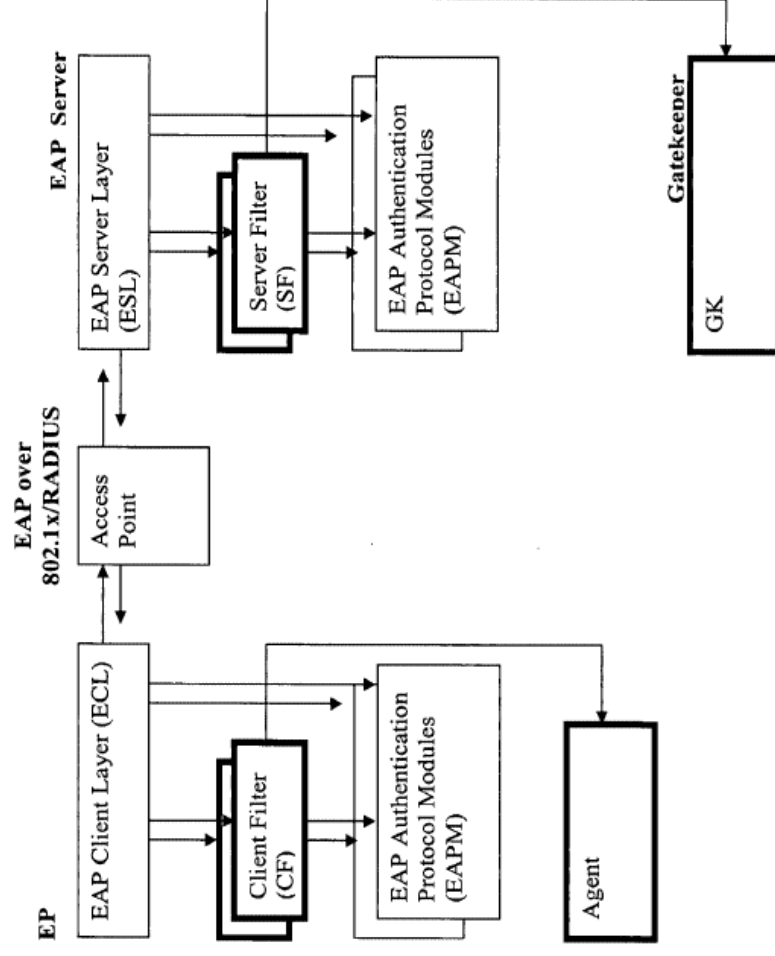
**Invention**

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.

Next, pages 9 through 11 (and Figures 4, 5a, and 5b therein) all describe authentication being conducted, for example by extensible authentication protocol (EAP) and 802.1X authentication:



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.

**Figure 5a: Client in Authentication State**

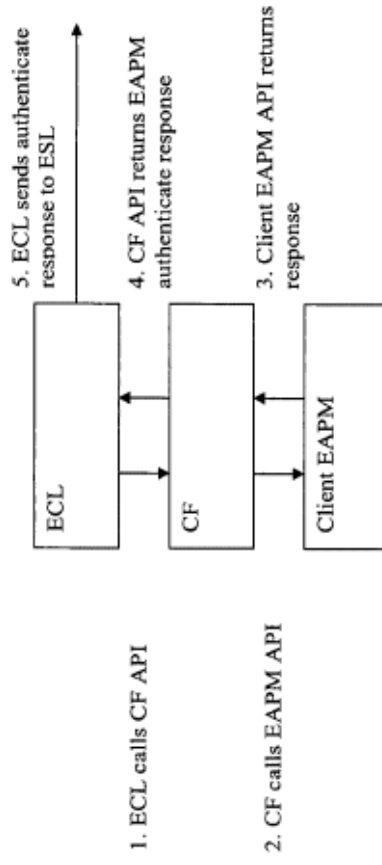
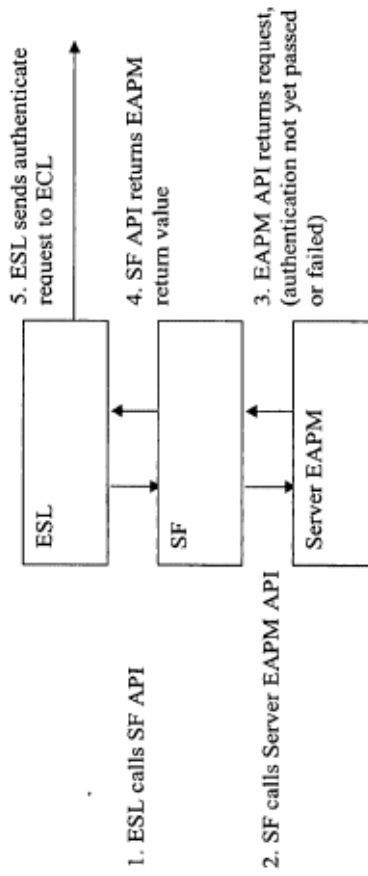


**Figure 5b: Server in Authentication State**



To use the invention, the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method. This authentication method corresponds to an authentication method supported by one of the EAPMs.

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>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.</p> <p>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.</p> <p>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.</p> |
|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

3.

See claim 1.

The provisional provides several examples of “obtaining system data from the access device[.]” For example, 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” can constitute “system data from the access device.”

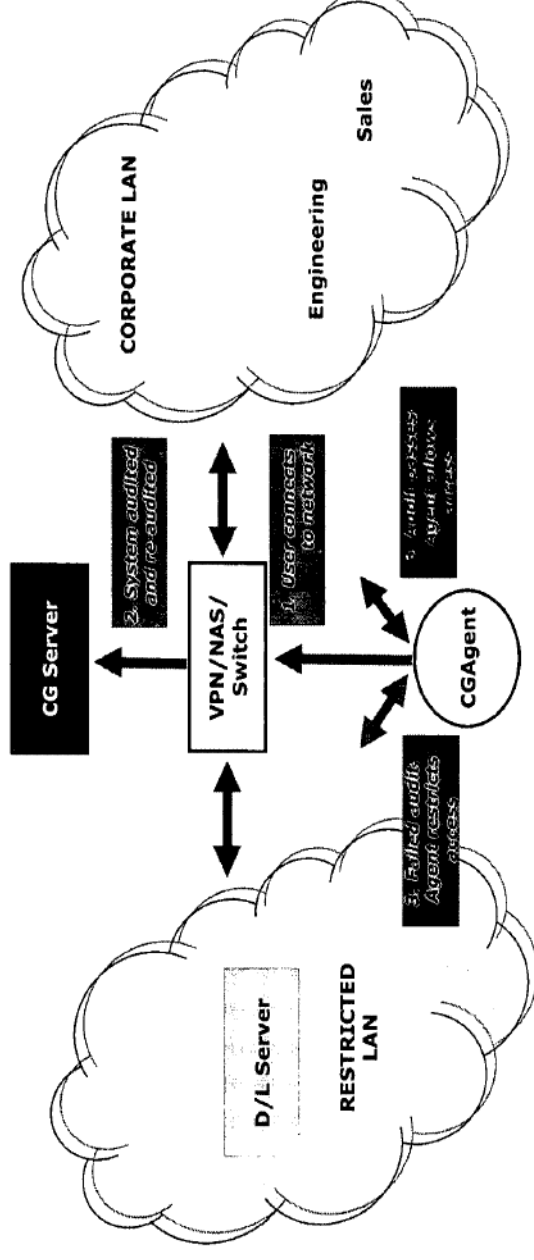
The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server’s ESL, SF, and EAPM. This process continues until 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.

The appendix figure on page 21 further states that the “*system* [is] audited and re-audited[.]” This reference to the device’s system further suggests “system data” that the gatekeeper uses to audit that device.

## Audit Mode Client Side Enforcement



(c) 2003 InfoExpress, Inc.

Additionally, the references to the types of device information used in prior art access control systems—e.g. that regarding the device’s “applications [and] configurations” (pages 4, 5)—means that a POSITA would understand that in the present invention too, “obtain[s] system data from the access device[.]”

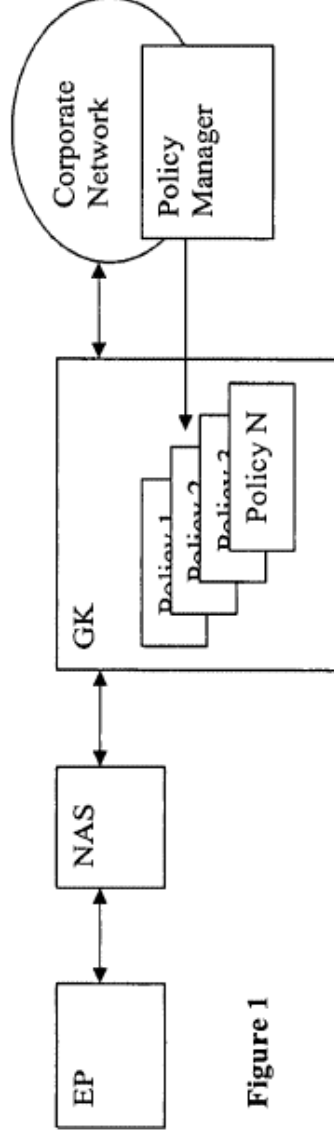


**Figure 1**

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.

Next, the provisional discloses “wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.” As described above for claims 1.2 and 1.3—“applying a security policy to the access device in response to the request; [and] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device”—the provisional provides several examples of using the CG server (i.e. the gatekeeper) to audit the endpoint device based on its audit data. Similarly, these excerpts further support this portion of the claim.

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>4.</p> | <p>See claims 1 and 3.</p> <p>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 status.”</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Additionally, the references to the types of device information that were absent from prior art access control systems—e.g. that regarding 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 status.”</p> |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. | <p>See claim 1.</p> <p>As described above with respect to claim 3, the provisional discloses “obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.”</p> <p>The provisional further discloses “communicating between the gatekeeper and an agent executing on the access device to obtain” information, including system data. For example, page 8 discloses “[an] auditing protocol [that] takes place between the EP agent software and the [gatekeeper]”—and thus “communicating between the gatekeeper and an agent executing on the access device[.]” Page 8 further states, “[a] client filter redirects calls for audit information to an agent on the EP and sends the responses”—that is the system data—ultimately to the gatekeeper. Finally, page 8 states “[t]he GK sends requests for more information on the reverse path and this continues until the audit is completed.” This shows “applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.”</p> |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Invention</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The provisional further details how the system uses an agent to obtain information, including system data, for the gatekeeper to use in "determin[ing] that the access device satisfies the requirements of the security policy." See, e.g., pages 12-13:</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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**

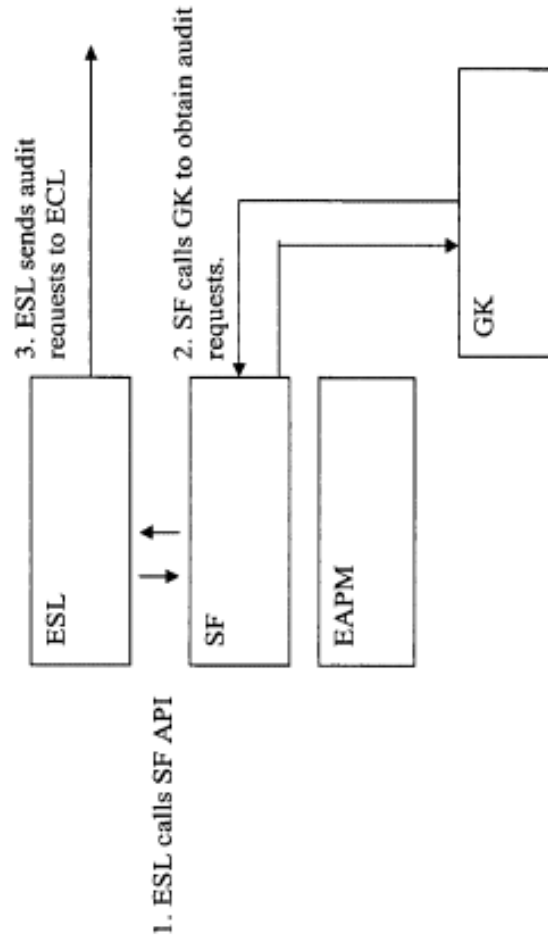
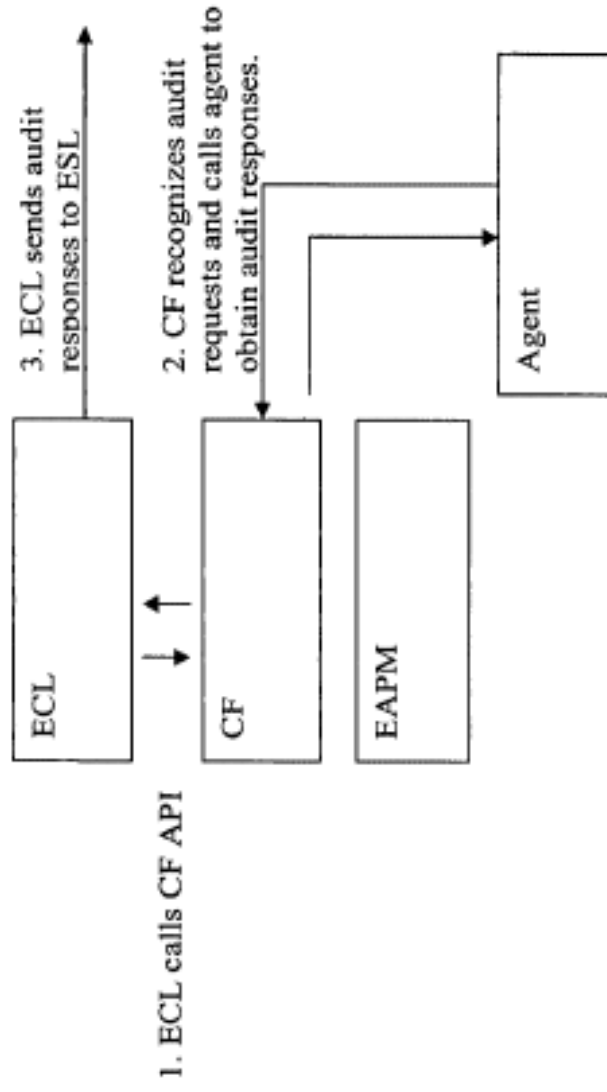


Figure 7b: Client Responding to Audit Requests



|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>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.</p> <p>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.</p> <p>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.</p> |
|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <p>6. See claims 1 and 5.</p> <p>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” could “include[] information regarding devices connected to the access device.”</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Additionally, the references to the types of device information that were present in certain prior art access control systems—e.g. that regarding device “applications, configurations, and user logins” (page 4)—means that a POSITA would understand that in the present invention too, “the system data includes information regarding devices connected to the access device.”</p> |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>10. The method of claim 1, wherein the access point is a network switch.</p> | <p>See claim 1.</p> <p>The provisional provides several instances “wherein the access point is a network switch.” Page 1 defines an access point (“AP”) to be “A <b>switch</b> 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 802.11 a or 802.11 b.” The provisional refers to APs throughout the text.</p> <p>ND –Network device such as a network printer, which is normally incapable of running an agent.</p> <p>EP – End point which can be a PC or ND.</p> <p>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.</p> <p>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.</p> <p>Also, the appendix figures on pages 19-21 all disclose a “switch” as the access point through which the access device connects to the network:</p> |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The diagram illustrates the LAN Mode architecture and traffic flow. It shows two main network segments: the **CORPORATE LAN** and the **RESTRICTED LAN**.

- CORPORATE LAN:** Contains departments like **Engineering** and **Sales**. It includes a **CGServer** and a **Switch**.
- RESTRICTED LAN:** Contains a **D/L Server** and is connected to the **Switch** in the Corporate LAN.
- CGAgent:** A component that connects to the **Switch** and enforces security policies.

**Traffic Flow and Security Policies:**

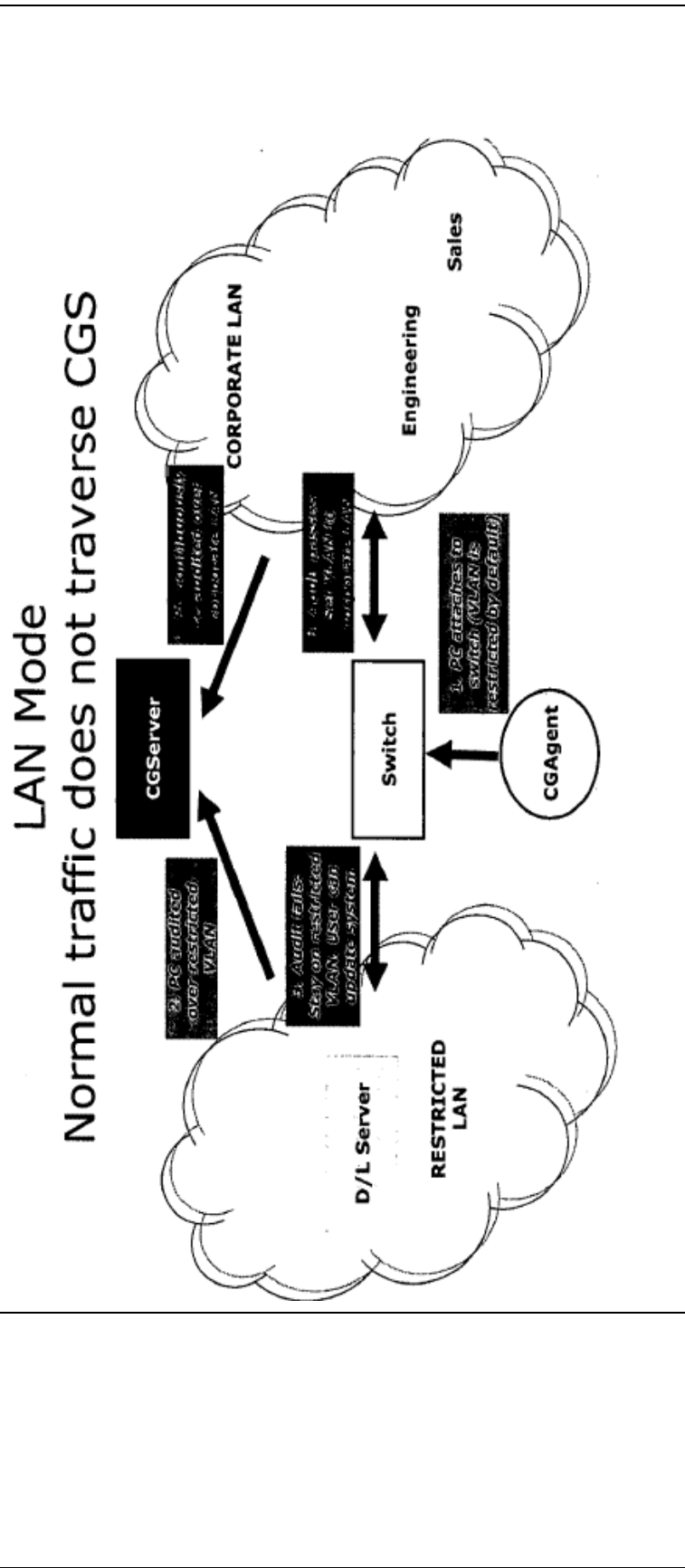
- Outgoing Traffic (Corporate LAN to Internet):**
  - Step 1: PC attaches to switch (VLAN is restricted by default).
  - Step 2: PC audited (over-restricted VLAN).
  - Step 3: Audit fails. Stay on restricted VLAN. User can update system.
- Incoming Traffic (Internet to Corporate LAN):**
  - Step 1: Audit process. Stay on D/L VLAN.
  - Step 2: Audit fails. Stay on restricted VLAN.

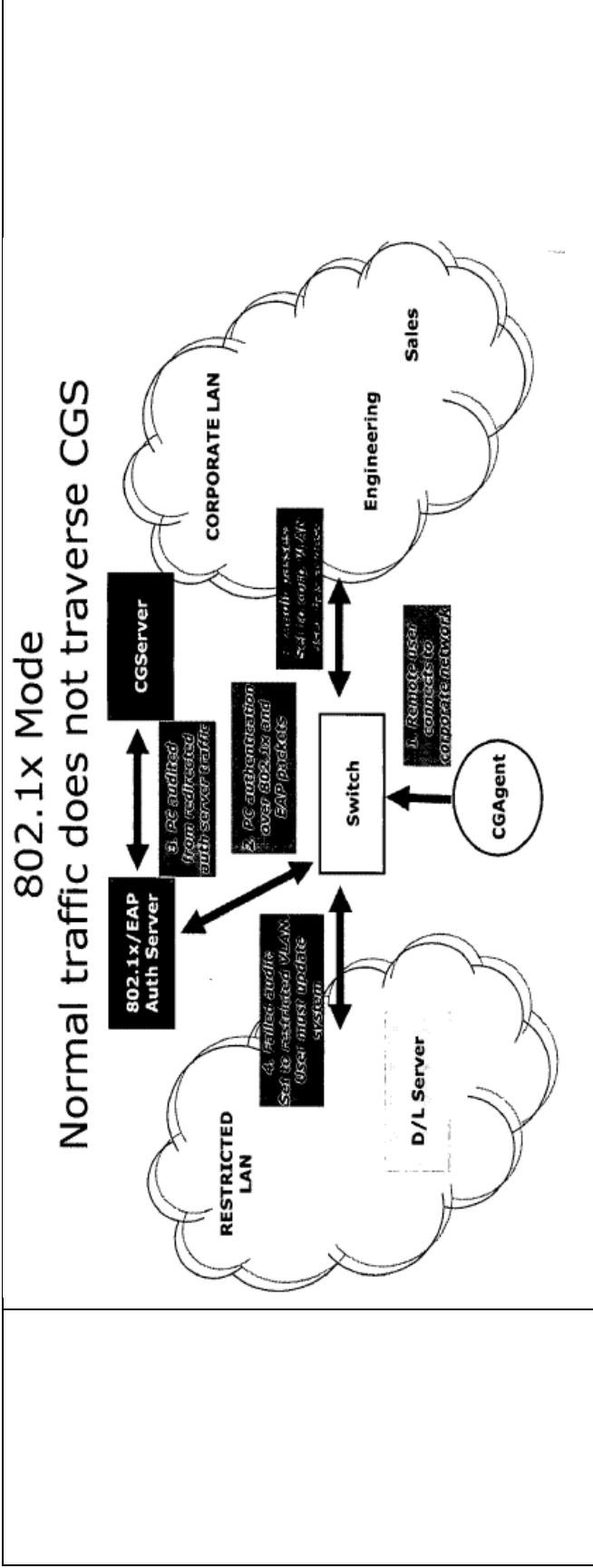
**Key Security Features:**

- CGServer:** Manages security policies and audits traffic.
- Switch:** Enforces VLAN restrictions and manages traffic flow.
- CGAgent:** Monitors and enforces security policies on the network.

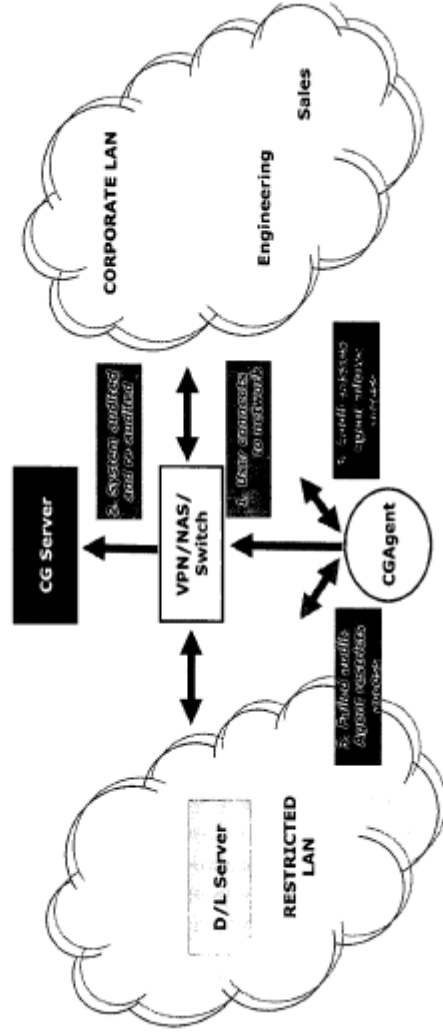
The diagram illustrates the LAN Mode architecture and traffic flow. It shows two network clouds: the **CORPORATE LAN** (top) and the **RESTRICTED LAN** (bottom). The **CORPORATE LAN** contains departments like **Engineering** and **Sales**. The **RESTRICTED LAN** contains a **D/L Server**. A central **Switch** connects these two networks. A **CGServer** is connected to the Corporate LAN, and a **CGAgent** is connected to the Restricted LAN. Arrows indicate traffic flow: from the Restricted LAN to the CGServer and from the CGServer to the Corporate LAN. Security restrictions are noted in boxes:
 

- CGServer:** 1. PC attaches to switch (VLAN is restricted by default); 2. PC audited (over restricted VLAN); 3. Audit fails: Stay on restricted VLAN. User can update system.
- Switch:** 1. Audit process: Stay on restricted VLAN. User can update system.
- CGAgent:** 1. PC attaches to switch (VLAN is restricted by default).





## Audit Mode Client Side Enforcement

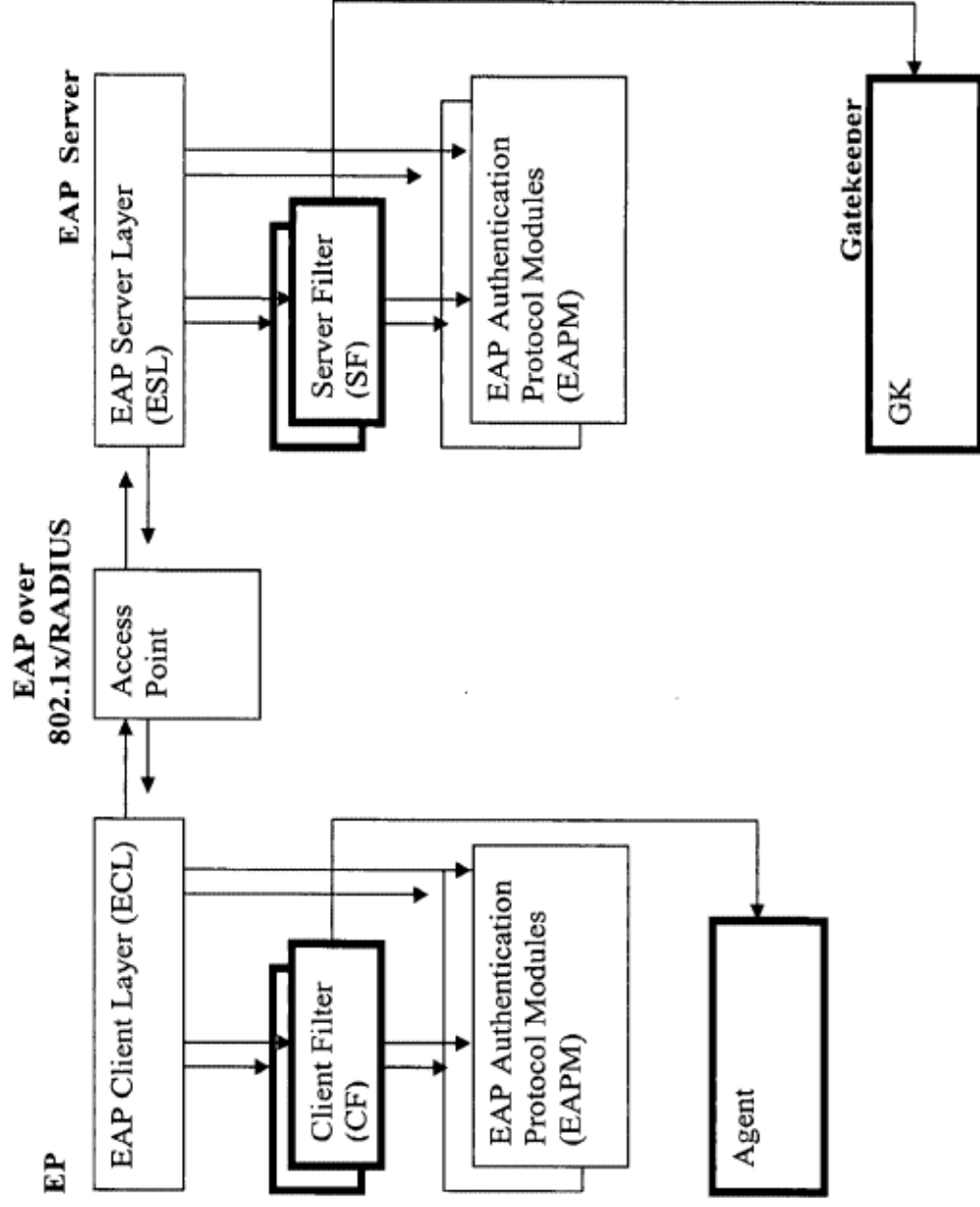


(c) 2003 InfoExpress, Inc.

6

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>11.</p> | <p>See claim 1.</p> <p>The provisional provides several instances “wherein the access point is a network switch.” Page 3 defines an access point (“AP”) to be “A <b>switch</b> 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 802.11 a or 802.11 b.” The provisional refers to APs throughout the text.</p> <p>ND –Network device such as a network printer, which is normally incapable of running an agent.</p> <p>EP – End point which can be a PC or ND.</p> <p>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.</p> <p>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.</p> <p>The specification’s references to “access point(s),” for example in Figure 4 (page 9), thus include reference to wireless access points by virtue of the definition on page 3:</p> |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

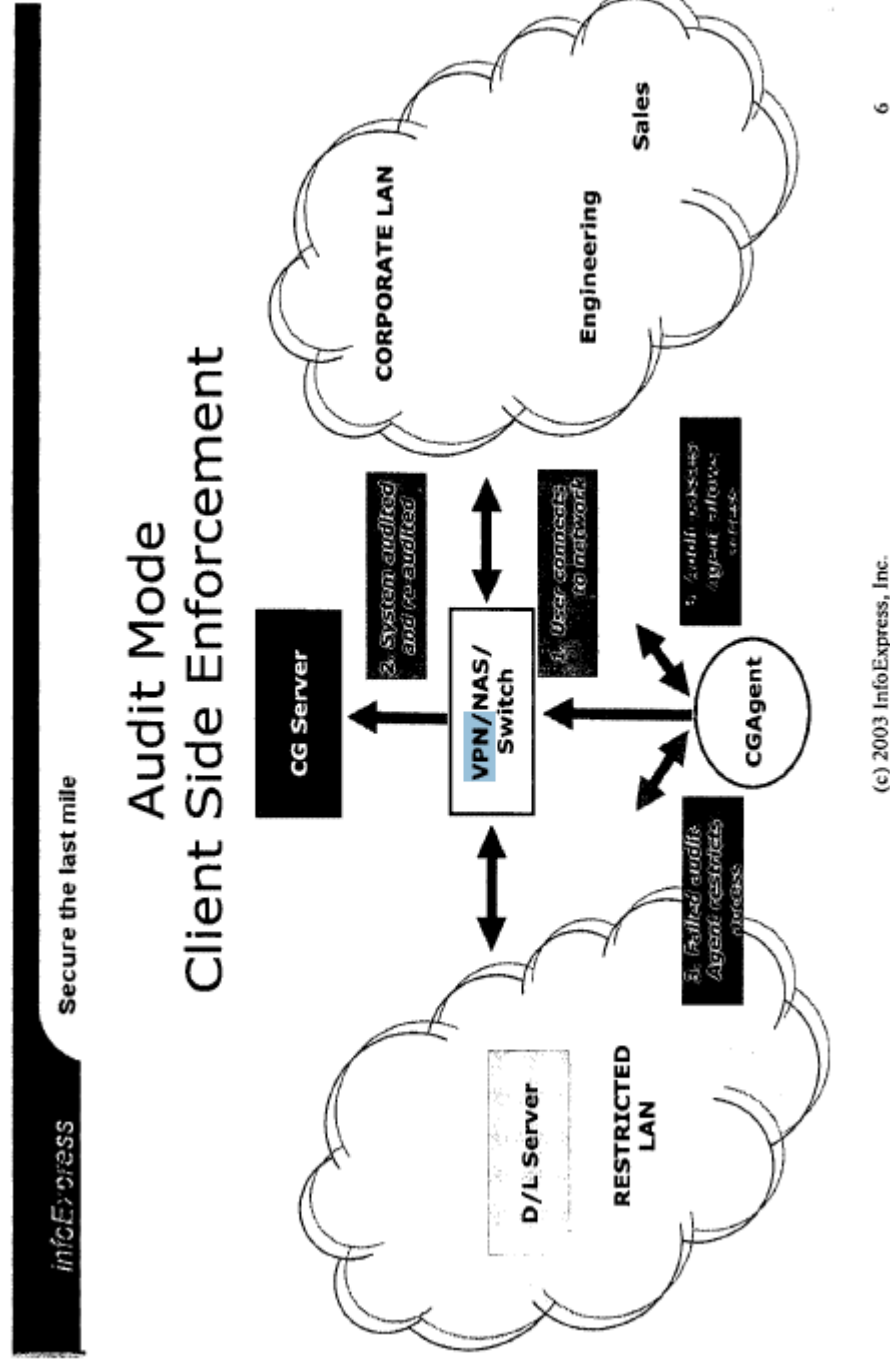
**Figure 4**



12.

See claims 1 and 10-11.

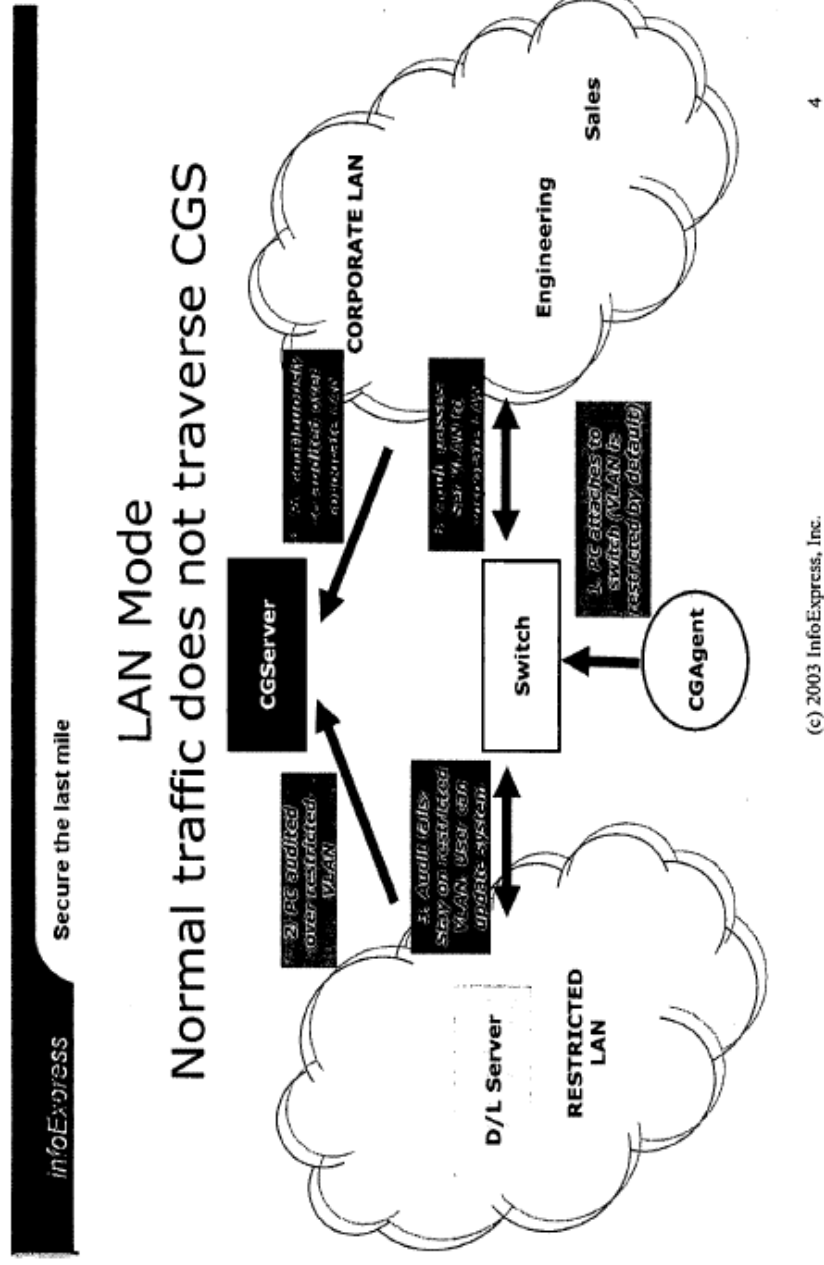
The appendix figure on page 19 shows a virtual private network (VPN), and thus shows “wherein the access point is a remote access virtual private network.”



13.

See claim 1.

The schematic in the appendix figure on page 19 shows a CyberGatekeeper Server—the claimed “gatekeeper”—with an arrow connecting it to the Corporate LAN—the claimed “less-restricted subset of the protected network.” The figure further states that the endpoint is “continuously audited over the corporate LAN.” In other words, while the endpoint has access to the Corporate LAN, the gatekeeper can still audit that endpoint. Thus, this figure supports “wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network.”



14.

See claim 1.

The provisional provides at least two portions “wherein the restricted subset of the protected network is characterized by an access control list.” On page 3, access control list (ACL) is described as “a set of filtering rules that specify what traffic is permitted through a port.” Because the ACL “specif[ies] what traffic is permitted through a port”—and thus to which parts of the network an endpoint can access—“the restricted subset of the protected network is characterized by an access control list.”

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.

Page 14 further states, “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” Because an ACL can provide full or limited access to the corporate network—that is, the “less restricted” subset—it follows that the ACL similarly “characterize[s]” the “restricted subset.”

|                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                      | <p style="text-align: center;">12</p> <ol style="list-style-type: none"> <li>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</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol> <p>Details of exemplary enforcement modes of the invention are given in the attached Appendix.</p> |
| <p><b>16 (Preamble):</b> A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising:</p> | <p>See claim 1 (Preamble), which describes how the specification discloses a “method of granting access to a protected network . . .”</p> <p>Additionally, the provisional discloses “[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network . . .” For instance, the GK is defined as “<i>software</i> 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.” Page 3. A POSITA would understand that the “software” comprises “[a] non-transitory computer-readable storage medium having stored thereon a program . . .”</p> <p><b>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.</b></p>                                                                                                                                |

|                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>16.1:</b> 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</p> | <p>See claim 1.1, which discloses “[a] receiving a request for access to a less-restricted subset of the protected network from an access device, [b] the request received through a communication port of an access point, [c] the communication port configured for communicating between the access device and a restricted subset of the protected network, [d] the restricted subset including a gatekeeper[.]”</p> |

|                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| the protected network, the restricted subset including a gatekeeper,                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                             |
| <b>16.2:</b> applying a security policy to the access device in response to the request; and                                                                                                                                                                            | See claims 1.2 and 1.3, which disclose “applying a security policy to the access device in response to the request; [and] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device[.]”                                                   |
| <b>16.3:</b> 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, when the requirements of the security policy are satisfied. | See claim 1.4, which 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, when the requirements of the security policy are satisfied.” |
|                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                             |
| <b>17.</b>                                                                                                                                                                                                                                                              | See claim 16 and also claim 2, which discloses “further comprising authenticating a user of the access device.”                                                                                                                                                                             |
|                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                             |

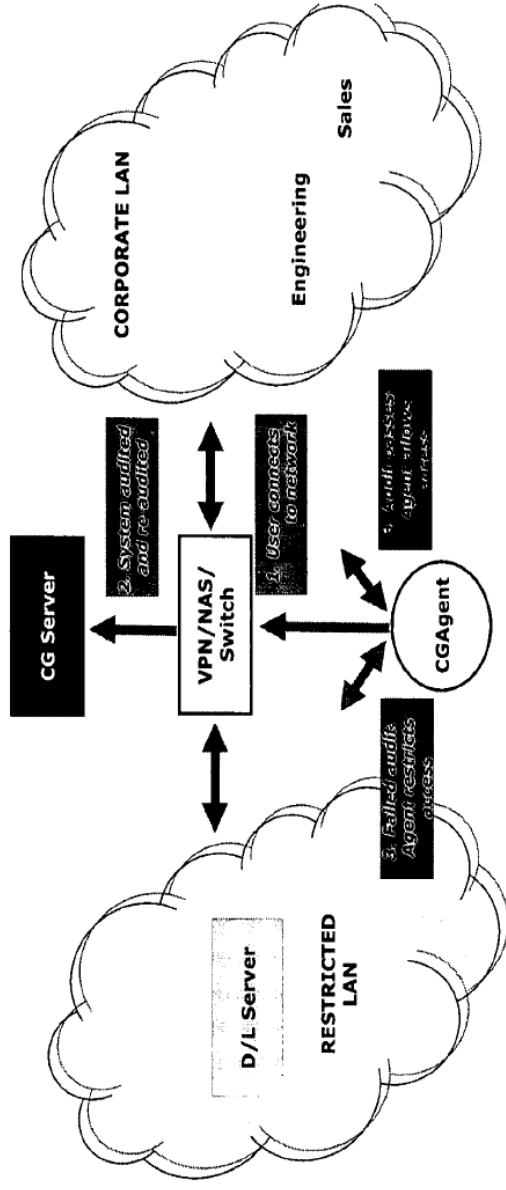
|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>18.</b> | See claim 16 and also claim 3, which discloses “further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>19.</b> | <p>See claims 16 and 18 and also claim 4, which discloses “wherein the system data includes antivirus software status.”</p> <p>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” may include “system data includ[ing] antivirus software version data.”</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The provisional also recognizes that certain prior art systems, like Cisco’s VMPS system, were inadequate in that they did not detect “EPs hav[ing] security vulnerabilities or EPs that ha[d] been breached (i.e., may have</p> |

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <p><i>a virus</i> or trojan running on them)[.]” Pages. 5-6. This shortcoming in the prior art means that a POSITA would understand that in the present invention too, “the system data includes antivirus software version data.”</p> <p>A problem with this system is that it does not check whether or not the applications and configuration on the EP comply with corporate security policies. This means that users whose EPs have security vulnerabilities or EPs that have been breached (i.e., may have a virus or trojan running on them) can access the corporate network.</p> |
| <b>20.</b> | <p>See claims 16 and 20, and also claim 5, which discloses “further comprising 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 that the access device satisfies the requirements of the security policy.”</p>                                                                                                                                                                                                         |
| <b>21.</b> | <p>See claims 16, and 20, and also claim 6, which discloses “wherein the system data includes information regarding devices connected to the access device.”</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>22.</b></p> | <p>See claim 16 and also claim 5, which discloses “further comprising 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 that the access device satisfies the requirements of the security policy.”</p> <p>Furthermore, the excerpt from page 13 describes a situation after the audit has been performed, the access device has been found compliant, the access device has been granted access, and the port on the access point has been reconfigured. At such time, “‘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 . . . ”</p> <p>These “updates regarding changes to previous audit information” constitute or suggest the presence of audit data. Per the previous analysis of claim 5, such information can come from “an agent executing on the access device[.]” This excerpt from page 13 thus describes “an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port . . . ”</p> <p>Put differently, “revaluating” these “changes” in audit information to determine if they are “inconsistent with the current state” shows “monitor[ing] security status of the access device [.]”</p> |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>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.</p> <p>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.</p> <p>After the audit has been performed, “keep alive” 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.</p> <p>Further, the appendix figure on page 21 explains the that the “system [is] audited and re-audited” which therefore supports “monitor[ing] security status of the access device after reconfiguring the communication port . . .”</p> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Audit Mode Client Side Enforcement

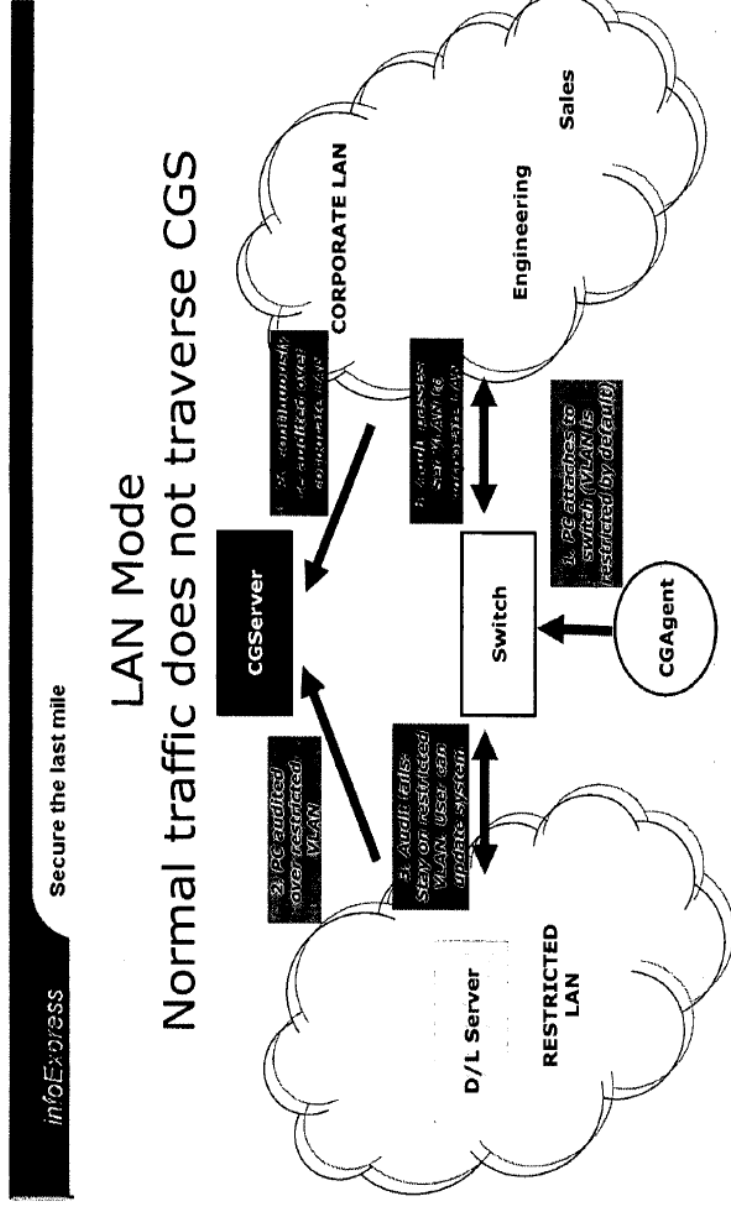


(c) 2003 InfoExpress, Inc.

27.

See claim 16.

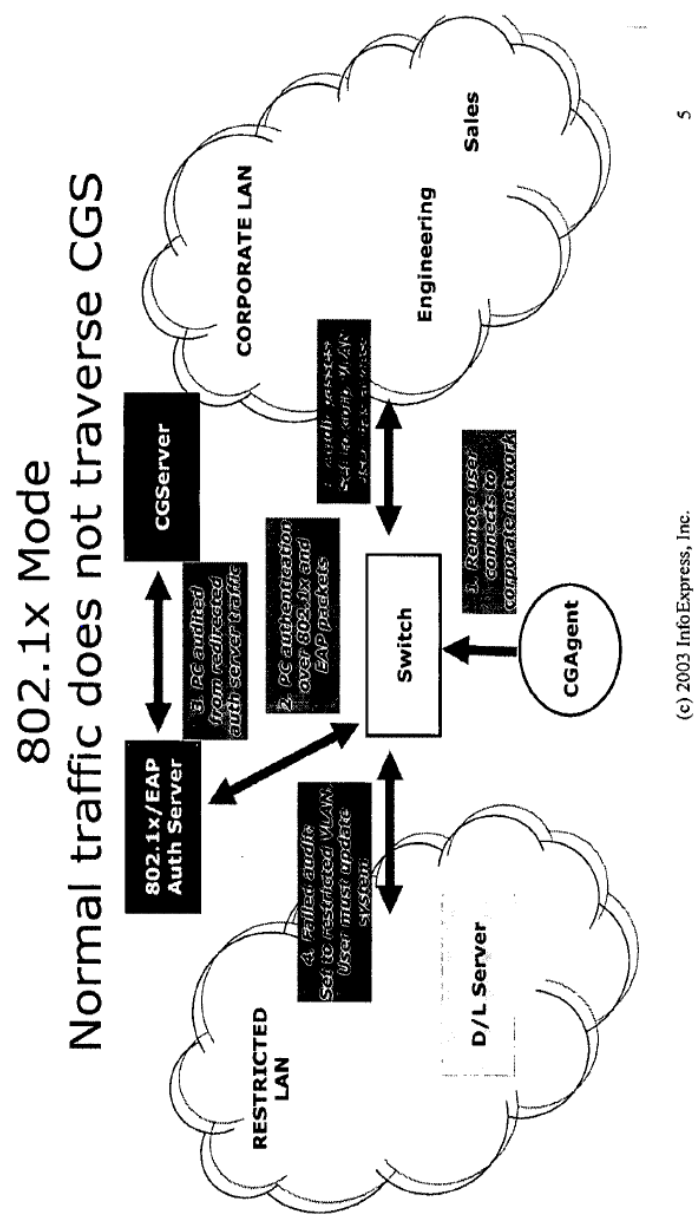
The appendix figure on page 19 supports “wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.” In the event that an “audit fails,” the switch confines the user to “stay on [a] restricted VLAN[.]” where the “user can update [their] system.” Although this depicts a scenario prior to a successful audit and reconfiguration, a POSITA would understand how it could apply after such events. Thus, this shows the “update . . .” element recited by the claim.



(c) 2003 InfoExpress, Inc.

4

The appendix figure on page 20 similarly supports this claim element. In the event of a “failed audit,” the switch is “set to [a] restricted VLAN[.]” where the “user must update [their] system.” Although this figure relates to 802.1X and authentication—which is occurring prior to a successful audit and reconfiguration—a POSITA would understand how this figure could apply after a successful audit and reconfiguration. Thus, this shows the “update . . .” element recited by the claim.



(c) 2003 Info Express, Inc.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>29.</b></p> | <p>See claim 16, and also claim 14, which describes “wherein the restricted subset of the protected network is characterized by an access control list.”</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                   | <p><b>30.</b></p> <p>See claim 16, and also claims 14 and 29, the last two of which describe “wherein the restricted subset of the protected network is characterized by an access control list.”</p> <p>Page 14 further describes one advantage of the present invention as, “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.” This essentially describes using an ACL and VLAN in concert, which provides a greater degree of control over access. Thus, this excerpt supports “wherein access to the restricted subset of the protected network is responsive to a VLAN configured to communicate with the protected network subject to the access control list.”</p> <p style="text-align: center;"><b>12</b></p> <ol style="list-style-type: none"> <li>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</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol> <p>Details of exemplary enforcement modes of the invention are given in the attached Appendix.</p> |