

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[1.0] A method for auditing a device, the method comprising:	The ‘080 provisional specification verifies that the invention was directed to the claimed “method for auditing a device” by their references to “controlling access” which includes auditing of the device. For example, the description explains “The invention is directed to controlling access to a corporate network based on audit criteria for end points”: <u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. 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...”).



Page 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.

Page 3

Definitions

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

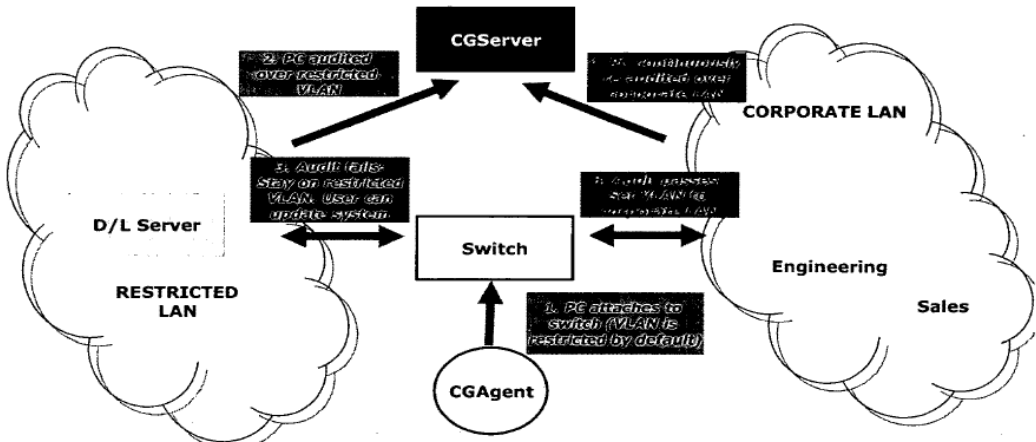
PC – A notebook, desktop PC, PDA, or similar computing device.

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

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

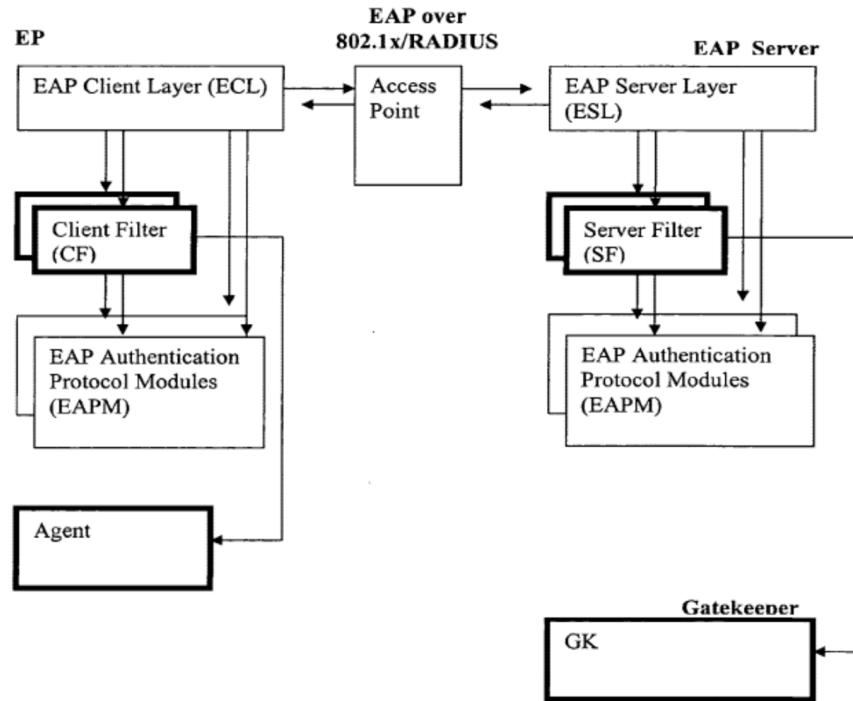
AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

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

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Figure 17 (page 19) depicts the invention's architecture for access control which sets forth, amongst other things, auditing: LAN Mode Normal traffic does not traverse CGS  <pre> graph TD subgraph Restricted_LAN [RESTRICTED LAN] DLS[D/L Server] end subgraph Corporate_LAN [CORPORATE LAN] Eng[Engineering] Sales[Sales] end CGS[CGServer] S[Switch] CGA((CGAgent)) DLS <--> S S <--> Eng S <--> Sales CGS <--> S CGA --> S CGS <--> CGA S -- "1. PE attaches to switch (VLAN is restricted by default)" --- CGA CGA -- "2. PE authenticates over restricted VLAN" --- CGS CGS -- "3. Authentication successful over restricted VLAN" --- S S -- "4. Switch passes Sess. VLAN to CGS" --- CGS CGS -- "5. Audit fails: Sess on restricted VLAN. User can update system" --- DLS </pre>
[1.1] performing an authentication using an EAP protocol from the device,	The '080 provisional provides support for performing an authentication using an EAP protocol from the device. For instance, pages 8 through 11 (and Figures 4, 5a, and 5b therein) all describe authentication being conducted, for example using the Extensible Authentication Protocol (EAP):

	Page 8 of the '080 provisional provides that the “auditing protocol” takes place over an “802.1x compliant AP which relays them to the EAP server” in order to grant or prohibit access to a “corporate network”: 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.
--	---

Pages 9-11



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.

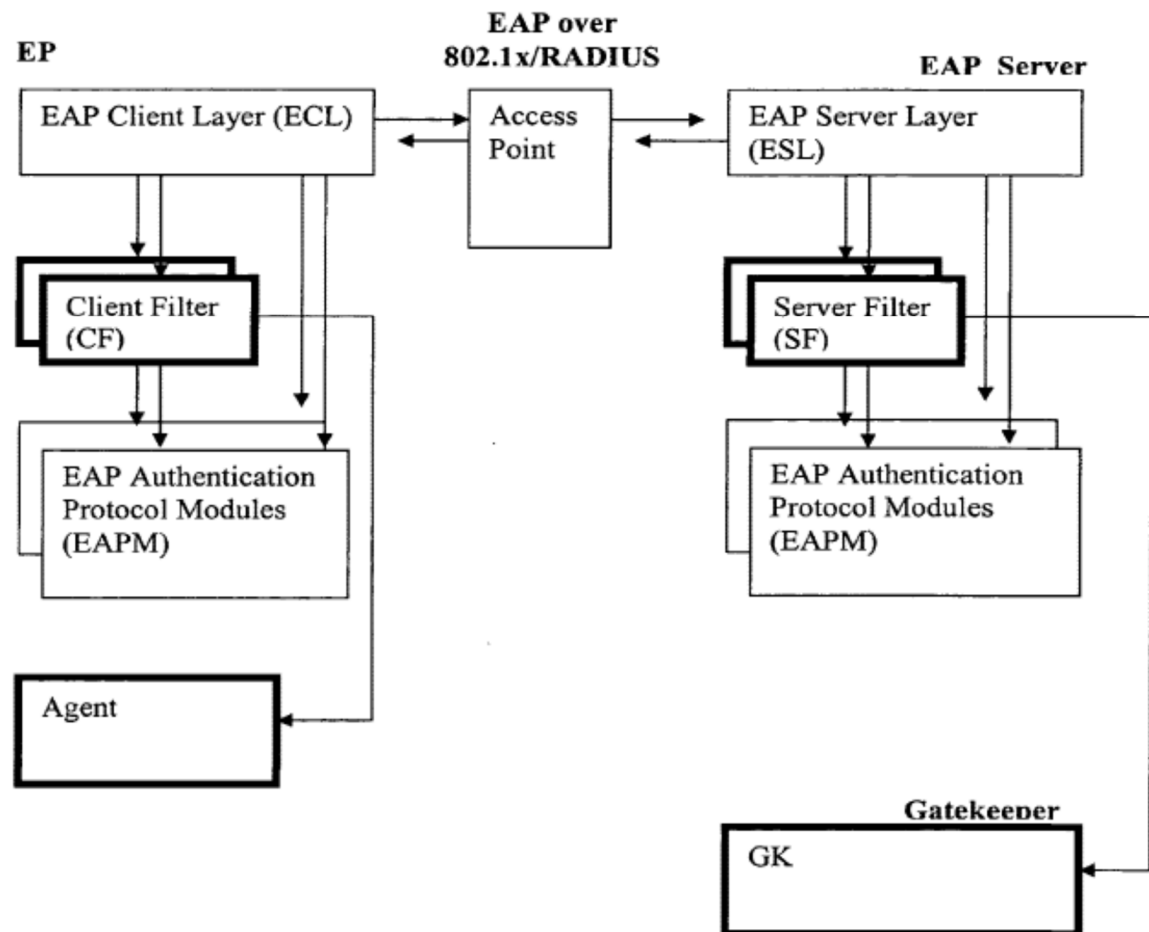
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Figure 5a: Client in Authentication State <pre> sequenceDiagram participant ECL participant CF participant ClientEAPM as Client EAPM ECL->>CF: 1. ECL calls CF API CF->>ClientEAPM: 2. CF calls EAPM API ClientEAPM->>CF: 3. Client EAPM API returns response CF->>ECL: 4. CF API returns EAPM authenticate response ECL->>ESL: 5. ECL sends authenticate response to ESL </pre> Figure 5b: Server in Authentication State <pre> sequenceDiagram participant ESL participant SF participant ServerEAPM as Server EAPM ESL->>SF: 1. ESL calls SF API SF->>ServerEAPM: 2. SF calls Server EAPM API ServerEAPM->>SF: 3. EAPM API returns request, (authentication not yet passed or failed) SF->>ESL: 4. SF API returns EAPM return value ESL->>ECL: 5. ESL sends authenticate request to ECL </pre> 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.

US8578444	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.
[1.2] the device being connected via a computer network to an access point configured to use an 802.1x protocol;	The '080 provisional discloses the device being connected via a computer network to an access point configured to use an 802.1x protocol. For instance, pages 3 and 9 (and Figure 4 therein) all describe authentication being conducted, for example using the Extensible Authentication Protocol (EAP) with a device connected “via a computer network to an access point configured to use an 802.1X protocol”:

	<u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Page 8 of the '080 provisional provides that the “auditing protocol” takes place over an “802.1x compliant AP which relays them to the EAP server” in order to grant or prohibit access to a “corporate network”:
--	--

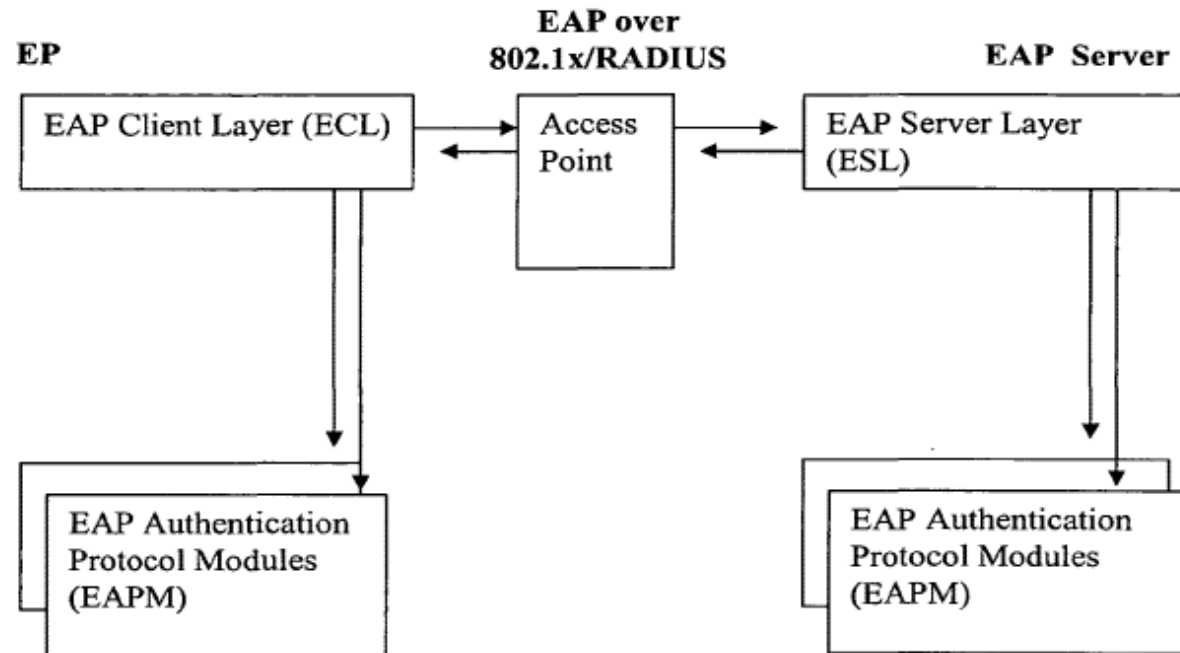
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	6 Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the 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.

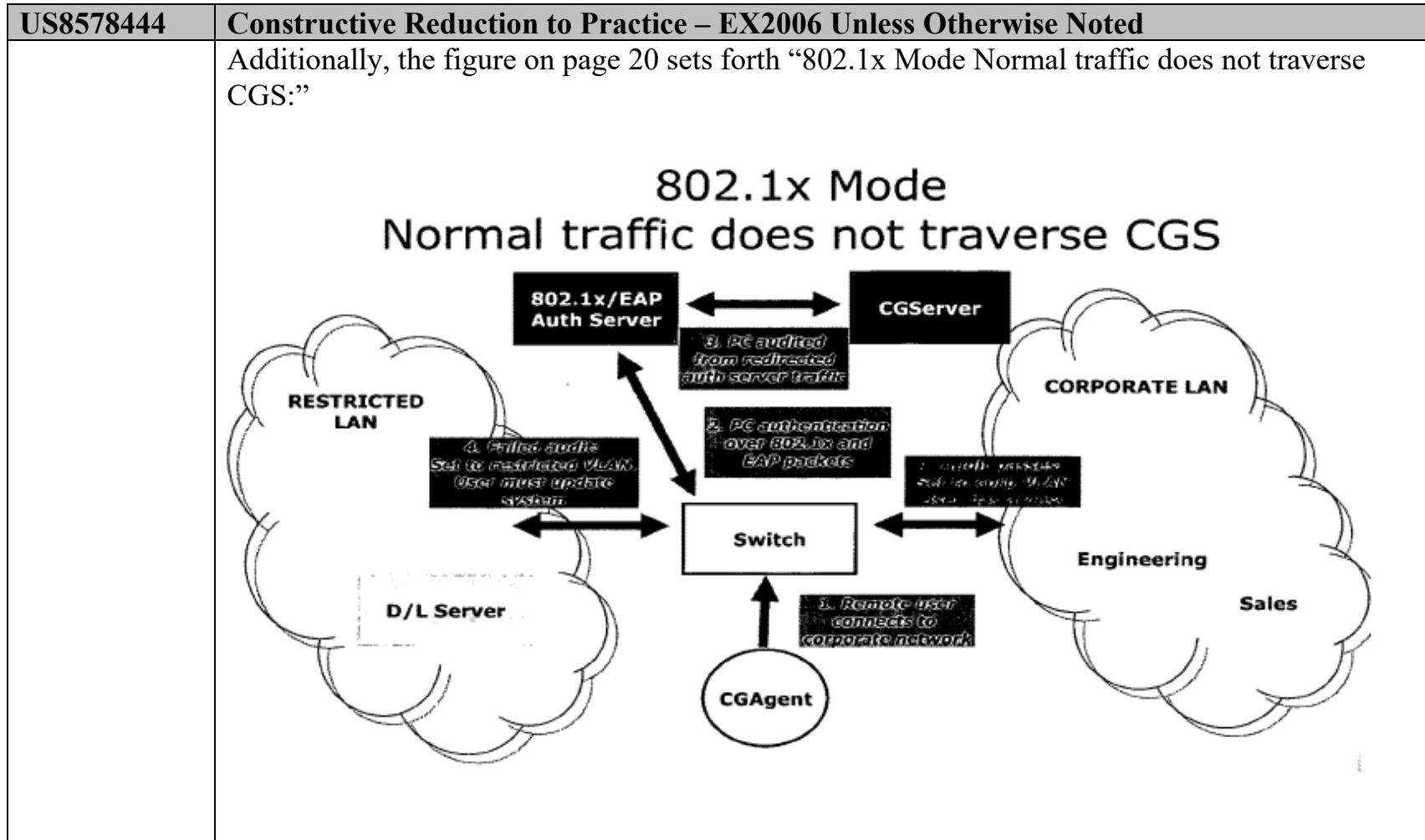
Page 9



The device being connected via a computer network to an access point configured to use an 802.1x protocol is future supported in Figure 3 on page 7, which recites “EAP over 802.1x/RADIUS”:

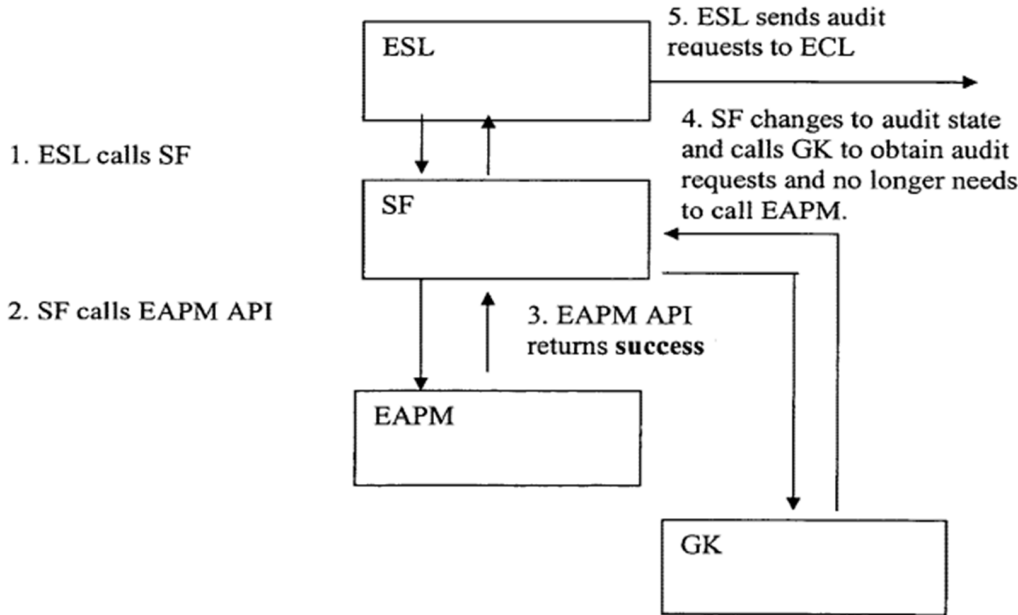
Figure 3





[1.3] sending a request for audit data to an agent running on the device;	The '080 provisional provides support for sending a request for audit data to an agent running on the device. For instance, page 8 provides that there is an “auditing protocol” which “calls for audit information,” i.e., “audit data” from the “agent on the EP,” i.e., the “agent running on the device”:
---	---

	<u>Page 8</u> 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. This limitation is also demonstrated in Figure 6 on page 9 and the description on page 11, which provides “the SF [server filter] changes to the audit state and calls GK to obtain audit requests to send back to the client.” The requests are processed by the agent on the client: “audit requests are passed to the agent API,” and the “agent returns information about the local system”:
--	--

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	<u>Page 11</u> 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  <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK ESL->>SF: 1. ESL calls SF SF->>EAPM: 2. SF calls EAPM API EAPM-->>SF: 3. EAPM API returns success SF->>GK: 4. SF changes to audit state and calls GK to obtain audit requests and no longer needs to call EAPM. ESL->>ECL: 5. ESL sends audit requests to ECL </pre>

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[1.4] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;	The '080 provisional provides support for receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent. For instance, pages 6 and 8 describe authentication being conducted, for example by extensible authentication protocol (EAP) with a device connected “via a computer network to an access point configured to use an 802.1X protocol,” as discussed above in claim 1.1 and 1.2. As set forth in claim 1.3 above, the provisional explains “receiving the audit data at a gatekeeper configured to control access to a network from the agent, the audit data pertaining to the device and having been obtained by the agent.” Further, as discussed on page 8, the audit data is sent from the PC (device) through the Access Point (AP) to the GK (gatekeeper). The auditing protocol takes place between the EP agent software (which runs on the device, as provided on page 6 below) and the GK, with the agent retrieving and providing the audit data to the GK.

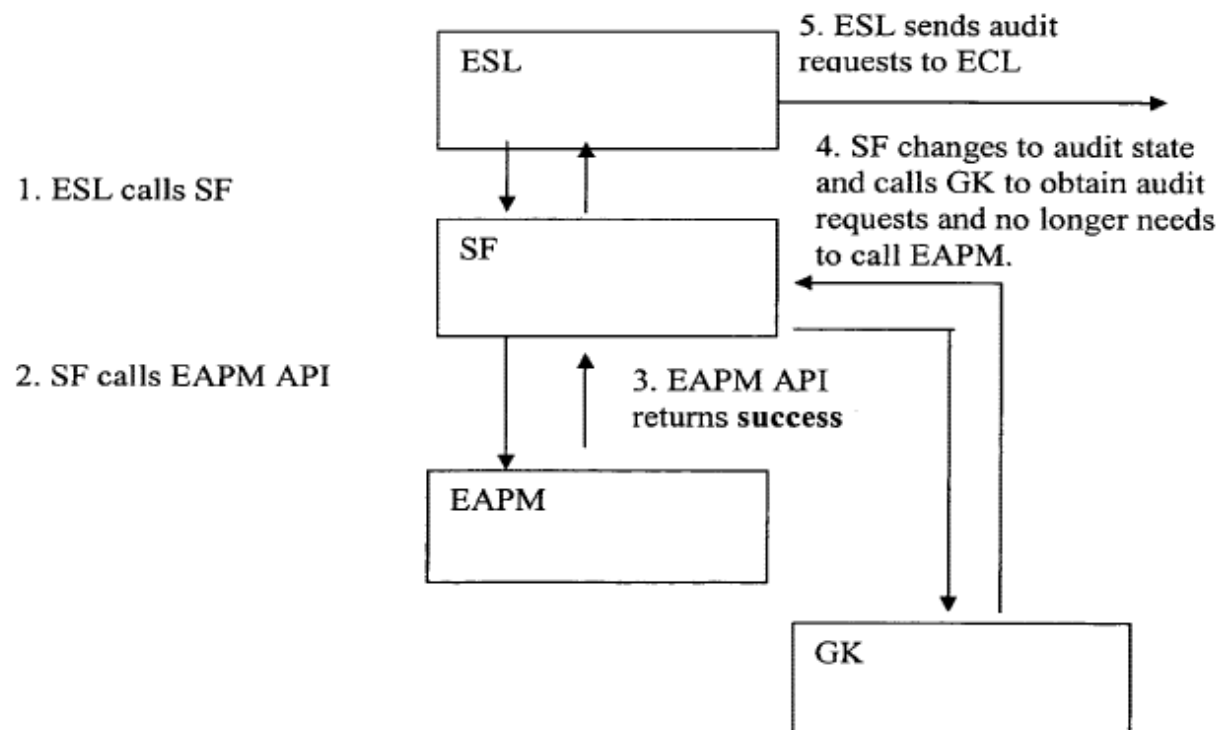
	<u>Page 8</u> Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled. <u>Page 6</u> GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND.
--	--

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 11 also confirms that the GK receives the audit data from the agent, as the GK is called “to obtain audit requests to send back to the client,” and the “agent returns information about the local system, which is converted to audit responses that are sent to the server.”

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



US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[1.5] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.	The '080 provisional supports the limitation of applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper. For example, as it applies to the “audit data,” the provisional explains that “If the EP's audit information complies with the policies, the GK lets the EP access the corporate network.” See also claim element 1.4. <u>Page 4:</u> 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. As it relates to “at least one requirement pertaining to the authentication,” the provisional treats audit data and authentication separately, as provided by Page 8, which states “an AP may be programed 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.” Further, as discussed on page 8, the implementation of the security policies includes both authentication and auditing, with auditing occurring after the authentication process. The audit data is sent from the PC (device) through the Access Point (AP) to the GK (gatekeeper). The PC's (endpoint's) access to a “corporate network” via an access point via “802.1 protocol implementation” and an “auditing protocol between the EP agent software and the CK” where the “request for audit data” is “obtained by the agent” and “receiv[ed] at a

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	gatekeeper configured to control access to a network”. The auditing protocol takes place between the EP agent software (which runs on the device) and the GK, which page 8 describes as “[an] auditing protocol tak[ing] place between the EP agent software and the [gatekeeper]” where “[t]he gatekeeper sends requests for [audit] information” where a “client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP”. Depending on the status of both the authentication and the audit, the device may be blocked or provided access to the corporate network.

	<u>Page 8:</u> 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. Pages 9-10 further provide that authentication requirements pertaining to Client EAPM and Server EAPMs, or "requirement[s] pertaining to authentication" over the EAP while both the client and server are in the "authentication state" before the auditing process occurs:
--	--

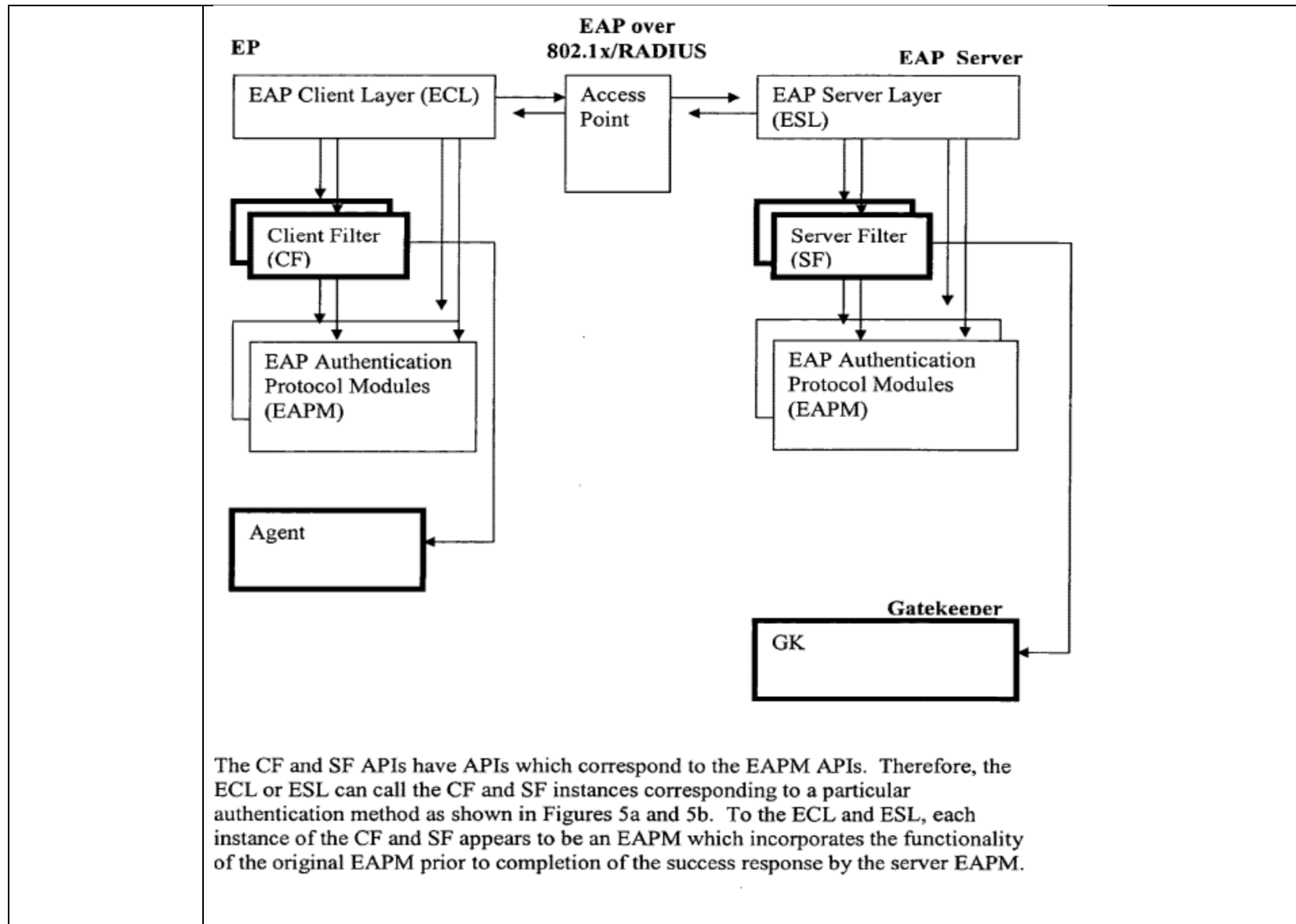


Figure 5a: Client in Authentication State

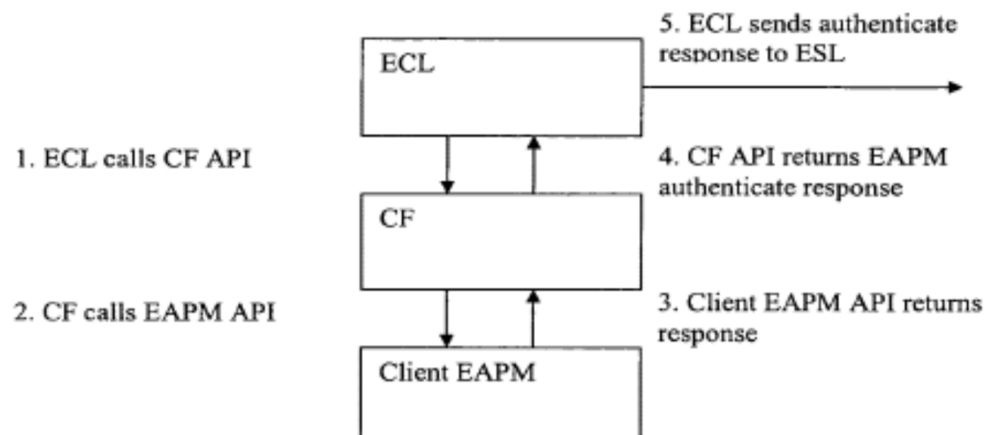
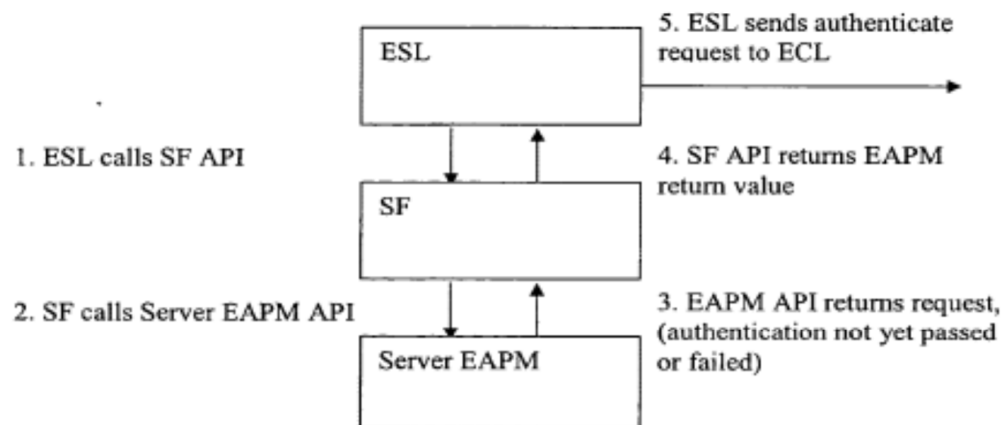


Figure 5b: Server in Authentication State

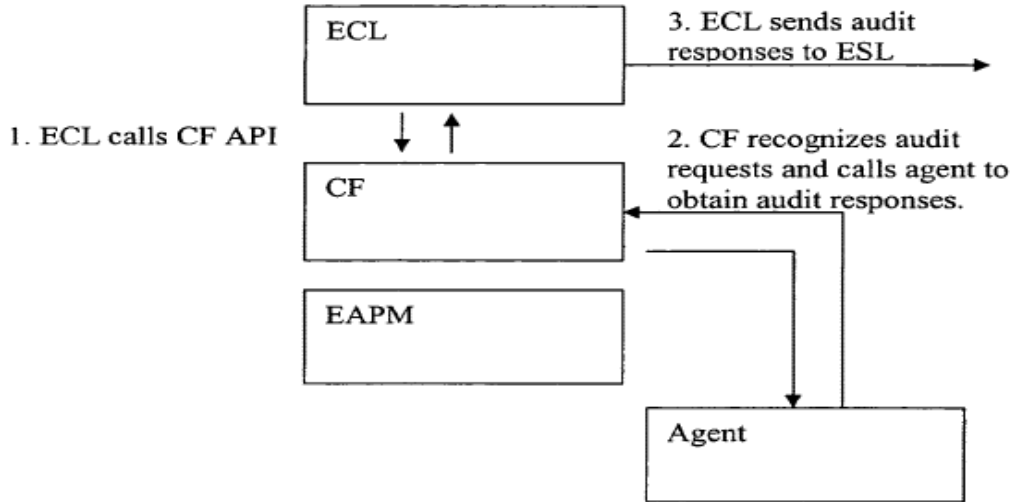


To use the invention, the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method. This authentication method corresponds to an authentication method supported by one of the EAPMs.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Once there is a success response from the server EAPM, as shown in Figure 6 on page 11 and Figures 7a-7b on pages 12-13, the SF changes to audit state and the GK is called to “obtain audit requests,” or a “requirement[] pertaining to audit data,” from the agent until the “necessary audit information” is passed to the SF from the GK:

US8578444	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 <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK ESL->>SF: 1. ESL calls SF SF->>EAPM: 2. SF calls EAPM API EAPM->>SF: 3. EAPM API returns success SF->>GK: 4. SF changes to audit state and calls GK to obtain audit requests and no longer needs to call EAPM. ESL->>ECL: 5. ESL sends audit requests to ECL </pre>

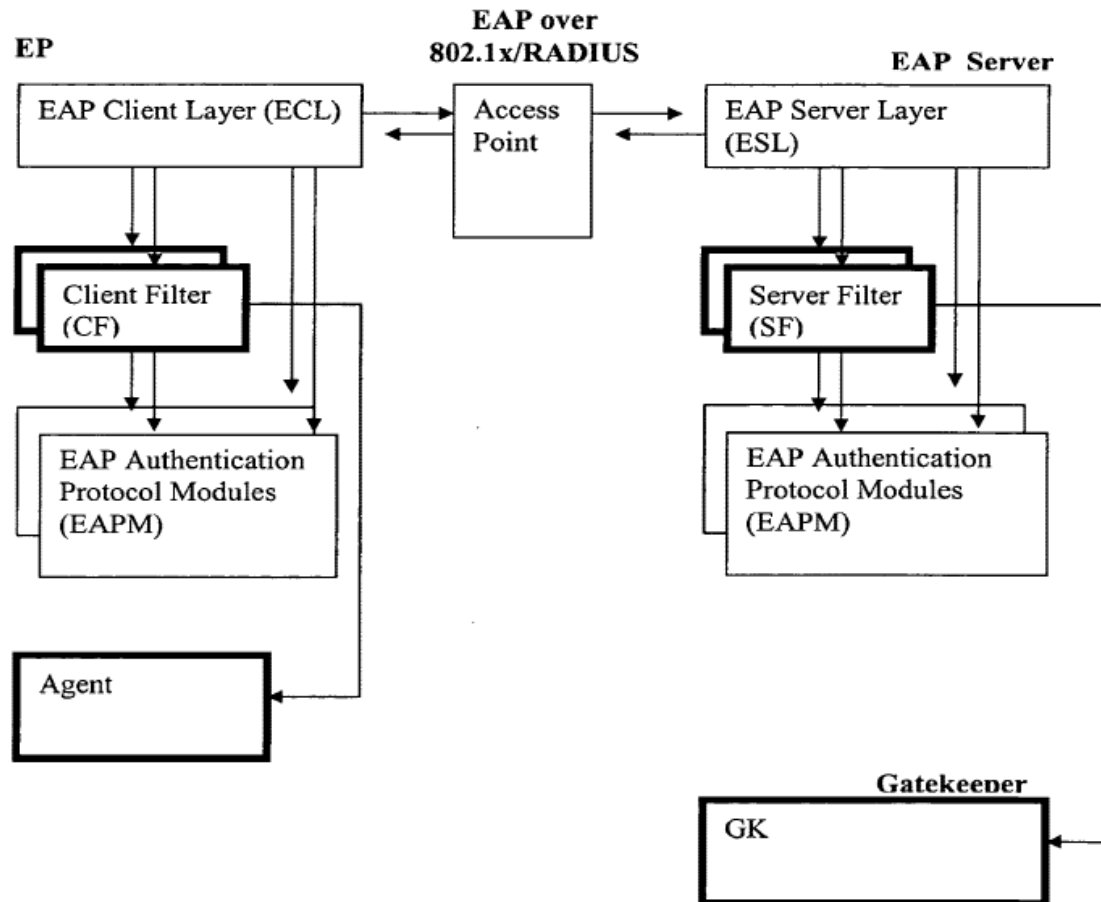
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and 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 <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>GK: 2. SF calls GK to obtain audit requests. Note left of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre> The diagram illustrates the 'Server in Audit State' process. It features four main components: ESL (top), SF (middle), EAPM (bottom left), and GK (bottom right). The process is defined by three numbered steps: 1. ESL calls SF API, indicated by a downward arrow from ESL to SF; 2. SF calls GK to obtain audit requests, indicated by an upward arrow from SF to ESL and a downward arrow from SF to GK; 3. ESL sends audit requests to ECL, indicated by a downward arrow from ESL to EAPM. The EAPM component is shown but has no outgoing arrows in this specific sequence.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Figure 7b: Client Responding to Audit Requests  <pre> sequenceDiagram participant ECL participant CF participant EAPM participant Agent ECL->>CF: 1. ECL calls CF API CF->>ECL: CF->>Agent: 2. CF recognizes audit requests and calls agent to obtain audit responses. ECL->>ESL: 3. ECL sends audit responses to ESL </pre> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. 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.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[2]	<i>See claim 1.</i> On page 14, when discussing the advantages of the invention, the provisional states that an EP can be restricted from accessing the network based on the audit criteria and that a single GK can control or configure many different APs: 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. Additionally, on page 14, the provisional explains that “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 further supports this claim limitation 2 detailing “wherein applying the security policy includes configuring the access point.” See also page 13 (“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.” On pages 8-9 and Figure 4, which describes a PC endpoint’s access to a “corporate network” via an “access point” based on the application of a security policy through “authentication” and “audit[ing],” which is done by “an AP” which may be “programmed to prohibit access by the PC to the corporate network” through the authentication and security policy.

	<u>Pages 8-9</u> 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.
--	--

Figure 4



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

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	As another example, support for this limitation is found on Pages 13-14, which describes how “[a]n EP attached to a port on the AP [<i>i.e.</i>, access point] can be restricted from accessing the corporate network if it does not meet audit criteria.” The provisional document includes controlling the network via 802.1X, VLANs and Access Control Lists (ACL). <u>Pages 13-14</u> Advantages of this invention are that: 1. The invention works with any AP that supports 802.1x. Additional protocols or interfaces are not needed to be compatible with this invention. 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.

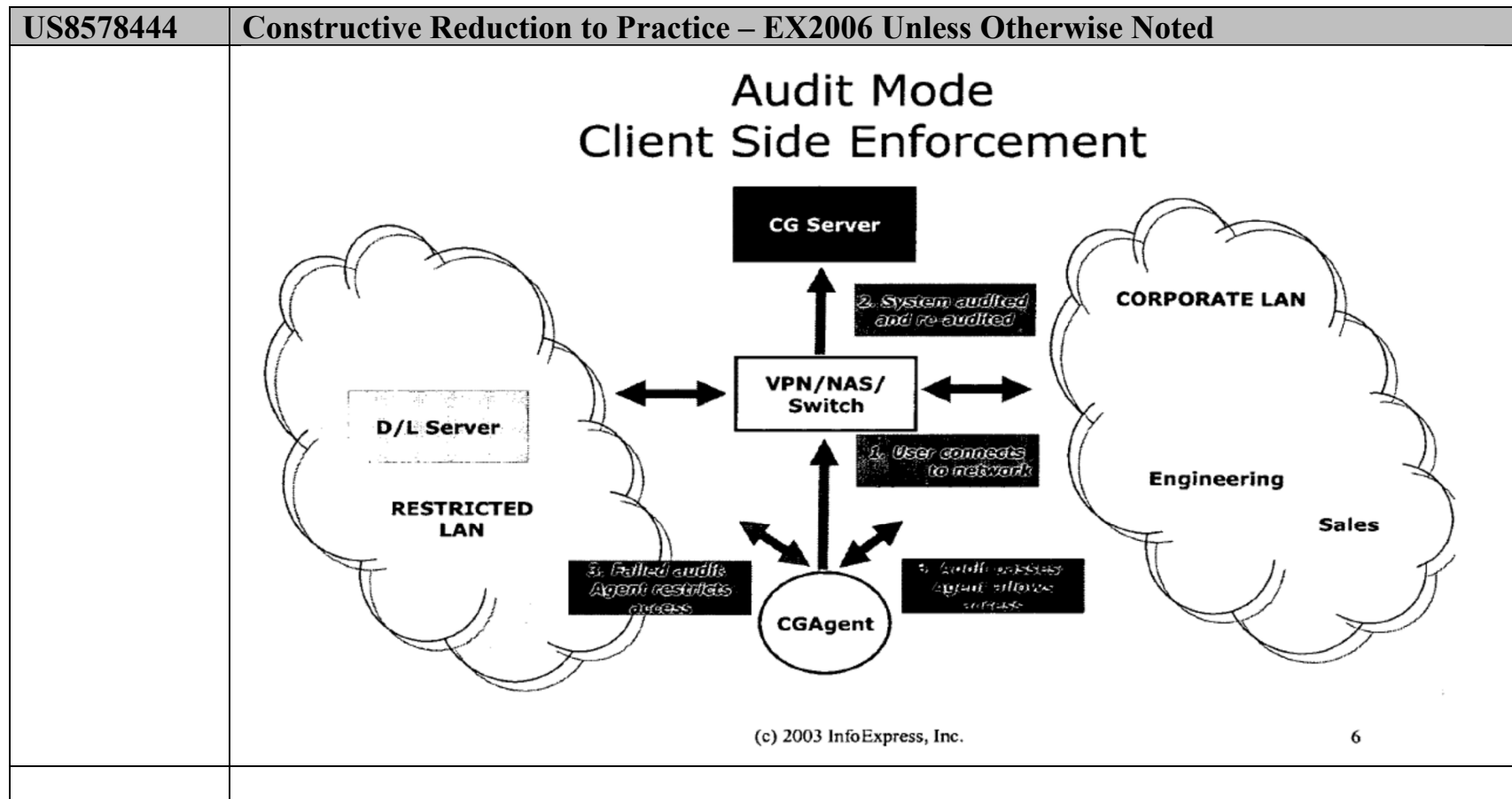
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[3]	<i>See</i> claims 1 and 2. The provisional explains “wherein configuring the access point includes assigning an access control list.” On page 3, access control list (ACL) is described as “a set of filtering rules that specify what traffic is permitted through a port.” 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,” it follows that configuring the AP includes assigning an ACL.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	<u>Pages 13-14</u> Advantages of this invention are that: 1. The invention works with any AP that supports 802.1x. Additional protocols or interfaces are not needed to be compatible with this invention. 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.
[4]	<i>See claims 1 and 2.</i> The provisional provides at least two portions “wherein configuring the access point includes assigning a VLAN.” On page 12, the access point for the EP may configured by being “set to a restricted VLAN where the EP has limited access” to the corporate network:

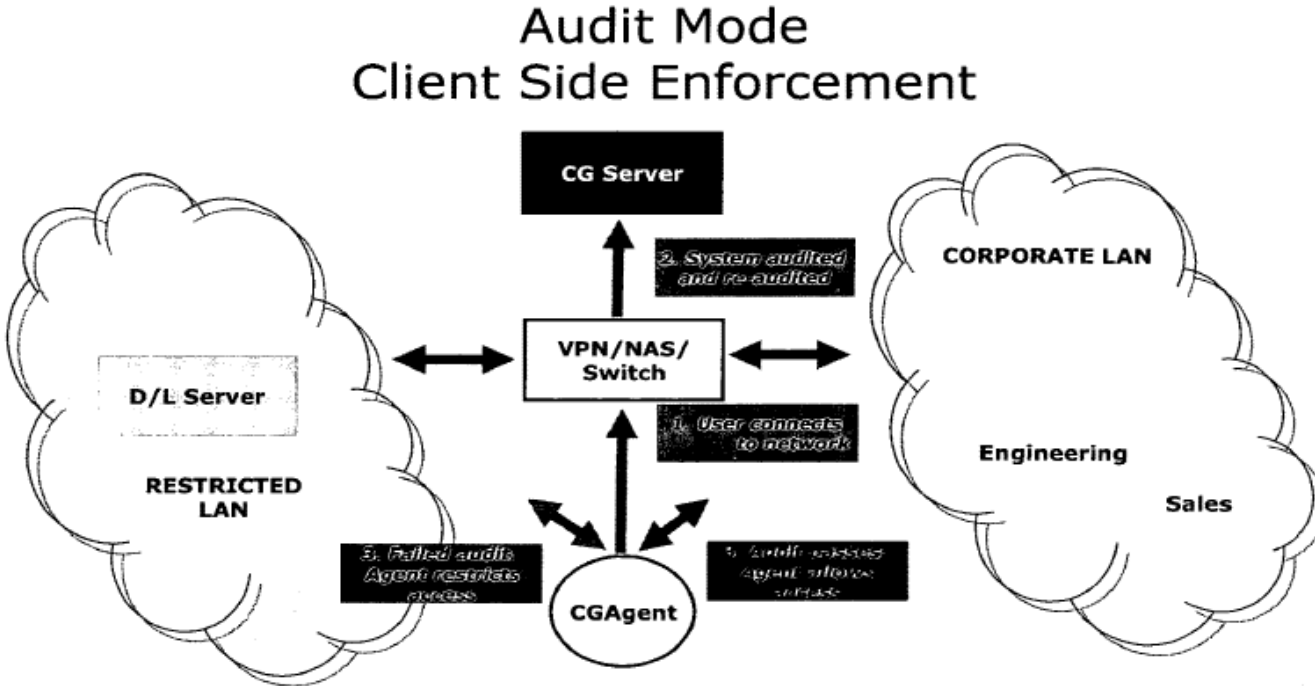
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines 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 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,” it follows that configuring the AP includes assigning a VLAN.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	<u>Pages 13-14</u> Advantages of this invention are that: 1. The invention works with any AP that supports 802.1x. Additional protocols or interfaces are not needed to be compatible with this invention. 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.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[5]	<i>See</i> claims 1 and 2. The provisional supports this limitation on page 13, which provides that continued updated audit information may be provided after configuration of the access point by “keep alives” and “updates regarding changes to previous audit information,” which are evaluated and modified appropriately after the AP is configured. <u>Page 13</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. 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. Further, the appendix figure on page 21 explains that the “system [is] audited and re-audited,” which supports receiving updated audit data pertaining to the device after configuring the access point:



US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[6]	<i>See</i> claims 1, 2 and 5. Page 13 discusses that continued updated audit information may be provided after configuration of the access point by “keep alives” and “updates regarding changes to previous audit information,” which are evaluated and modified appropriately after the AP is configured while the device is on a “less-restricted subset of the network,” (e.g. corporate network) as if there is an update to the audit information “access to the network is modified appropriately by changing the VLAN used for the EP” or the more restricted subset of the network. <u>Page 13</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. 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. Further, the appendix figure on page 21 explains that the “system [is] audited and re-audited,” which supports receiving updated audit data pertaining to the device after configuring the access

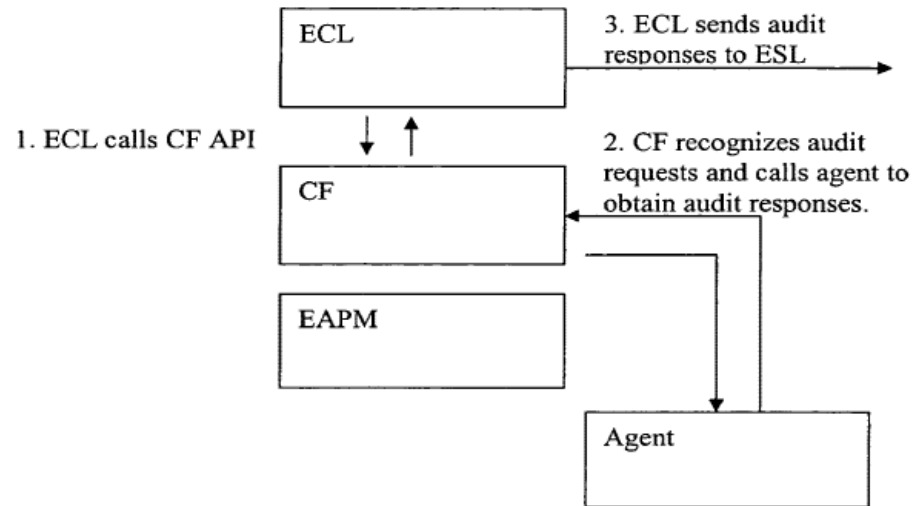
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	point. Based on this auditing and reauditing, the “audit passes” and the “agent allows access” to the corporate LAN (that is, the “less restricted subset of the network”), and another where the “audit fails” and the “agent restricts access” to the “restricted LAN.” <u>Page 21</u>  Audit Mode Client Side Enforcement The diagram illustrates a network architecture for audit mode client side enforcement. It features two main network segments: a RESTRICTED LAN on the left and a CORPORATE LAN on the right. The RESTRICTED LAN contains a D/L Server. The CORPORATE LAN includes departments for Engineering and Sales. A central VPN/NAS/Switch acts as the bridge between these two LANs. Above the switch is a CG Server, and below it is a CGAgent. The process flow is as follows: 1. User connects to network: A user from the Corporate LAN connects to the VPN/NAS/Switch. 2. System audited and re-audited: The VPN/NAS/Switch communicates with the CG Server for auditing. 3. Failed audit: Agent restricts access: If the audit fails, the CGAgent restricts access to the Restricted LAN. 4. Audit passes: agent allows access: If the audit passes, the CGAgent allows access to the Restricted LAN.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	<u>Page 8</u> Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled. According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[7]	<i>See</i> claims 1, 2 and 6. The provisional supports this limitation on page 13, which provides that continued updated audit information may be provided to the GK after configuration of the access point by “keep alives” and “updates regarding changes to previous audit information,” as claim 1 (and Figures 7a-7b on pages 12-13 below) provides that such audit information when the server is in the “audit state” is provided to and passes through the GK. This is further supported by the fact that the EP is “isolated from the company network until it successfully passes an audit with the GK,” meaning that the audit data must be received by the GK from the agent. <u>Pages 12-13</u>

US8578444	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 <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>ESL: Note right of SF: 2. SF calls GK to obtain audit requests. SF->>GK: Note right of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre>

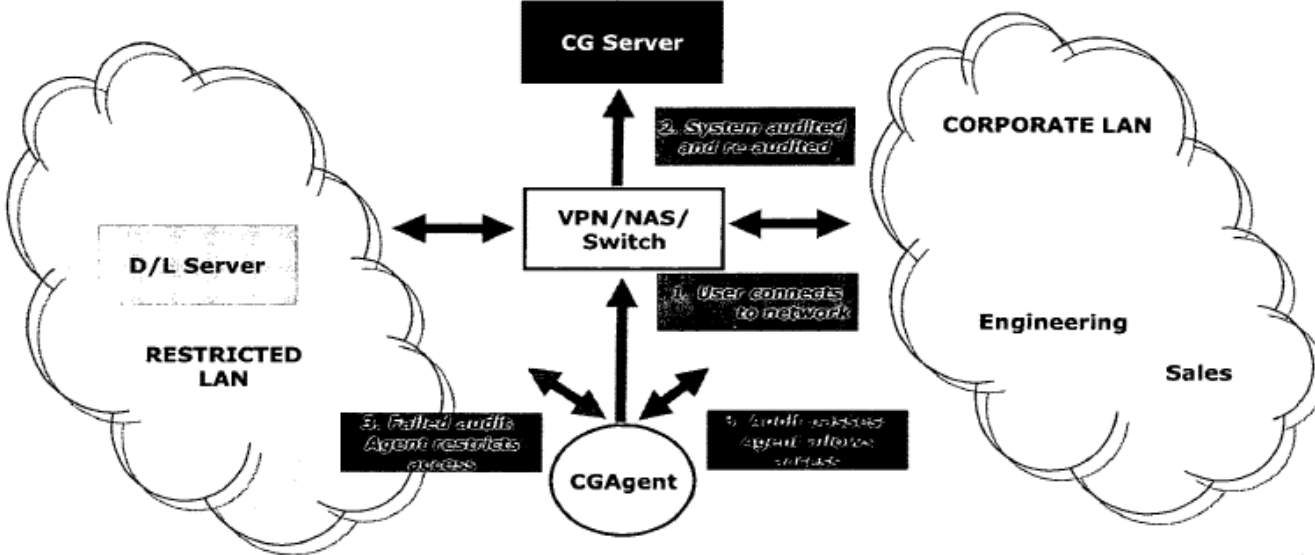
Figure 7b: Client Responding to Audit Requests



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.

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.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Further, the appendix figure on page 21 explains that the “system [is] audited and re-audited” after configuration to the access point is established, and the “CGAgent” or “GK” receives information from the “agent” during this time, which allows the GK to “allow[]” or “restrict[]” the user from the restricted and less restricted LAN. Audit Mode Client Side Enforcement  <pre> graph TD subgraph Restricted_LAN [RESTRICTED LAN] DLS[D/L Server] end subgraph Corporate_LAN [CORPORATE LAN] Eng[Engineering] Sales[Sales] end CGS[CG Server] VNS[VPN/NAS/Switch] CGA((CGAgent)) VNS <--> DLS VNS <--> Eng VNS <--> Sales VNS <--> CGS CGA <--> VNS CGA <--> CGS 1[1. User connects to network] --> VNS 2[2. System audited and re-audited] --> CGS 3[3. Failed audit: Agent restricts access] --> CGA 4[4. Audit successful: Agent allows access] --> CGA </pre> The diagram illustrates the Audit Mode Client Side Enforcement process. It shows a central VPN/NAS/Switch connected to a RESTRICTED LAN (containing a D/L Server) and a CORPORATE LAN (containing Engineering and Sales). The switch is also connected to a CG Server and a CGAgent. The process flow is as follows: 1. User connects to network: A user connects to the network through the VPN/NAS/Switch. 2. System audited and re-audited: The system is audited and re-audited, with information sent to the CG Server. 3. Failed audit: Agent restricts access: If the audit fails, the CGAgent restricts access to the Restricted LAN. 4. Audit successful: Agent allows access: If the audit is successful, the CGAgent allows access to the Corporate LAN.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[10]	<i>See claim 1.</i> 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” includes “audit data pertaining to an application.” <u>Page 11</u> The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server’s ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server’s authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the references to the types of device information used in prior art access control systems—e.g. that regarding “applications [and] configurations” (pages 4 and 5)—means that a

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	POSITA would understand that in the present invention too includes a “request for audit data pertaining to an application.” <u>Pages 4-5</u> 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.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[12]	<i>See claim 1.</i> 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” includes “information that concerns [the] operating system of the 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. Additionally, the references to the types of device information used in prior art access control systems—e.g. that regarding “applications [and] configurations” (pages 4, 5)—means that a POSITA would understand that in the present invention too includes “information that concerns [an] operating system of the device.”

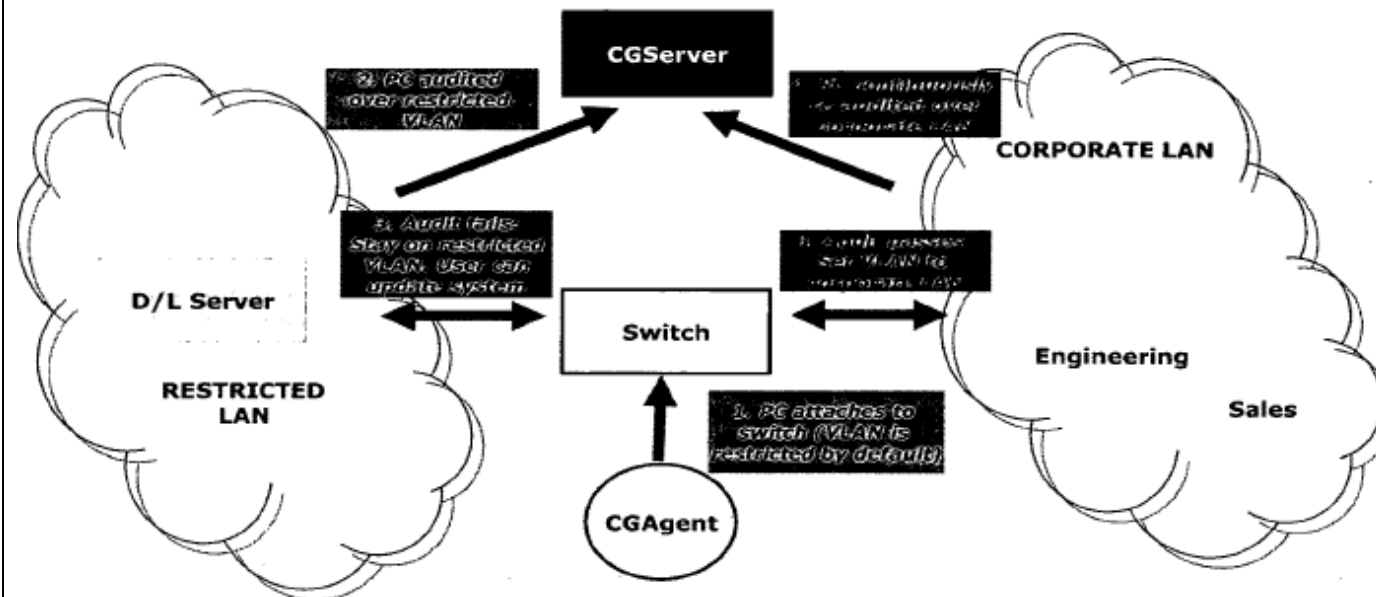
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	<pre> graph LR EP[EP] <--> NAS[NAS] NAS <--> GK[GK] GK <--> CN((Corporate Network)) CN <--> PM[Policy Manager] PM --> P1[Policy 1] PM --> P2[Policy 2] PM --> PN[Policy N] P1 --> GK P2 --> GK PN --> GK </pre> Figure 1 When the 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.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[17]	<i>See claim 1.</i> The ‘080 provisional supports the limitation “gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.” Specifically, the appendix figures on pages 18 and 20 provide that, in an event the “audit fails,” the user “stay[s] on [a] restricted VLAN[,]” where that “user can update [their] system.” Furthermore, the figure shows that the endpoint is “continuously audited over the corporate LAN.” The GK “take[s] part in bringing a software on the device up to date” because the GK communicates with and informs the device that the software is not up to date in response to a failed audit when the “GK returns a failure response.” <u>Page 13</u> If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. After the audit has been performed, “keep 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 19

LAN Mode

Normal traffic does not traverse CGS



US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Page 20 802.1x Mode Normal traffic does not traverse CGS <pre> graph TD Switch[Switch] Auth[802.1x/EAP Auth Server] CGS[CGServer] CGA((CGAgent)) Switch <--> Auth Switch <--> CGS Switch <--> CGA subgraph RESTRICTED_LAN [RESTRICTED LAN] DLS[D/L Server] end subgraph CORPORATE_LAN [CORPORATE LAN] Eng[Engineering] Sales[Sales] end Switch --- RESTRICTED_LAN Switch --- CORPORATE_LAN </pre> 1. Remote user connects to corporate network 2. PC authentication over 802.1x and EAP packets 3. PC audited from redirected auth server traffic 4. Failed audit, set to restricted VLAN. User must update system
[22.0] A method for auditing a device, the method comprising:	See claim 1.0. The ‘080 provisional specification verifies that the invention was directed to the claimed “method for auditing a device” by their references to “controlling access” and the like. For example, the description on page 3 provides that access to a corporate network is based on “audit criteria”:

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	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. Figure 17 (page 19) depicts the invention's architecture for access control: LAN Mode Normal traffic does not traverse CGS <pre> graph TD CGServer[CGServer] Switch[Switch] CGAgent((CGAgent)) subgraph RESTRICTED_LAN [RESTRICTED LAN] DLServer[D/L Server] end subgraph CORPORATE_LAN [CORPORATE LAN] Engineering[Engineering] Sales[Sales] end CGServer <--> Switch Switch <--> CGAgent Switch <--> RESTRICTED_LAN Switch <--> CORPORATE_LAN </pre>

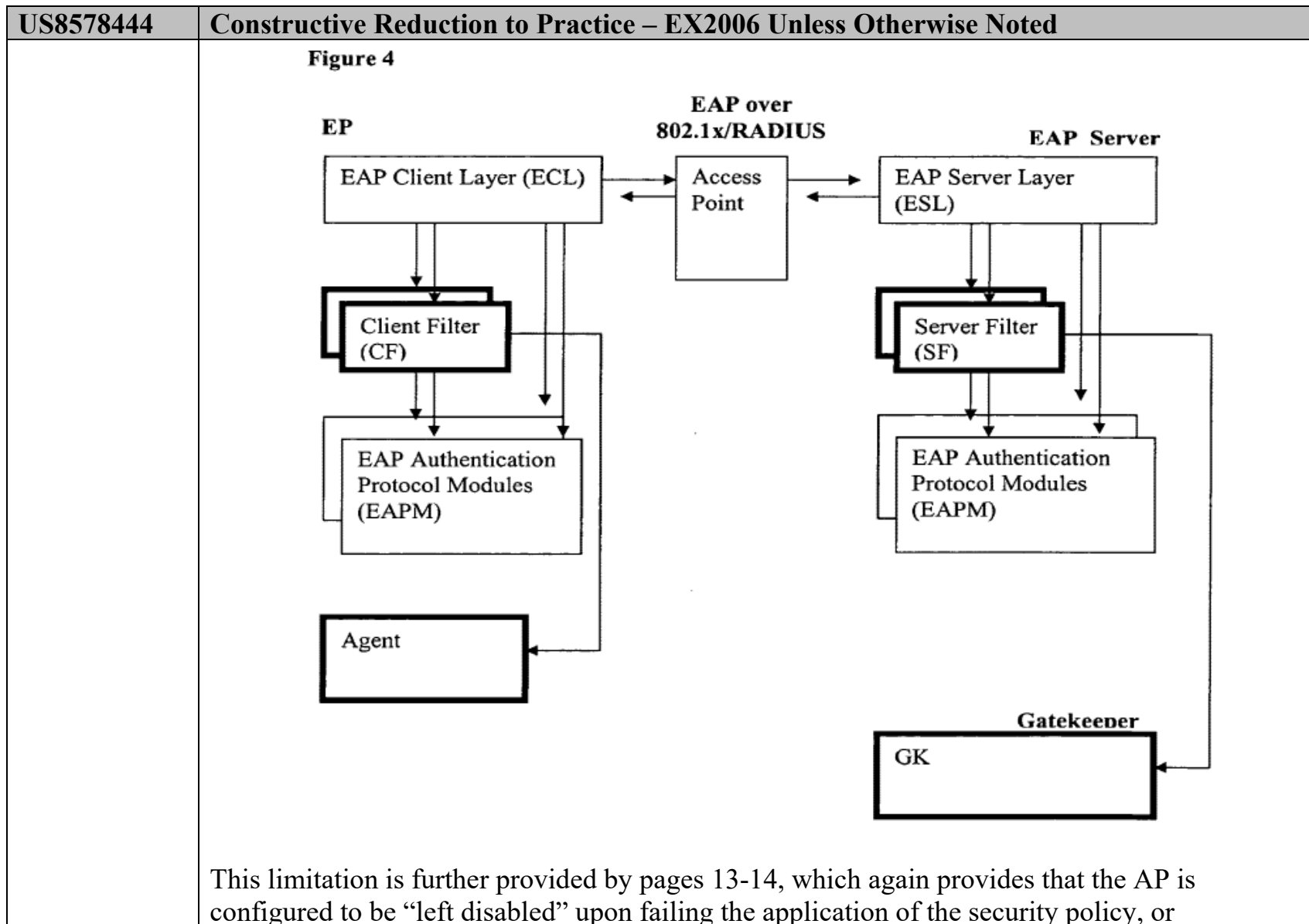
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.1] performing an authentication using an EPA protocol from the device,	<i>See</i> claim 1.1, which discloses “performing an authentication using an EAP protocol from the device.”
[22.2] the device being connected to an access point configured to use an 802.1x protocol;	<i>See</i> claim 1.2, which discloses “the device being connected via a computer network to an access point configured to use an 802.1x protocol.”
[22.3] sending a request for audit data to an agent running on the device;	<i>See</i> claim 1.3, which discloses “sending a request for audit data to an agent running on the device.”

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.4] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;	<i>See claim 1.4, which discloses “receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent.”</i>

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.5] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper,	<i>See claim 1.5, which discloses “applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.”</i>

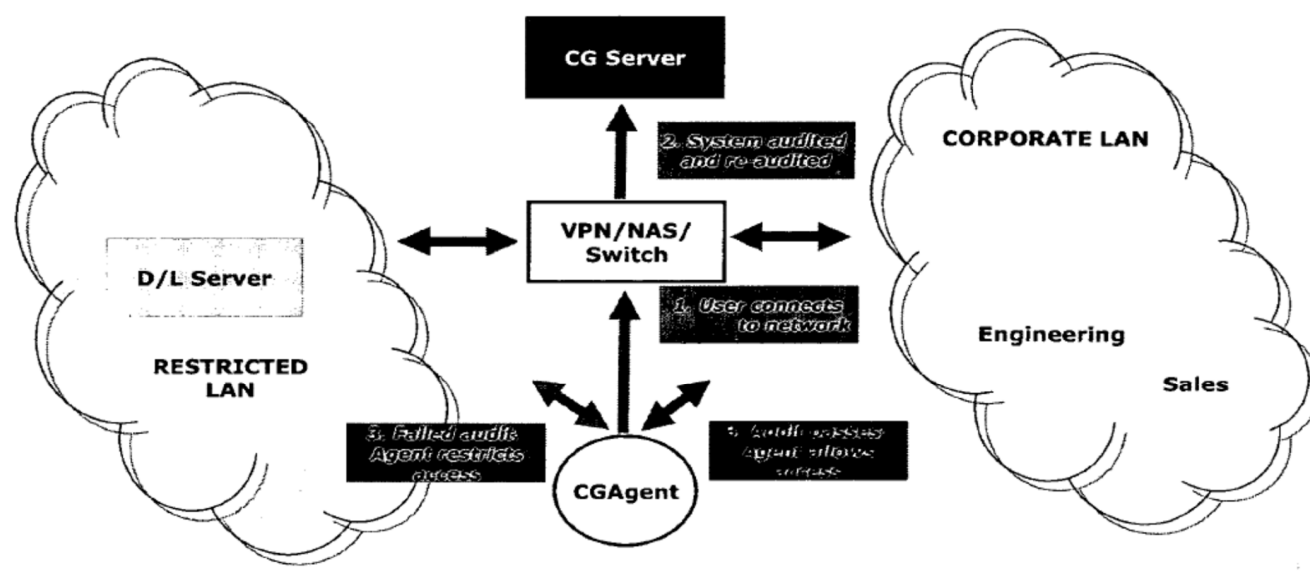
US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.6] where applying the security policy includes configuring the access point;	<i>See also</i>, claims 2, 3 and 4. The provisional supports the limitation of “applying the security policy includes configuring the access point.” As stated above for limitation 1.5 and shown on page 8, the security policy includes the configuration of an access point, based on whether an “audit is successful,” in which case the PC is allowed access to the corporate network via the AP, and if the audit is not successful the AP restricts access or “is left disabled.” Either way, the AP is configured based on the application of the security policy, as further provided by Figure 4 on page 9:

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	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.



US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	alternatively the AP is configured to allow access to the “restricted VLAN.” Regardless, the EP’s access is controlled by the AP until an audit is successfully passed with the GK: 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. 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

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
[22.7] receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network; and	<i>See</i> claims 6 and 7, which further discloses “receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network.”
[22.8] re-auditing the device in accordance to the security policy using the received updated audit data.	<i>See also</i> claims 6 and 7. The '080 provisional supports “ re-auditing the device in accordance to the security policy using the received updated audit data.” For example, the appendix figure on page 21 explains the that the “system [is] audited and re-audited” which therefore supports “continued compliance of the device with the security policy using the updated audit data.”

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	Audit Mode Client Side Enforcement  (c) 2003 InfoExpress, Inc. 6 Additionally, the excerpt from page 13 goes on to describe how “‘keep alives’ and updates regarding changes to previous audit information are exchanged.” These “updates regarding changes to previous audit information [that] are exchanged” constitute “received updated audit data”; it is further explained that these communications are with “the device” that was the subject of the prior audit.

US8578444	Constructive Reduction to Practice – EX2006 Unless Otherwise Noted
	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.