Deploying 802.1x-Based Port Authentication on the Cisco Virtual Office Solution

This white paper provides detailed design and implementation pieces of information relating to deployment of 802.1x-Based Port Authentication with the Cisco Virtual Office (CVO).

Please refer to the CVO overview (found at http://www.cisco.com/go/cvo) for further information about the solution, its architecture, and all of its components.

Purpose and Scope

This guide explains how the IEEE 802.1x-based authentication for Ethernet ports is implemented in the Cisco Virtual Office solution. This document may not explain all the alternative designs or configuration options.

Introduction

The 802.1x-based authentication described in this document is used to authenticate hosts connecting to the Ethernet switch ports of the router. Switch ports are supported on fixed configuration and modular integrated services routers (ISR). Modular routers support switch ports as an add-on interface card. A device connecting through the wireless interface will use its own authentication mechanism. Deploying this feature in CVO ensures that only authenticated hosts can gain access to the VPN. Unauthenticated hosts can only access the Internet. This is particularly helpful for separating “spouse and kids” computers from employee computers.

Following are the important functions provided by this feature.

- User authentication and port security—Only authorized users get access to the VLAN.
- Automatic VLAN assignment—Port is assigned the appropriate VLAN based on the user credentials.
- Guest VLAN—Clientless hosts can be assigned to a separate VLAN designated as a guest VLAN.
- Single-host/multi-host mode.

The 802.1x authentication is enabled on the spoke routers, which contacts the RADIUS server hosted in the management network for user authentication.

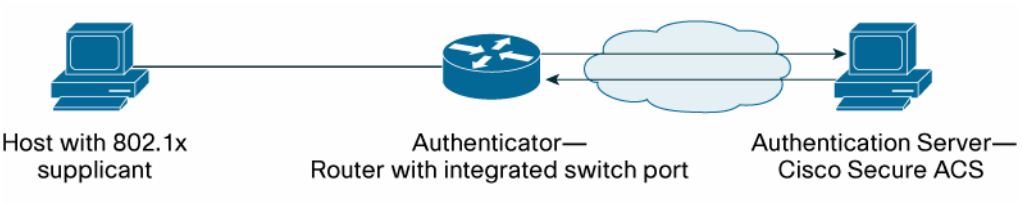
Overview

Using this feature, each device getting connected to the switch ports of the CVO spoke router is authenticated. Depending on the outcome of the authentication process, the port is enabled or disabled. Optionally, the port can be placed in a different VLAN with different access permissions.

In the CVO solution, two VLANs are configured on each spoke. One is called trusted VLAN (e.g. VLAN 10) where all the authenticated hosts are connected. Unauthenticated hosts are connected to the non-trusted VLAN (e.g. VLAN 20). The trusted VLAN is the default VLAN of the switch ports.

There are three main components in the 802.1x-based port authentication. They are the supplicant, authenticator, and RADIUS server (Figure 2).

Figure 1. 802.1x Components



The supplicant is the 802.1x client that runs on the device that needs to be authenticated. Supplicant support may come as part of the operating system or as third-party software. Care should be taken not to run multiple supplicants at the same time. The authenticator is the CVO spoke router and the authentication server is a Cisco Secure Access Control Server (ACS).

When a new IP host is connected to the switch port, the router initiates the communication using Extensible Authentication Protocol over LAN (EAPoL). The supplicant running on the device will respond to it. Then the router proceeds with further authentication. If there is no response from the device it is considered as a clientless device. Once the router gathers the credentials from the device, it is forwarded to the RADIUS server for authentication. If the credentials are valid, the port becomes enabled and gets attached to the trusted VLAN. If the credentials are invalid, the port is shut. If the connected device does not respond to EAPoL messages (clientless device), the port is shut down or assigned to the guest VLAN if it is configured on the port.

On the Cisco Virtual Office spoke router, the computer with valid credentials will go to the primary VLAN and the remaining computers will be assigned to the guest VLAN. This way, the hosts are separated into a trusted or non-trusted category based on the 802.1x authentication status. Only the traffic from the primary VLAN has access to the VPN tunnel. Guest VLAN members can only access the Internet. This separation prevents unsafe hosts from accessing corporate network.

The authentication mechanisms used in CVO deployment are EAP-MD5-Challenge EAP-PEAP and EAP-TLS (other EAP protocols also will work as long as the supplicant and the authentication server supports it). The 802.1x supplicant running on the hosts establishes an EAP session with the Cisco Secure ACS and authenticates itself using username/password credentials. The user account needs to be configured on the Cisco Secure ACS. The supplicant needs to be configured to perform the EAP-MD5-Challenge, EAP-PEAP or EAP-TLS. EAP-PEAP and EAP_TLS can be optionally configured to authenticate the Cisco Secure ACS using digital certificates. In this case the ACS should be pre-loaded with a certificate issued by a Certificate Server. EAP-TLS authenticates end host using digital certificates along with user credentials supplied. So each host should have its own certificate from a Certificate Server which is trusted by the ACS server.

The configuration interface of the supplicants will depend on its vendor and the supported operating system. Supplicants may provide different options to gather the user credentials. It can prompt the user for credentials at the time of authentication, allow the credentials to be preconfigured, or get it from the operating system (Windows login credentials, for example).

The following sections explain in detail the 802.1x features used in the Cisco CVO solution.

802.1x Features

The following configurations are based on a Cisco 1811 Router running Cisco IOS Software Release 12.4(20)T. The hosts are connected to the switch ports (f2 to f9) and the fastethernet0 is connected to the ISP. VLAN 10 is the trusted VLAN and VLAN 20 is the guest VLAN. For other hardware platforms, the sample configurations may need minor modifications. Each port in the switch card is individually configured to enable 802.1x authentication. It is possible to configure some ports with authentication enabled and some without authentication.

Basic Port Authentication

This is the basic mode of operation of this feature. Once the port authentication is enabled, the router asks for credentials before the host can establish network access. If the connected host has an 802.1x supplicant installed, it will respond with the credentials. If the validation is successful, the port will be enabled and be part of the designated VLAN. If the authentication fails, the port is shut down.

(

Sample configuration:

```
aaa new-model
aaa group server radius dot1x
 server-private <ip address> auth-port 1812 acct-port 1813 key 0 <key>
aaa authentication dot1x default group dot1x
! Enable dot1x feature globally
dot1x system-auth-control
!
interface FastEthernet2
 switchport access vlan 10
 ! Enable authenticator functionality
 dot1x pae authenticator
 ! Enable dot1x on this interface
 dot1x port-control auto
 ! Enable periodic re-authentication
 dot1x reauthentication
 ! Re-authentication timeout.
 dot1x timeout reauth-period  120
!
```

The configuration needs to be added to each switch port that needs to do dot1x authentication.

Guest VLAN

Hosts that do not have 802.1x supplicant capability will not be able to respond the EAPoL requests initiated by the router. Normally the port will be shut down if the router identifies that the connected host is clientless. If the guest VLAN feature is enabled, the port will be associated with a different VLAN instead of shutting down.In the following configuration, guest VLAN is configured to be VLAN 20.

```
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 20
```

```
!
```

Single-Host/Multi-Host Mode

The port can be configured to allow only one host or multiple hosts connecting to it. In single-host mode, only one host will be allowed to connect to the port. In multi-host mode, more than one host can be connected to the port using an Ethernet hub attached to it. A single host directly connected to the port also will work in multi-host mode. Single-host mode is enabled by default. It should be noted that in multi-host mode, the authentication status of the connected port is determined by the first host which does the authentication process. If the first host is authenticated then rest of the hosts also gets the same access. If the authentication failed for the first host then the remaining hosts also get the same limited access. It is recommended to use single-host mode. It is more secure to allow only one authorized host per port than to share one authorized port with potentially unauthorized hosts.

```
interface FastEthernet2
 dot1x host-mode single-host
 ! “dot1x host-mode multi-host” is the other option
```

Forced Authorization/Unauthorization

By enabling forced authorization on a port, the clientless hosts can connect to it and still be part of the trusted VLAN. This has the same effect as not enabling dot1x on the port. This can be particularly useful if a user wants to connect an IP phone or other device that does not have a supplicant but still needs to be part of the secure VLAN. Any host can be connected to this port and be part of the secure VLAN without going through 802.1x authentication. Similarly, the port can be forced to be unauthorized. This has the same effect as shutting down the port.

```
interface FastEthernet2
 dot1x port-control force-authorized
 ! “dot1x port-control force-unauthorized” has the opposite effect
```

Re-Authentication

The port can be configured to re-authenticate the hosts periodically. The re-authentication period is also configurable. Periodic re-authentication will remove the hosts from the trusted VLAN if its credentials are removed from the RADIUS server. It may not be helpful to detect if a new user is using the authenticated host, mainly because most of the supplicants cache the credentials once they are entered by the original user. If the Ethernet cable is moved to a new host or the host is rebooted, the switch port will detect Layer-2 termination and clear the associated 802.1x session. This may not be possible if the port is expanded using a hub. A bad user can then spoof the MAC address of the authenticated host on a different host, and try to use the existing 802.1x session. If re-authentication is enabled, the spoofed host can be forced to perform authentication when the re-authentication timer fires.

```
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout reauth-period 600
 dot1x reauthentication
!
```

The timeout can also be initiated by the radius server. The aaa authorization network default group dot1x command gives authority to the network group called dot1x. Dot1x group was defined earlier

with the aaa authentication dot1x default group dot1x.The time out period is defined on the radius server itself.

```
aaa authorization network default group dot1x
interface FastEthernet2
 switchport access vlan 10
 dot1x pae authenticator
 dot1x port-control auto
 dot1x timeout reauth-period server
 dot1x reauthentication
!
```

On the ACS, the time feature is located under Interface Configurations -> RADIUS (IETF) -> select [027] Session Time Out. Depending on which column was selected, session timeout will appear under group settings or user settings and enter a value (in seconds).

Voice VLAN

Using this feature, Cisco IP phones can be placed in a separate VLAN when they are connected to Ethernet switch port. This is not an 802.1x feature. But it is useful because the IP phones may not support 802.1x supplicant. IP phones can be placed in a separate VLAN bypassing 802.1x authentication. That VLAN can be configured to provide only voice access. The voice VLAN can also use the same DHCP pool as the trusted VLAN by using the ip unnumbered Vlan 10 sub-interface command. If an IP phone is a non-Cisco IP phone, the Voice VLAN feature will not work automatically. Using MAC bypass will permit a non-Cisco phone to be placed onto the voice vlan.

```
interface FastEthernet2
 switchport access vlan 10
 switchport voice vlan 11
 dot1x pae authenticator
 dot1x port-control auto
```

Some 802.1x Diagnostic Commands

Table 1. 802.1X Diagnostic Commands

Command	Description
show dot1x	Display 802.1x overview.
show dot1x interface [FastEthernet | Vlan] [interface number]	Display 802.1x status for the specified interface.
show dot1x interface [Fast Ethernet | Vlan] [interface number] detail	Display detailed 802.1x status for the specified interface. This includes the details about the associated clients.
clear dot1x all	Clear all the 802.1x associations.
clear dot1x interface [FastEthernet | Vlan] [interface number]	Clear all the 802.1x associations on a specified interface.
dot1x re-authenticate	Force re-authentication of all existing clients.
dot1x re-authenticate interface [FastEthernet | Vlan] [interface number]	Force re-authentication of clients associated to a specified interface.
debug dot1x all	Enable all 802.1x debugs.

Cisco Secure ACS

This solution involves user credential validation. This is done using a RADIUS server. On the Cisco Virtual Office solution, Cisco Secure ACS 4.0 is used to validate user credentials. The Cisco

Secure ACS is configured to authenticate using “RADIUS (Cisco IOS/PIX 6.0)” mode. Each username and password can be configured on the User Setup interface of Cisco Secure ACS.

Deployment Considerations and Caveats

Hardware and Software Details

The CVO solution is supported on most Cisco integrated services router platforms (880 and above). The 802.x feature described in this document is support on Cisco IOS Software Release 12.4(20)T and later.

End-User Experience

The end-user experience will largely depend on the supplicant used. Many 802.1x supplicants are commercially available now. Some supplicants ask for credentials only when an authentication is in progress. This enables the user to enter the credentials dynamically. However, this requires the user to be present when the authentication is taking place. This may not always be practical.

Some clients need the credentials to be preconfigured as user profiles. This helps the clients to authenticate and establish network connectivity when the computer is still booting up. It also does not require the user to be present when the authentication is in progress. This may not be desirable in some cases where security procedures require the computer to be authenticated only after the end user logs into it. The supplicant could fulfill this requirement by giving an option to delay authentication until boot process is complete. It can also give an option to use operating system login credentials to be used as the 802.1x credentials.

DHCP Integration

Some supplicants have integration with the DHCP process running on the host. This gives an option to send DHCP requests only after the authentication process is completed. This way the computer will get IP address from the right DHCP address pool associated with trusted or nontrusted VLANs.

Client Initiated Re-Authentication

Some supplicants allow the users to initiate a re-authentication from the host side. This can be useful when the end user changes the credentials and wants to apply the new credentials for the authentication. Depending on the previous status, the host could move from a nontrusted VLAN to trusted VLAN, or vice versa.

Zone-Based Firewall

Zone-Based Policy Firewall (ZFW) is a new way to configure and deploy firewall policies. Firewall policies are applied to different zones. Each zone is made up of different interfaces with different network privileges. Traffic between each zone is blocked until a policy is set to allow traffic between two zones. In CVO, each VLAN and the FastEthernet 4 interfaces are in different zones. 802.1x will place the connected device in its appropriate VLAN, authenticated devices in VLAN 10, IP Phones in VLAN 11 and guests in VLAN 20. Once the devices are connected, ZFW will will either permit or deny traffic between zones based on the ZFW policies. Advanced Layered Security guide has more information on ZFW description and ZFW configurations.

Connecting Behind Cisco IP Phone

Cisco IP Phone does forward EAP messages during the 802.1x process. Connecting behind the phone will prompt for user credentials. With correct credentials the end user will be granted

access. A guess pc will not be able to connect behind the phone after a corporate pc authenticates.

Adding a Hub or a Switch behind CVO router

A home user might add a switch or a hub behind the CVO router to increase the number of ports. If a switch is used, 802.1x will place that port into the guest vlan. A switch is placed in the guest vlan because the switch does not have a supplicant. The switch will not forward any eap messages and therefore all hosts connected to switch will be placed in the guest vlan. A hub will forward all traffic including eap messages. If a guest connects to the hub, the guest will be placed in the guest vlan. If a corporate pc with a supplicant connects right after that, the corporate pc will boot off the guest pc. After the corporate pc disconnects, the guest pc still cannot gain access.

References

1. Cisco Virtual Office: http://www.cisco.com/go/cvo
2. Cisco IOS Software 802.1x information: http://www.cisco.com/warp/public/732/Tech/security/trust/8021x/
3. Cisco IOS Software DMVPN: http://www.cisco.com/go/dmvpn
4. Cisco IOS Software IPsec: http://www.cisco.com/go/ipsec
5. Cisco IOS Firewall resources: http://www.cisco.com/go/firewall
6. Cisco IOS Software documentation: http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm
7. Cisco IOS Software infrastructure security: http://www.cisco.com/go/infrastructure
8. Cisco integrated services routers: http://www.cisco.com/go/isr

Appendix A: 802.1X Sample Configuration

```
aaa new-model

!

aaa group server radius radius-eap

 server-private <deleted> auth-port 1812 acct-port 1813 key <deleted>

aaa authentication dot1x default group dot1x

!

ip dhcp pool

 !Corporate network DHCP pool

 import all

 network 10.10.10. 255.255.255.0

 domain-name mycompany.com

 option 150 ip <IP phone tftp server>

 netbios-name-server <ip addresses>

 dns-server <corporate dns server addresses>
```

```
 default-router 10.10.10.1
!
dhcp pool public
 !Guest DHCP pool
 !Inherit the DHCP parameters from ISP
 import all
 network 10.1.1.0 255.255.255.0
 default-router 10.1.1.1
!
interface FastEthernet 0
 switchport access vlan 10
 switchport voice vlan 11
 dot1x port-control auto
 dot1x timeout reauth-period 60
 dot1x max-req 1
 dot1x reauthentication
 dot1x guest-vlan 20
 spanning-tree portfast
!
interface FastEthernet 1
 switchport access vlan 10
 switchport voice vlan 11
 dot1x port-control auto
 dot1x timeout reauth-period 60
 dot1x max-req 1
 dot1x reauthentication
 dot1x guest-vlan 20
 spanning-tree portfast
!
interface FastEthernet 2
 switchport access vlan 10
 switchport voice vlan 11
```

```
 dot1x port-control auto
 dot1x timeout reauth-period 60
 dot1x max-req 1
 dot1x reauthentication
 dot1x guest-vlan 20
 spanning-tree portfast
!
interface FastEthernet 3
 switchport access vlan 10
 switchport voice vlan 11
 dot1x port-control auto
 dot1x timeout reauth-period 60
 dot1x max-req 1
 dot1x reauthentication
 dot1x guest-vlan 20
 spanning-tree portfast
!
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nbar protocol-discovery
 ip pim sparse-dense-mode
 ip nat inside
 ip inspect test in
 ip virtual-reassembly
 ip tcp adjust-mss 1360
 no autostate
 tms-class
 service-policy input mark_incoming_traffic
!
```

```
interface Vlan11
 ip unnumbered Vlan10
 ip access-group allow_skinny_acl in
 ip nbar protocol-discovery
 ip inspect test in
 no autostate
 service policy input mark_incoming_traffic
!
interface Vlan20
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-dense-mode
 ip nat inside
 ip inspect test in
 ip virtual-reassembly
 no autostate
!
ip access-list extended auth_proxy_acl
 remark --- Auth-Proxy ACL ---------
 permit tcp any 172.16.0.0 0.15.255.255 eq www.443
!
ip access-list extended auth_proxy_inbound_acl
 remark --- Auth-Proxy Inbound ACL -----------
 permit udp any any eq domain
 permit udp any any eq netbios-ns
 permit udp any any eq netbios-dgm
 permit tcp any any eq 2000
 permit udp any any eq tftp
 permit udp any any eq 5060
 permit ip any host 10.10.10.1
 deny   ip any 172.16.0.0 0.15.255.255
 permit ip any any
!
```

```
ip access-list extended fw_acl
 remark ---- DMVPN Firewall ----
 permit esp any any
 permit udp any any eq isakmp
 permit udp any eq isakmp any
 permit udp any eq non500-isakmp any
 permit udp host <addr of public ntp server> eq ntp any
 permit udp host <addr of second public ntp server> eq ntp any
 permit tcp 172.16.0.0 0.0.255.255 any eq 22
 permit eigrp any any
!
ip access-list extended nac_acl
 permit ip any 172.0.0.0 0.255.255.255
 deny ip any any
!
ip access-list extended nac_inbound_acl
 remark --- NAC Inbound ACL ---------
 permit udp any any eq domain
 permit udp any any eq netbios-ns
 permit udp any any eq netbios dgm
 permit ip any host 10.10.10.1
 deny   ip any 172.16.0.0 0.15.255.255
 permit ip any any
!
ip access-list extended nac_ip_phone_acl
 permit ip any any
!
ip access-list extended nat_acl
 deny   ip any <mgmt subnet> <inverse mask>
 permit ip 10.10.10.0 0.0.0.15 any
 permit ip 10.1.1.0 0.0.0.255 any
!
```

```
ip access-list extended smg_acl
 permit ip host 10.10.10.1 <mgmt subnet> <inverse mask>
!
ip access-list extended tidp-acl
 permit ip any any
!
ip access-list extended voice_acl
 permit udp any any eq domain
 permit tcp any any eq 2000
 permit udp any any eq 5060
!
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.