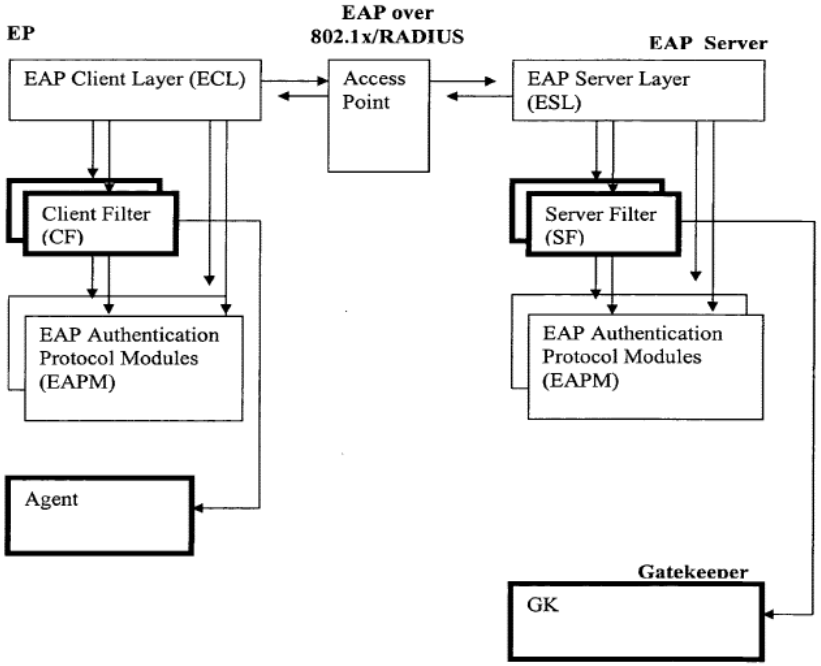
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[1.0] A method for applying a security policy to network devices, the method comprising:	EX2006 verifies that the invention was directed to the claimed "method for applying a security policy to network devices". For example, the description explains "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 with specify the audit criteria . . ." Page 3 **GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x** The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. **Definitions** GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. To access the corporate network, the device must pass both authentication AND an **audit**. ("an AP may be programmed to prohibit access… until authentication with the authentication server passes AND an audit with the software agent with the GK passes…").

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 8 **Invention** According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.
[1.1] performing an authentication of a device connected to an access point;	EX2006 describes performing an authentication of a device connected to an access point. First, page 8 states "an AP [access point] may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes . . ." Page 8 **Invention** According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. Next, pages 9 through 11 (and Figures 4, 5a, and 5b therein) all authentication being conducted, for example by extensible authentication protocol (EAP) and 802.1X authentication:

Page 9



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.

Page 10

Figure 5a: Client in Authentication State

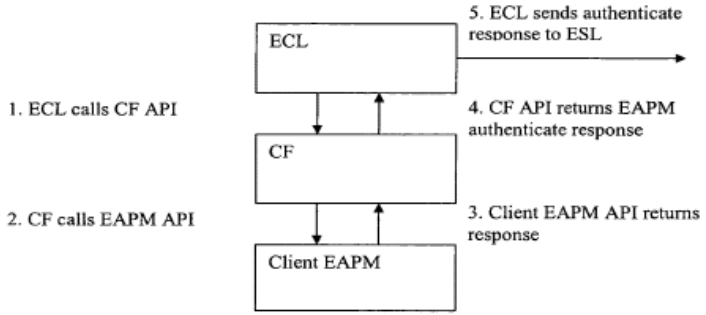
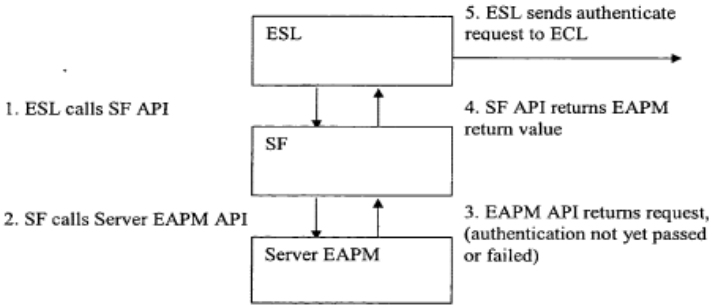


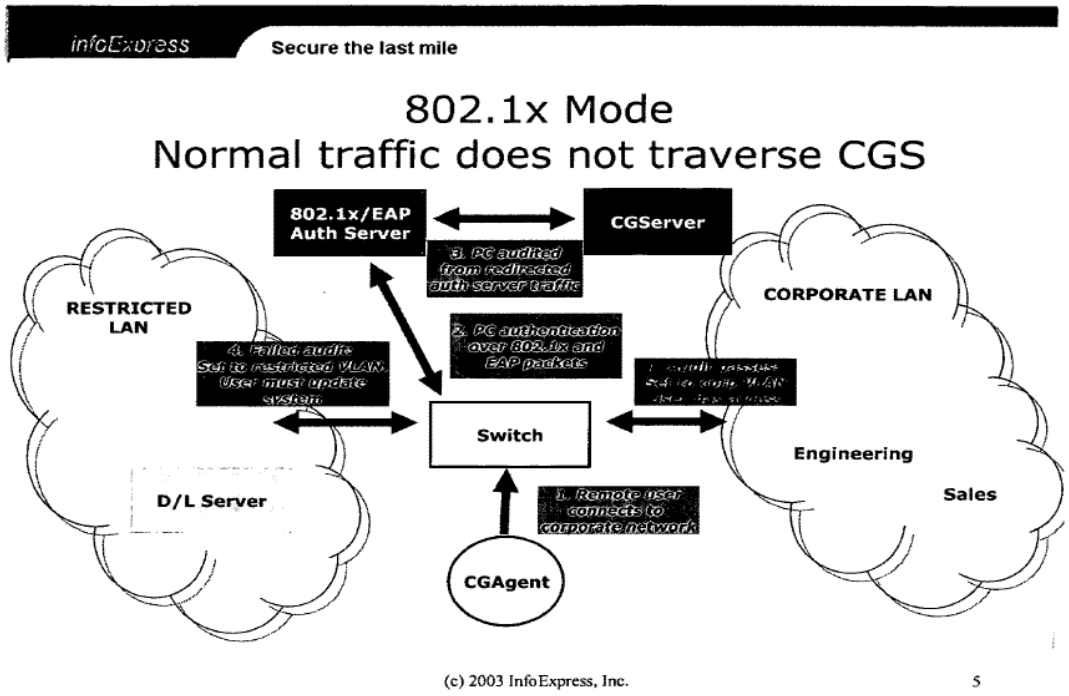
Figure 5b: Server in Authentication State



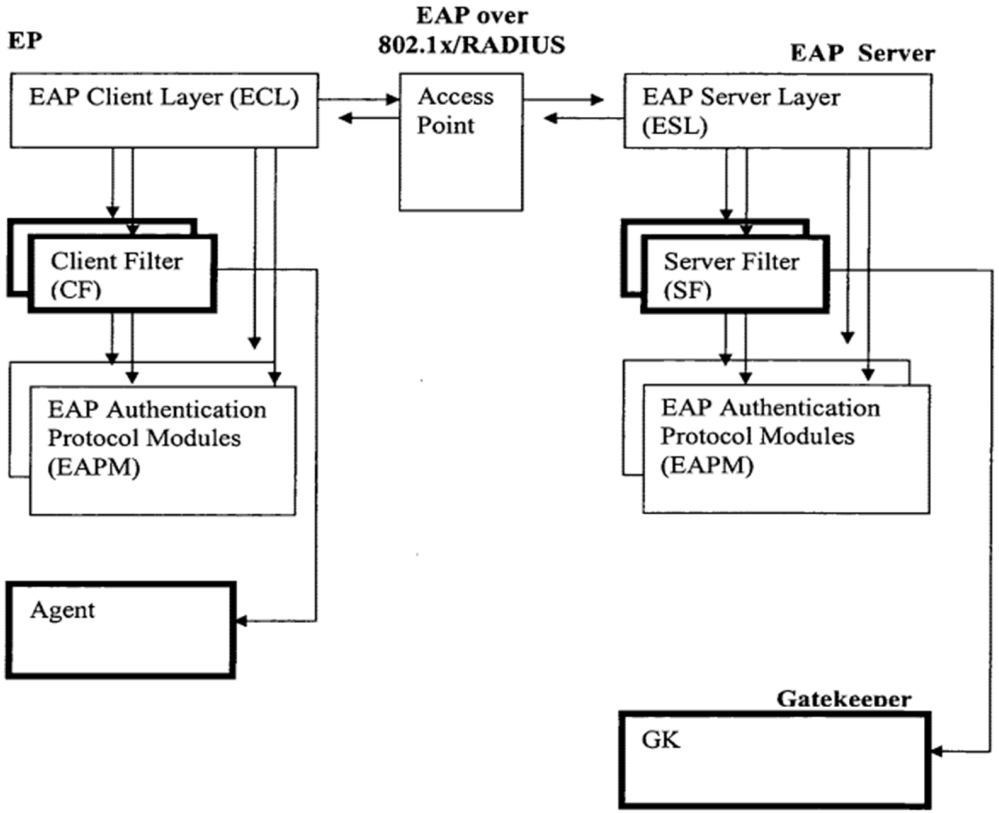
To use the invention, the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method. This authentication method corresponds to an authentication method supported by one of the EAPMs.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 11 The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the appendix at page 20 further describes authentication, in accordance with EAP and 802.1X ("2. PC authentication over 802.1x EAP packets"):

Page 20



In figure 4 (provisional page 9) shows the device (endpoint (EP)) that is performing the authentication is connected to an access point.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 9 **Figure 4** 
[1.2] scanning the device to collect information regarding the device;	The provisional describes scanning the device to collect information regarding the device. For instance, page 8 provides that there is an "auditing protocol" which "calls for audit information," (e.g. information regarding the device) "A client filter redirects calls for audit information . . ."; subsequently the responses to such requests are "sen[t] to the GK

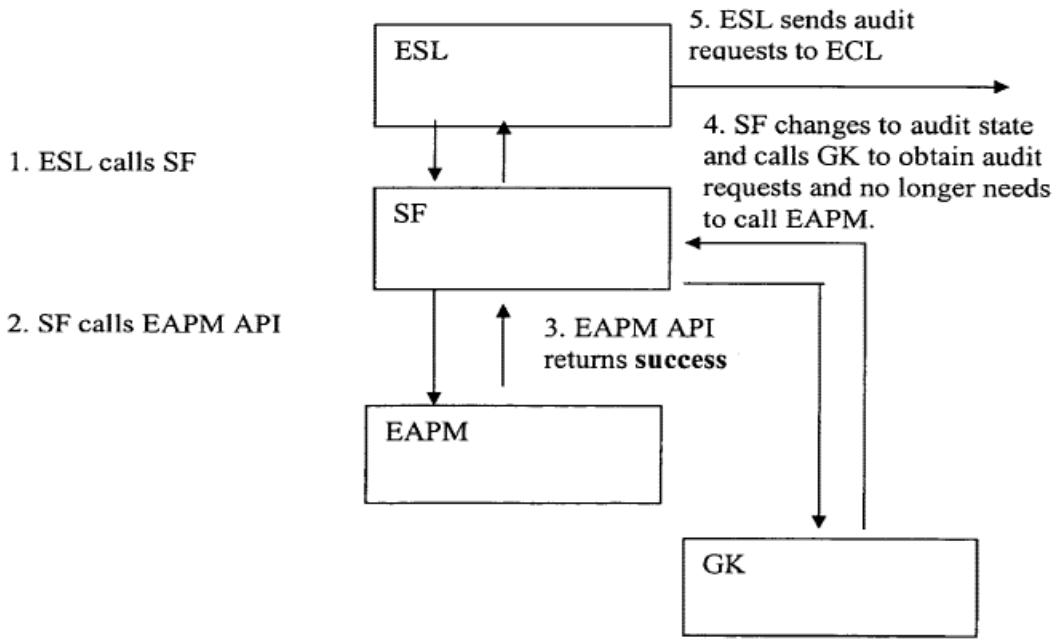
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	[gatekeeper] for evaluation." The information provided by the device, in response to the requested audit information, constitute the results of scanning the device to collect information about the device. Page 8 In the invention, 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. The provisional also supports this limitation by disclosing, on pages 11-13 and Figures 6, 7a, and 7b, that the server filter ("SF") "changes to the audit state and calls GK [gatekeeper] to obtain audit requests to send back to the client." In turn, and on the client side, "audit requests are passed to the agent . . . The agent returns information about the local system, which is converted to audit responses that are sent to the server."

Pages 11-13

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

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

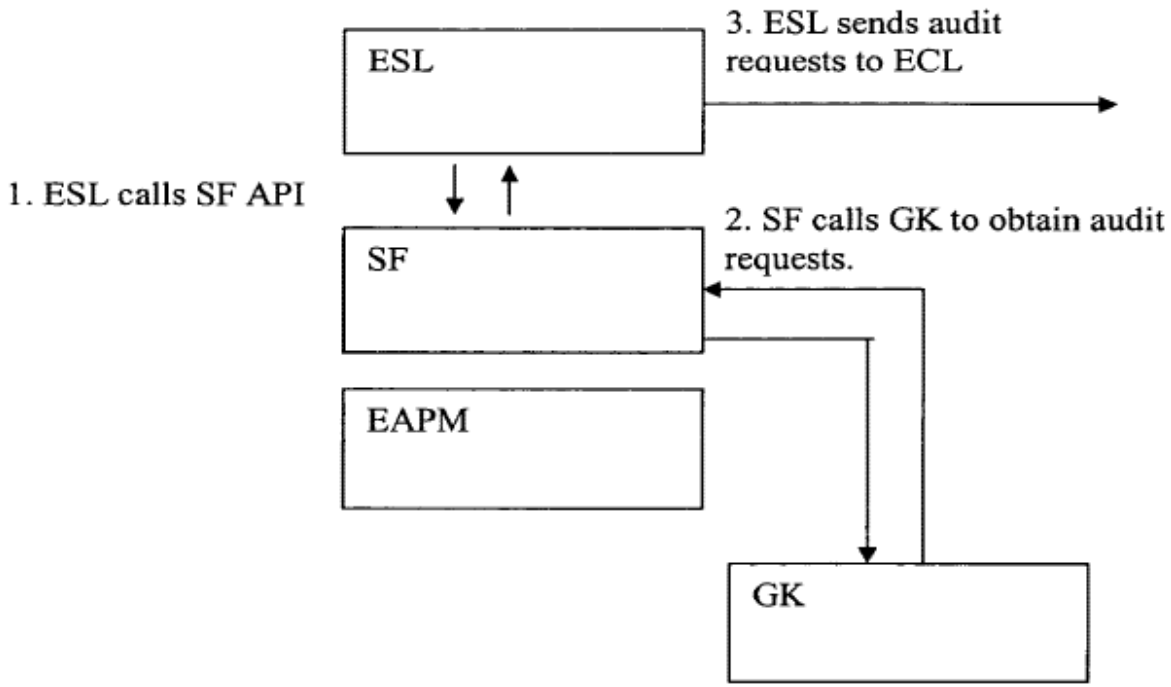
Figure 6: Server Changing to Audit State



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

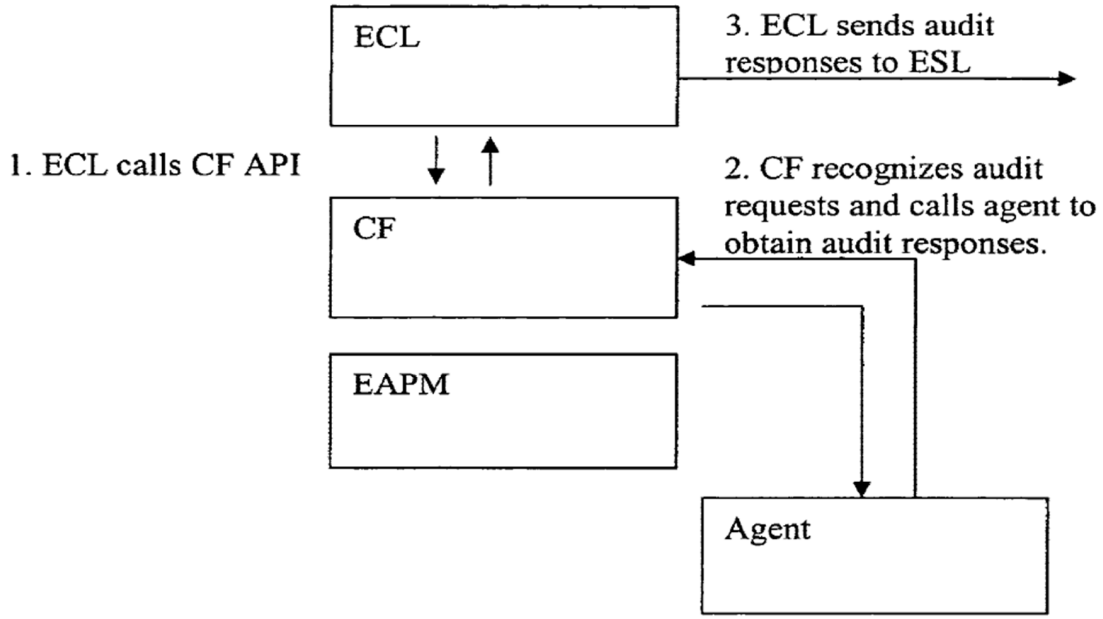
During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF.

Figure 7a: Server in Audit State



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

Figure 7b: Client Responding to Audit Requests



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[1.3] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and	The provisional describes applying a security policy including both authentication and the audit data (the information, see claim element 1.2). The application of this security policy takes place in response to the gatekeeper (called the GK or CGServer). Page 3 The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. **Definitions** GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. First, as noted above with respect to the preamble, the provisional describes "applying a security policy . . ." such as requiring authentication and a audit of the system. Next, the provisional describes "the security policy including one or more requirements pertaining to the authentication and the information." For example, the provisional describes the invention as one where "an AP [access point] 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."

	Page 8 **Invention** According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. This is further detailed in the embodiment on pages 10-13 and Figures 5a, 5b, 6, 7a and 7b, where the server is first in an authentication state, wherein it "obtain[s] the proper authentication response." Once "authentication succeeds" and the server "returns a success response" the server changes to an audit state. Then, a request for information is sent from the gatekeeper to the device and audit information is exchanged between the gatekeeper and the device, until "the audit indicates the client EP [endpoint] is in compliance, the SF returns a success response."

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

Figure 5a: Client in Authentication State

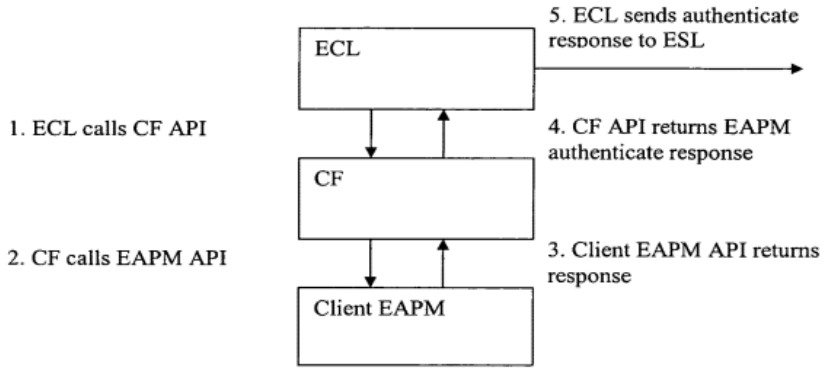
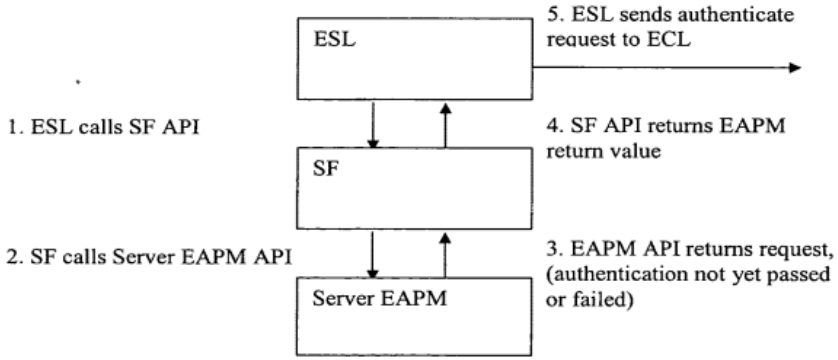


Figure 5b: Server in Authentication State



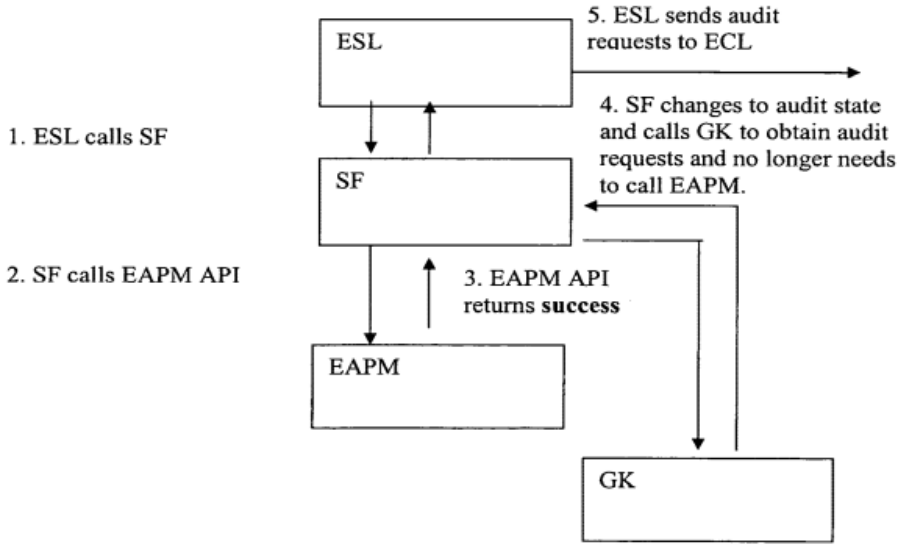
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

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.

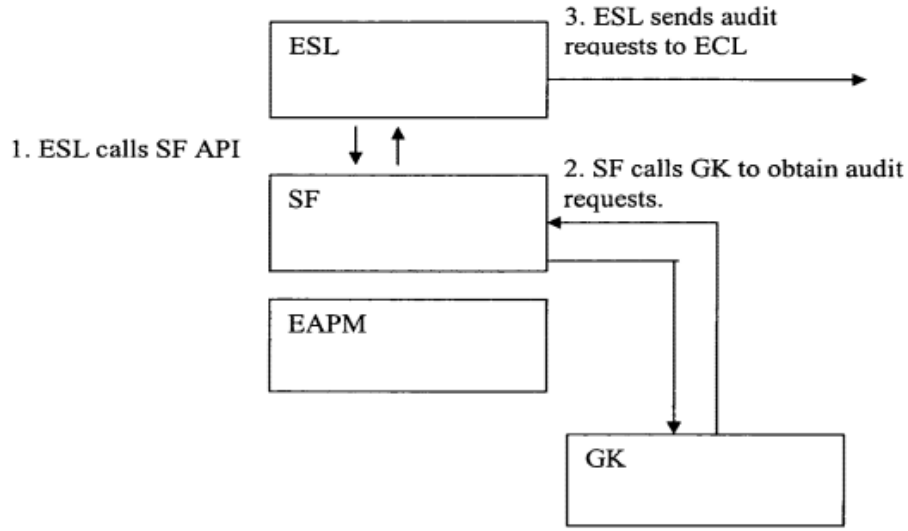
Figure 6: Server Changing to Audit State

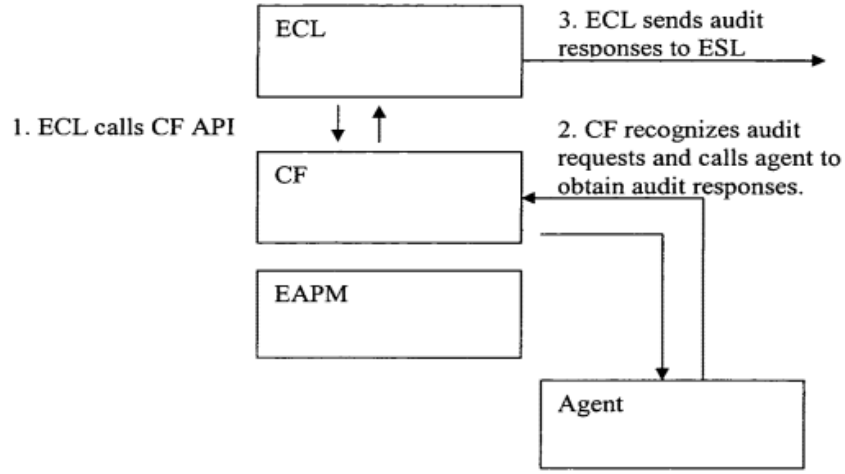


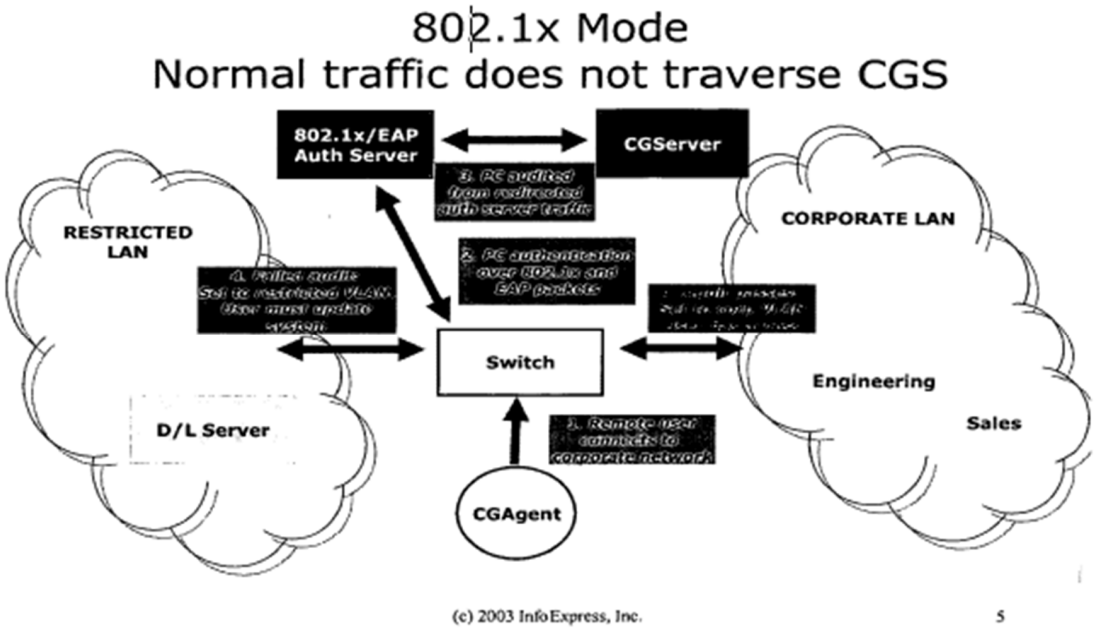
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

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



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Figure 7b: Client Responding to Audit Requests  If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. Page 20 (describing an "802.1x Mode" for authentication, and an "audit mode," both of which are under control of the CG Server, the "gatekeeper."

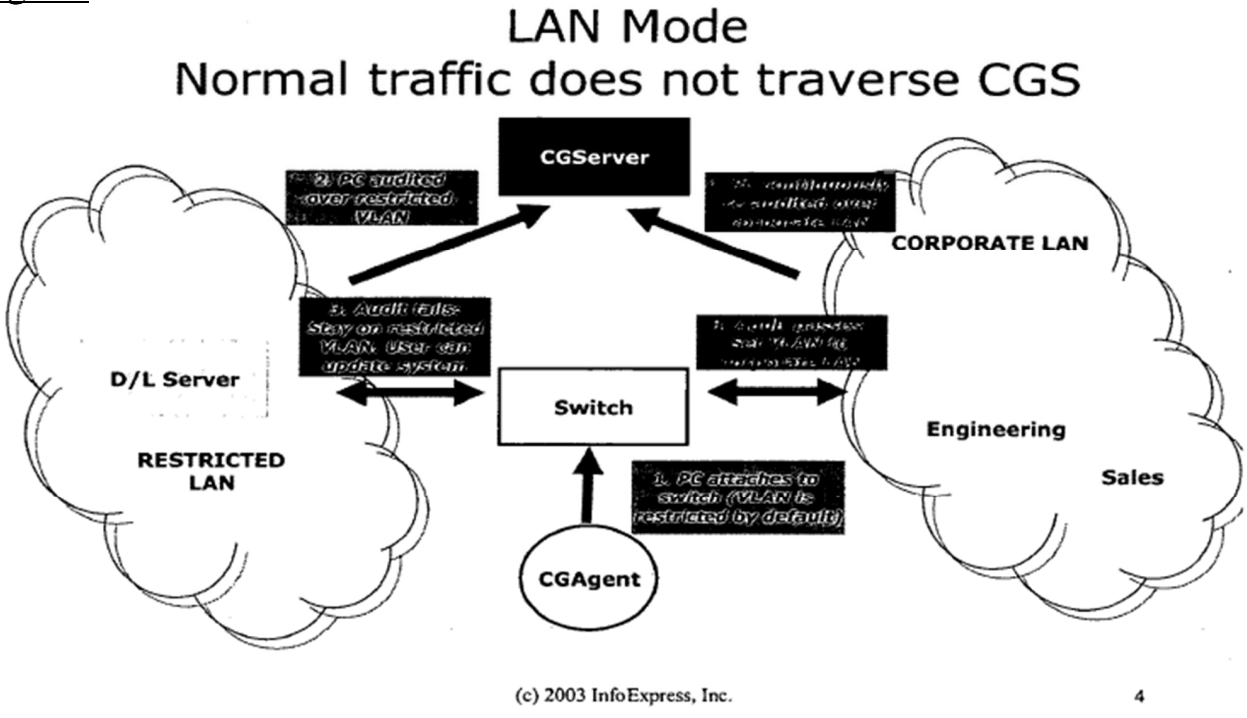
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 
[1.4] configuring the access point in response to a result of applying the security policy.	The provisional includes configuring the access point in response to a result to a result of applying the security policy. Page 8 states, "If the audit is successful, the server sends a message to the AP [access point] which enables the EP's port allowing access for the PC. . . ." This process of "send[ing] a message to an AP" to allow for access shows "configuring" it. Additionally, because this configuring occurs "[i]f the audit is successful," it is thus "in response to a result of applying the security policy."

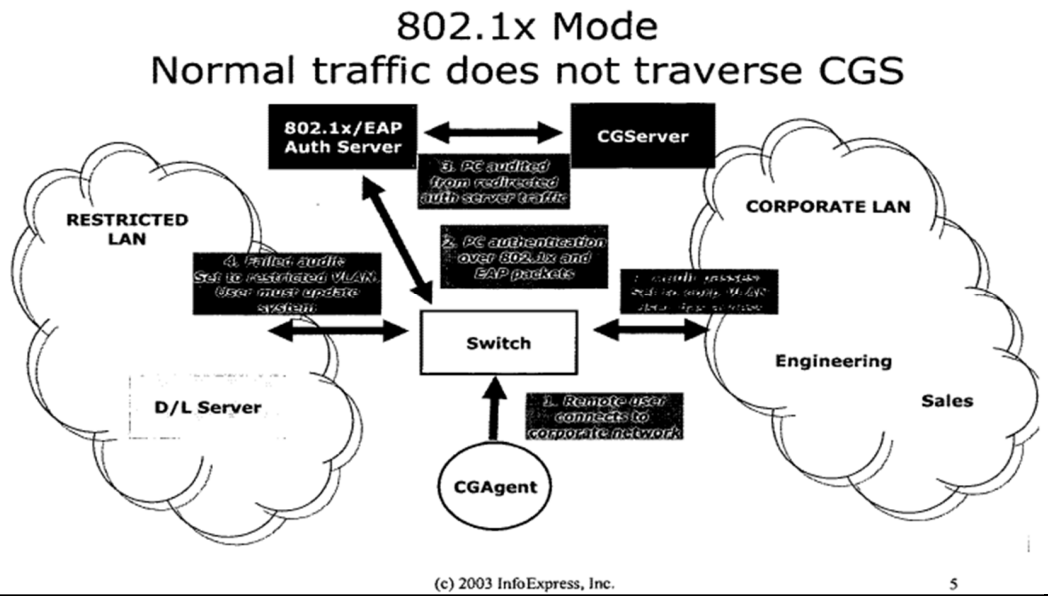
	Page 8 **Invention** According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled. 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 "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 both describe "configuring the access point." Further for this example, the process described can

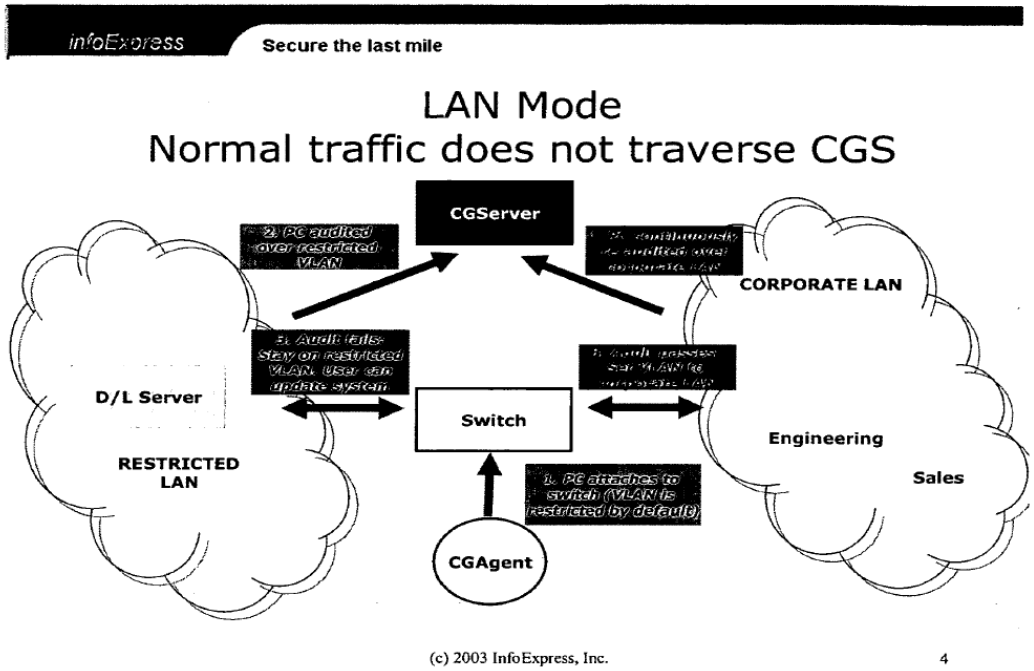
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	take place when "the audit indicates the client EP is in compliance"—that is "in response to a result of applying the security policy." Page 13 If the audit indicates the client EP is in compliance, the SF returns a success 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 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.

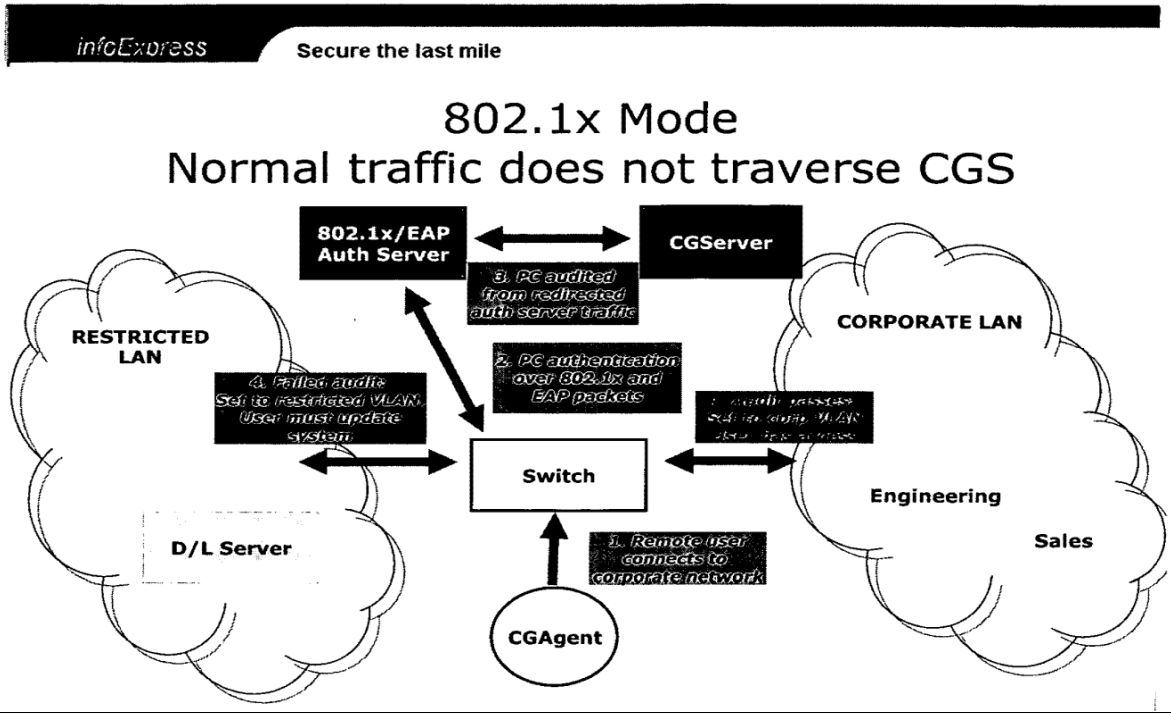
	Page 14 2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP 3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. 5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods. Details of exemplary enforcement modes of the invention are given in the attached Appendix. The appendix figures on page 19-20 further depict this, by showing a switch that can be used to communicate with a "Corporate LAN." Upon a successful audit, the switch is "configure[ed]" ("Audit passes set VLAN to corporate LAN", "Failed audit Set to restricted VLAN") to allow such communication.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 19



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 
[2] The method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.	See [1]. The gatekeeper facilitates updates by leaving the device on the restricted LAN with the download server where, per Page 20, box 4, "User must update system" and can do so via D/L Server. In the event of a failed audit, the "Audit fails Stay on restricted VLAN User can update system". When the system is informed by the CGServer that it failed the audit, the user then knows to update their system. Additionally, the figure contains a "D/L Server" as part of the Restricted LAN. "D/L" is an abbreviation of "download," and furthermore, such a download server would provide updates to the software on that user device (which the user

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	would download to their device). Thus, the figure depicts "facilitating updates" recited by the claim. Additionally, the CG Server—that is, the gatekeeper—signifies that "facilitating updates" is done "in response to applying the security policy, using the gatekeeper." The user "can" (page 19) or "must" (page 20) update their system. <u>Page 19</u> 

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 
[3] The method of claim 1, wherein configuring the access point includes setting an access control list on the access point.	See [1]. The provisional supports "wherein configuring the access point includes setting an access control list on the access point." It explains that an access control list ("ACL") "is a set of filtering rules that specify what traffic is permitted through a port," and further explains that the ACLs can be used to configure the access point:

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 8 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. It further describes "setting the port to the VLAN whose router interface has the desired ACL." "Setting the port to the VLAN whose router interface has the desired ACL" is a way of "setting an access control list on the access point," and thus "configuring" the access point: Page 12 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.
[4] The method of claim 1, wherein configuring the access point includes assigning a VLAN.	*See* [1] including [1.4] including the discussion on configuring the access point and VLANs. The provisional includes "configuring the access point includes assigning a VLAN." Page 13 describes how "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." ***Specifying a VLAN*** and ***passing it back*** are ways of "assigning a VLAN," and also

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	"configuring the access point." We further know from the next page (14) that "setting the port to the VLAN" is yet another description of "assigning a VLAN." 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 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.

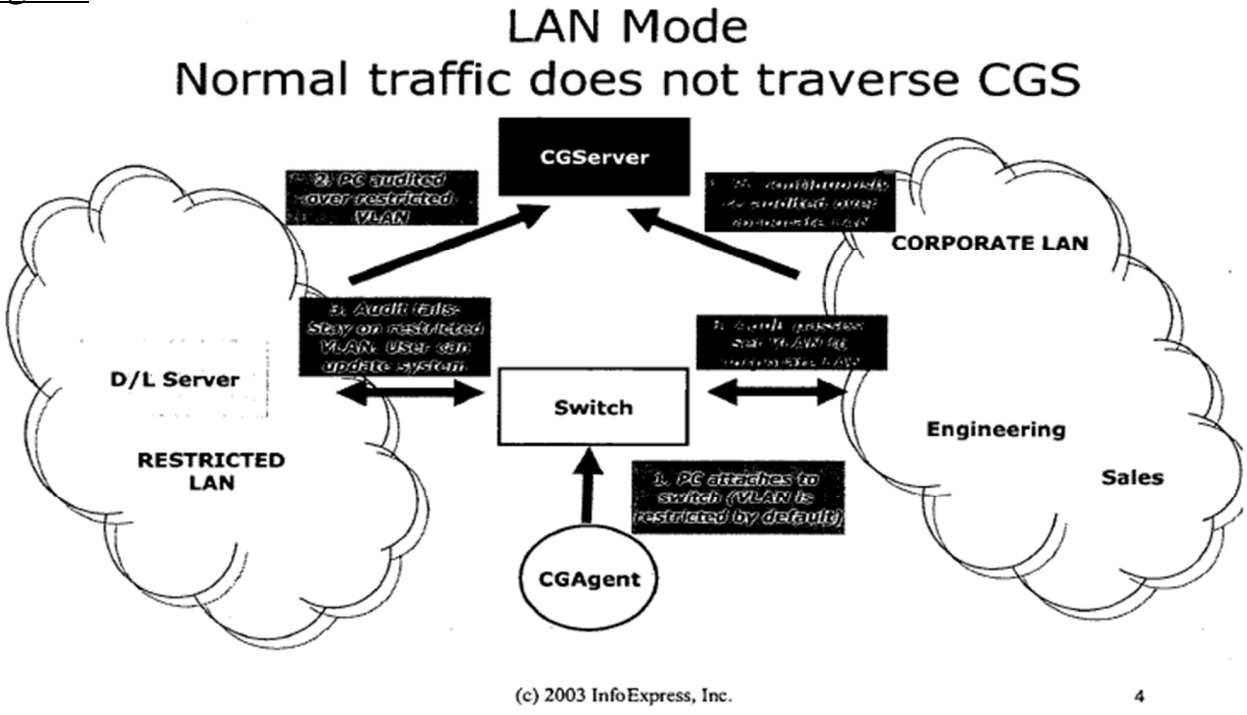
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

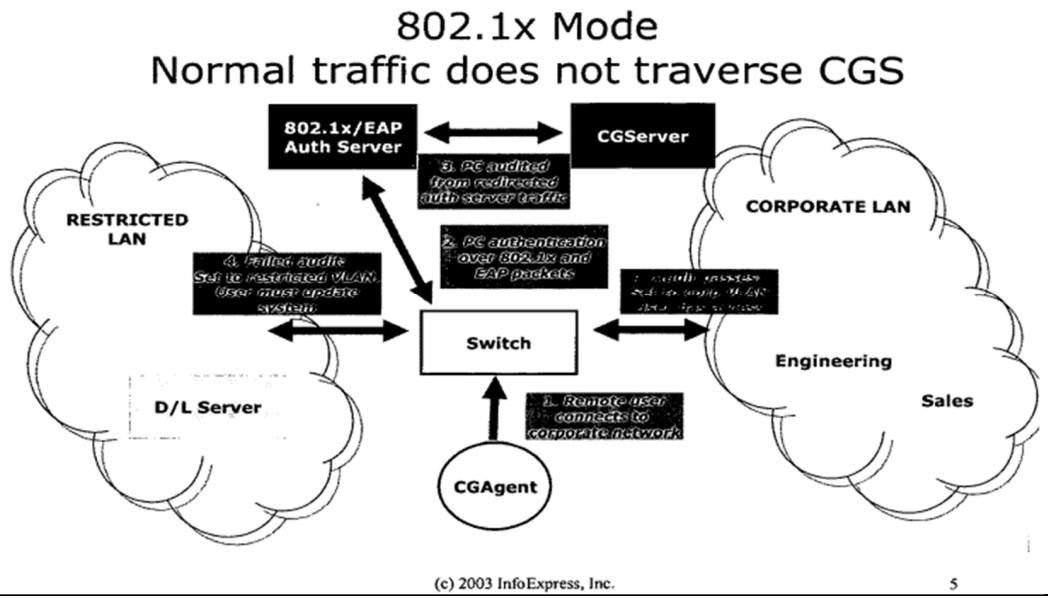
2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from 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.

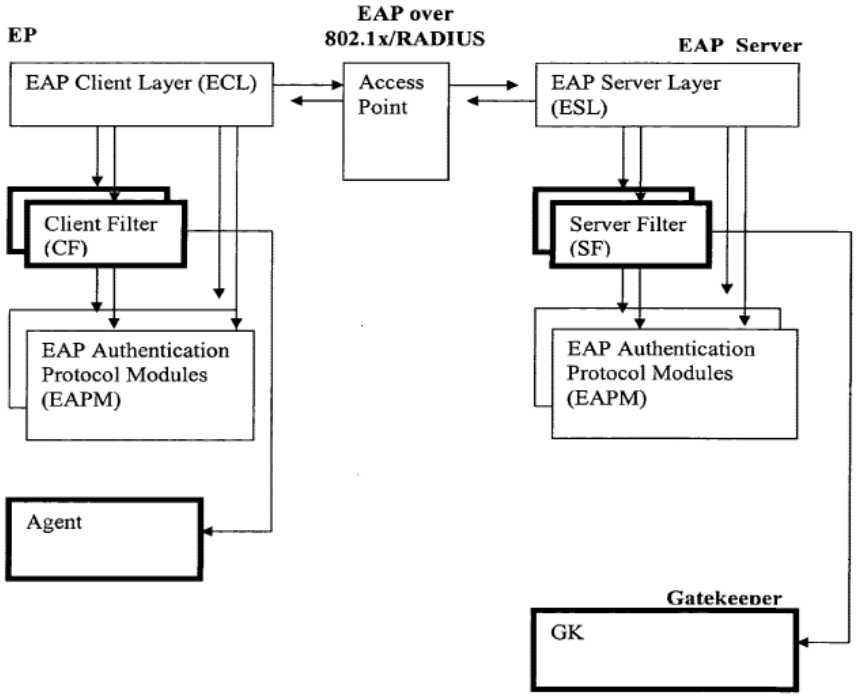
The appendix figures on page 19-20 further depict this, by showing a switch that can be used to communicate with a "Corporate LAN." Upon a successful or failed audit, the switch is "configure[ed]" ("Audit passes set VLAN to corporate LAN", "Failed audit Set to restricted VLAN") to allow/deny such communication.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 19



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 
[7] The method of claim 1, wherein the authentication includes using an EAP protocol.	*See* [1]. 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:

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted



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.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

Figure 5a: Client in Authentication State

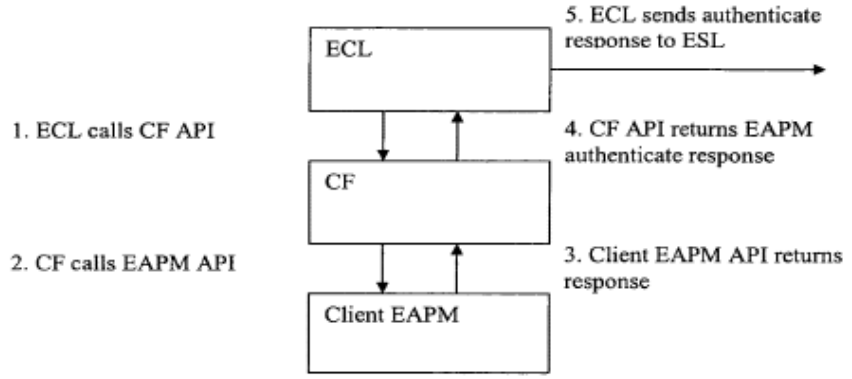
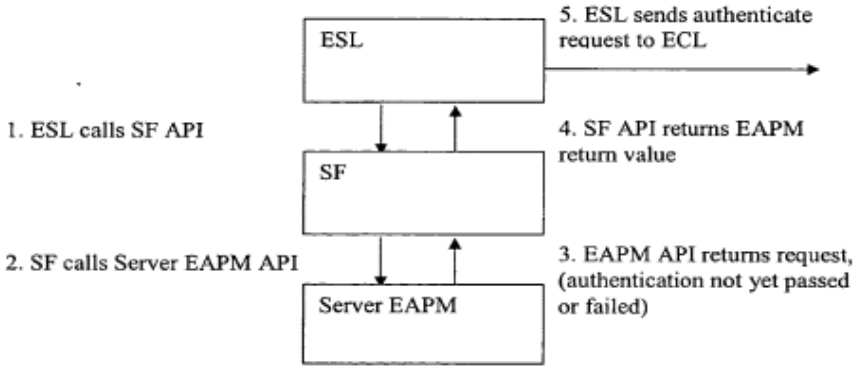
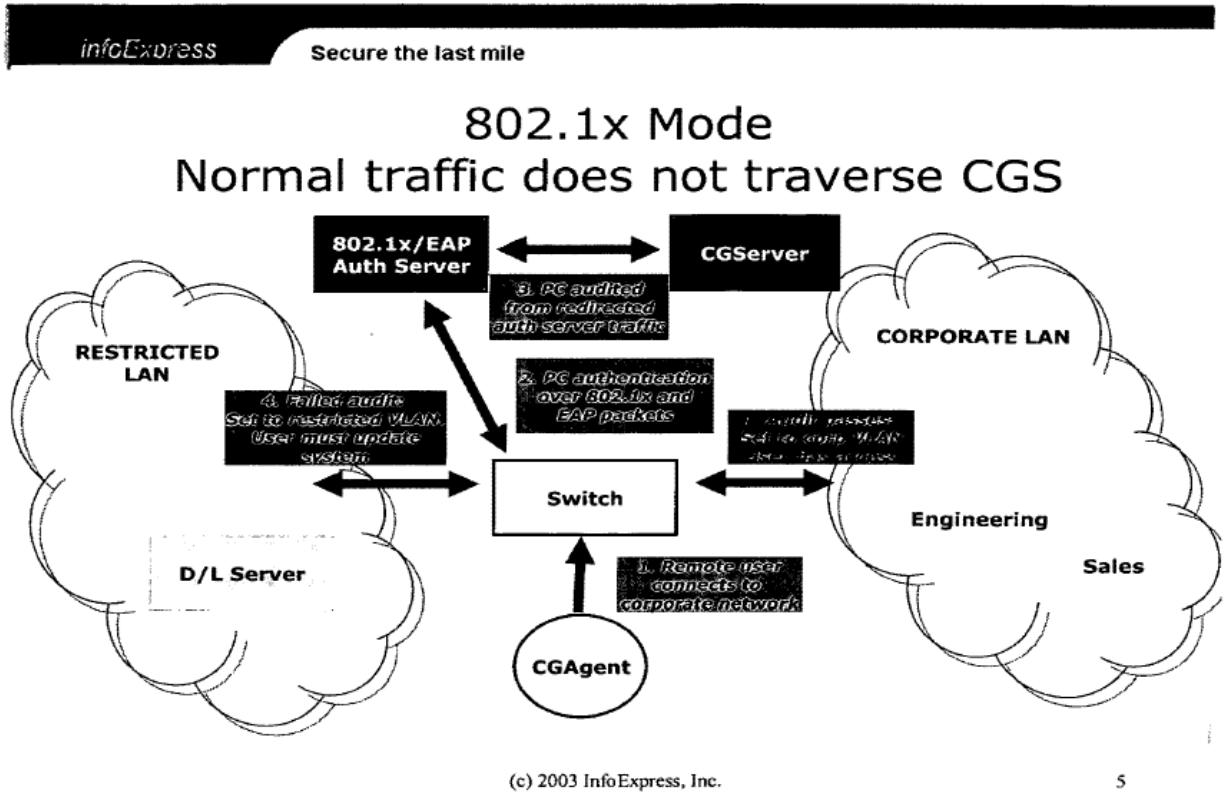


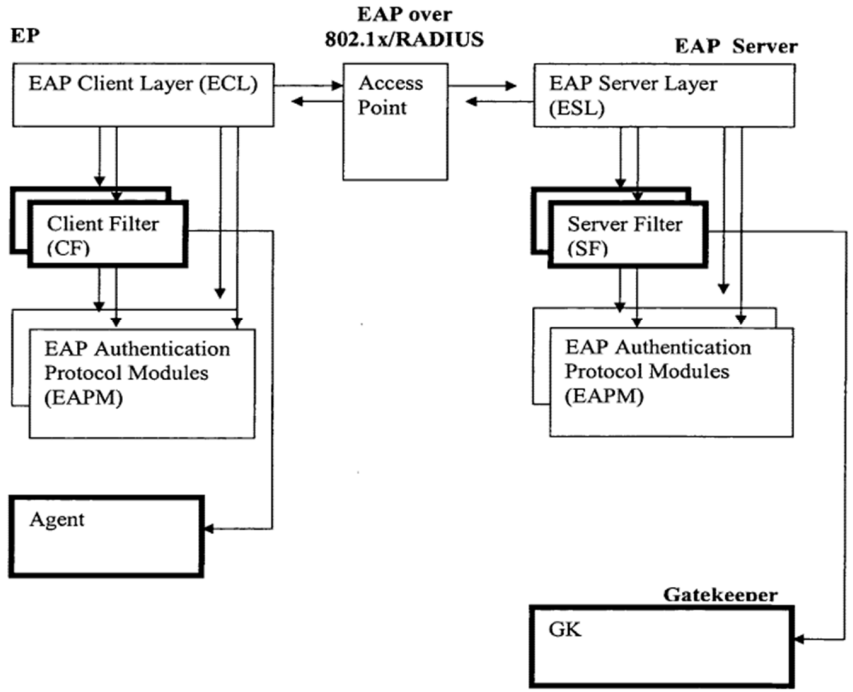
Figure 5b: Server in Authentication State



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.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the appendix at page 20 further describes authentication, in accordance with EAP and 802.1X:

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[8] The method of claim 1, wherein the authentication includes using a RADIUS protocol.	*See* [1]. The provisional shows this element in Figure 4 (page 9). This figure shows using authentication with extensible authentication protocol ("EAP") "over 802.1x/RADIUS".[1] **Figure 4** 

[1] RADIUS stands for Remote Authentication User Dial-in Service. EX1401, 8:37-38.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[9] The method of claim 1, wherein one of the requirements pertains to a status of an application on the device.	*See* [1]. 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 include information regarding the "status of an application on the device." Additionally, the provisional refers to information regarding device "applications" as the type of information that was present in some prior art systems (e.g., InfoExpress's own CyberGatekeeper Remote system, described on page 4):

	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. 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. By default, the GK is designed to prevent access to the corporate network if there are no rules granting access to the corporate network. If the EP's audit information complies with the policies, the GK lets the EP access the corporate network by setting a filter rule(s) that allows traffic from the EP to communicate with the corporate network. The GK continues to audit the EP regardless of whether the EP passed or failed the audit. This allows GK to allow or deny access if the EP configuration or applications change.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	InfoExpress's CyberGatekeeper Remote was able to "check for the same ***application running*** on a different version of Windows." EX2013 at 41. That is, the Remote was able to detect an application's ***status***, as distinct from its mere presence on the endpoint. Compound Tests are created from one or more Basic Tests. If any of the Basic Tests are true, the Compound Test itself is true even if the other Basic Tests are false. Compound tests are useful for combining multiple Basic Tests into a single test category. For example, a compound test may include several Basic Tests that each check for the same application running on a different version of Windows. This may be necessary if the application uses different files for various versions of Windows, even though it is the same application. A POSITA would understand that in the present invention too, "one of the requirements pertains to a status of an application on the device."
[10] The method of claim 1, wherein one of the requirements pertains to a status of an operating system exon the device.	*See* [1]. 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 include information regarding the "status of an operating system exon [sic, on] the device."

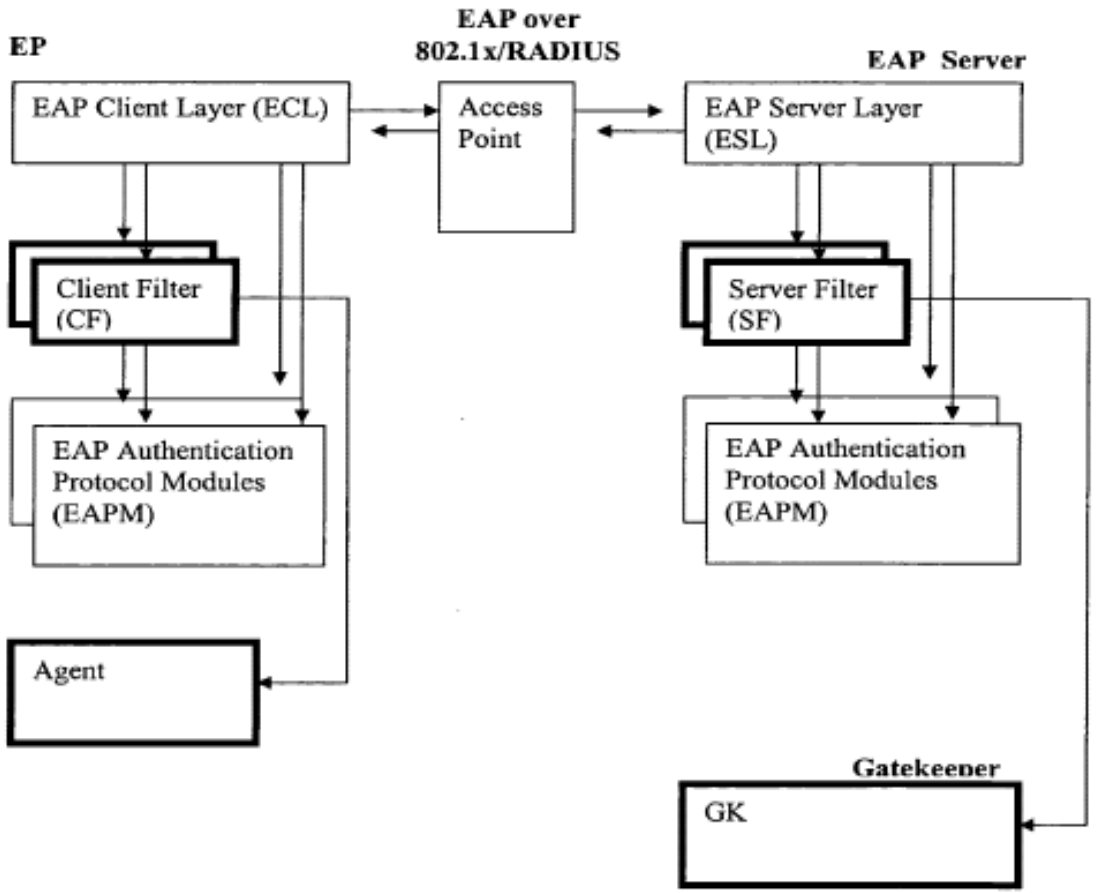
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the provisional, on pages 4 and 5, lists examples of device information used in prior art access control systems regarding applications configurations . A POSITA would understand that in the present invention too, one of the requirements pertains to a status of an operating system on the device.
[14] The method of claim 1, wherein the scanning is performed using an agent on the device.	See [1]. As described above with respect to claim 1.2 ("scanning the device to collect information regarding the device"), the provisional supports "[t]he method of claim 1, wherein the scanning is performed using an agent on the device." First, page 8 describes "the auditing protocol tak[ing] 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.lx

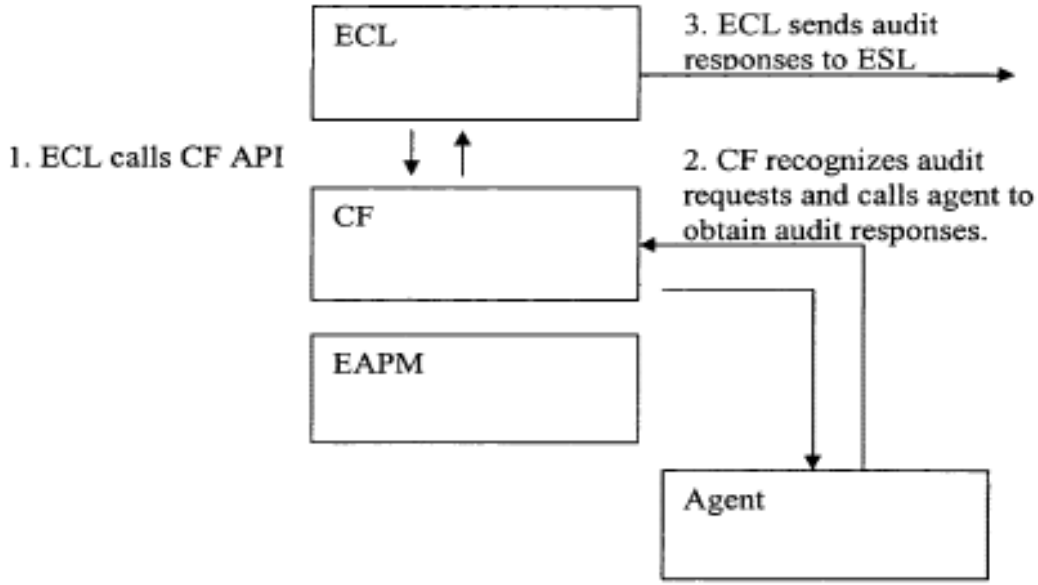
US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	compliant AP . . .” Because the “EP agent” receives “calls for audit information” and send its responses thereto (that is, the audit information), this excerpt supports “scanning performed using an agent on the device.” **Invention** 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.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 11 states, "[t]he agent returns information about the local system, which is converted to audit responses . . " Indicating that the scanning is being performed using an agent on the device. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, Figures 4 (page 9) and 7b (page 13) schematically depict the scanning being performed using an agent on the device.

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

Figure 4



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Figure 7b: Client Responding to Audit Requests 
[16.0] A method of providing access over a communication network, the method comprising:	The provisional was directed to the claimed "method of providing access over a communication network" as shown by its references to "access" on the first page of the patent application. This includes the title itself ("Gatekeeper Invention for Controlling Access . . .") and the description on page 3:

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted

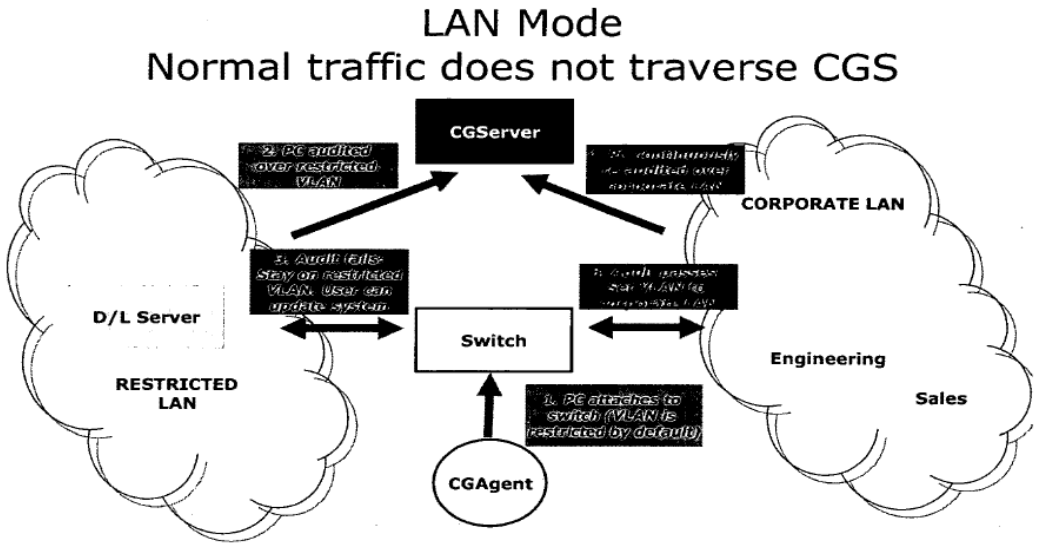
GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x

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

Definitions

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

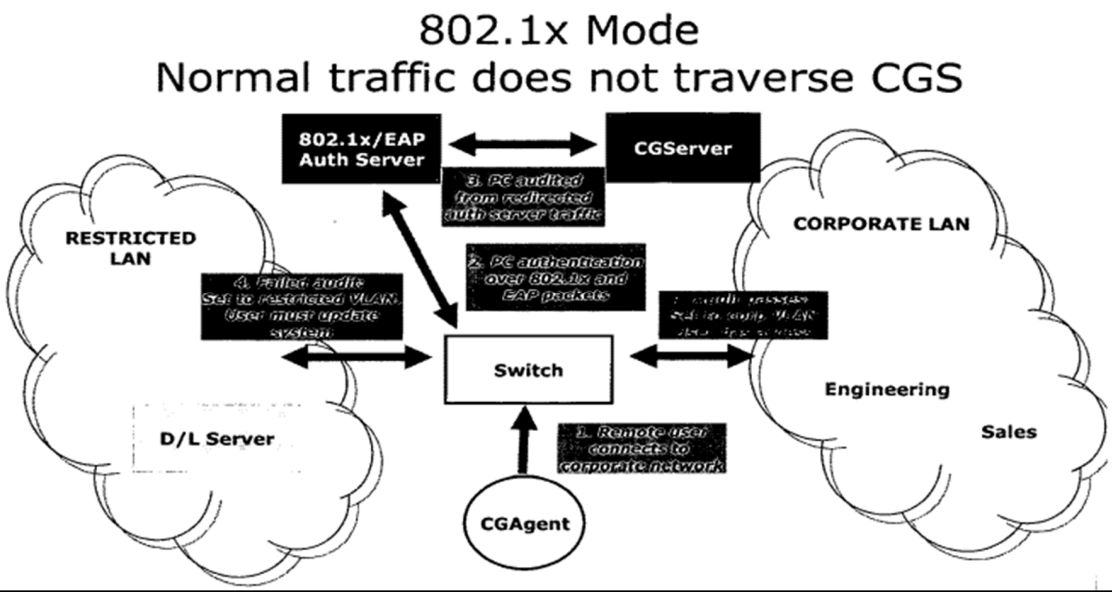
Figure 17 (page 19) depicts the invention's architecture for access control:



US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[16.1] receiving at an access point a request for access to a less-restricted network, the request coming from an access device;	The provisional discusses receiving an endpoint device's request for access to a "corporate network"—that is, a "less-restricted subset of the protected network from an access device". Therefore, in the invention described in the provisional the access point will "receive a request for access to a less-restricted subset of the protected network from access device (endpoint)". Page 3 **GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x** The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. **Definitions** GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

	Page 8 describes a PC endpoint's request for access to a "corporate network" via an access point: **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 when an endpoint requests access but 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 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. The figure on page 20 shows an access device (as denoted by the CGAgent, which is running on the access device), connecting to a switch (access point) and requesting access to the corporate LAN (the less-restricted network).

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 
[16.2] applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;	See [1.2] ("scanning the device to ***collect information*** regarding the device") and [1.3] ("applying a security policy, the security policy including one or more requirements pertaining to the authentication and ***the information***"). Scanning a device to collect information, and then "applying a security policy" by analyzing that collected information to determine whether the endpoint complies with network policies is another way to describe "applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device".

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[16.3] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;	See [2] ("The method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.")
[16.4] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device; and	See: • [1.4] ("configuring the access point in response to a result of applying the security policy"); • [4] ("wherein configuring the access point includes assigning a VLAN"); and • [5] ("wherein the authentication identifies the user of the device").
[16.5] authenticating a user of the access device, wherein granting access is further based on the authentication.	See: • [1.1] ("performing an authentication of a device connected to an access point"); • [7] ("wherein the authentication includes using an EAP protocol"; and • [8] ("wherein the authentication includes using a RADIUS protocol").

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.0] A method of providing access over a communication network, the method comprising:	See [16.0] ("A method of providing access over a communication network, the method comprising").
[22.1] receiving at an access point a request for access via a less-restricted network, the request coming from an access device;	See [16.1] ("receiving at an access point a request for access to a less-restricted network, the request coming from an access device").
[22.2] applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;	See [16.2] ("applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device").

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.3] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit; and	See [16.3] ("providing information to the access device to improve compliance of the access device to the security policy, in response to the audit").
[22.4] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device, the granting of access includes configuring the access point to allow the access.	See: • [16.4] ("granting access to the less-restricted network based on satisfaction of the security policy by the updated access device"); • 1.4 ("configuring the access point in response to a result of applying the security policy"); • [4] ("wherein configuring the access point includes assigning a VLAN"); and • [5] ("wherein the authentication identifies the user of the device").

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[23] The method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device.	See: • [14] ("The method of claim 1, wherein the scanning is performed using an agent on the device.") and • [1.2] ("scanning the device to collect information regarding the device").
[25] The method of claim 22, wherein performing the audit includes receiving operating system information from the access device.	See [10] ("The method of claim 1, wherein one of the requirements pertains to a status of an operating system [] on the device.").

US8677450	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[27] The method of claim 22, wherein the information includes a software update of software on the access device.	See [2] ("The method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.").