# CISCO

# Enterprise Network Virtualization – Access Control System Assurance Guide

# Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS.  CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Enterprise Network Virtualization Access Control System Assurance Guide*
© 2008 Cisco Systems, Inc. All rights reserved.

# Preface

This document details the findings of the end-to-end validation of a Network Virtualization - Employee, Partner, and Guest Access Control Solution in a customer representative Multilayer Campus network environment.

The system under test included design guidance from the following design guides:

- Network Virtualization - Access Control Design Guide
- Network Virtualization - Guest and Partner Access Deployment Guide

*Table 1*      *Modification History*

| Date | Comment |
|------|---------|
| September 12, 2008 | Initial Release |

# Definitions

This section defines words, acronyms, and actions that may not be readily understood.

| Term | Definition |
|------|------------|
| 802.1D | Spanning Tree Protocol (STP, IEEE 802.1D) standard |
| 802.1w | Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) |
| 802.1Q | Industry-standard trunking encapsulation (IEEE 802.1Q) |
| ACS | Access Control Server |
| AS | Autonomous System |
| BGP | Border Gateway Protocol: Inter-domain routing protocol that exchanges reachability information with other BGP systems |
| BPDU | Bridge Protocol Data Unit |
| CA | certificate authority |
| CE | customer edge router; a router that is part of a customer network and that interfaces to a Provider Edge (PE) router. CE routers are not aware of associated VPNs. |
| CEF | Cisco Express Forwarding |
| CSSC | Cisco Secure Service Client |
| CUCM | Cisco Unified Communications Manager |

| Term | Definition |
|------|-----------|
| CVD | Cisco Validated Design |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| EAP | Extensible Authentication Protocol (RFC-5216) |
| ECMP | Equal Cost Multipath |
| EIGRP | Enhanced Interior Gateway Routing Protocol |
| FTP | File Transfer Protocol |
| GRE | generic routing encapsulation |
| HTTP | Hypertext Transfer Protocol |
| IGP | Interior Gateway Protocol |
| LDP | Label Distribution Protocol |
| MAB | MAC Authentication Bypass |
| MD5 | Message Digest 5 (RFC 3748) |
| MP-iBGP | Multiprotocol internal BGP |
| MPLS | Multiprotocol Label Switching |
| P | provider router; A router that is part of a service provider's network resides inside the core of the service provider and provides interconnectivity to PE routers |
| PE | provider edge router; a router that is part of a service provider network connected to a customer edge (CE) router. All VPN processing occurs in the PE router |
| PEAP-MSCHAPv2 | Microsoft Challenge Authentication Protocol v2 |
| PIN | place in network |
| PKI | public key infrastructure |
| POP3 | Post Office Protocol 3 |
| PPS | Packet per Second |
| QoS | Quality of Services |
| RAC | RADIUS Authorization Component |
| RADIUS | Remote Authentication Dial-in User Service |
| SONA | Cisco Service Oriented Network Architecture |
| SP | service provider |
| SRND | Solution Reference Network Design |
| StackWise | stack of switches are united into a single logical unit using special stack |
| STP | Spanning Tree Protocol |
| SVI | Switch Virtual Interface |
| TLS | Transport Layer Security |
| UDLD | Unidirectional Link Detect Protocol |
| VLAN | virtual LAN |

| Term | Definition |
|------|------------|
| VPN | virtual private network; a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone. |
| VRF | VPN routing/forwarding instance; a VRF comprises an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. |

# C O N T E N T S

**F I G U R E S**

# **T A B L E S**

# Executive Summary

This document details the findings of the end-to-end validation of the Enterprise Network Virtualization – Access Control Solution in a customer representative Multilayer Campus network environment. This solution validation was executed using MPLS/VPN for Path Isolation within the Network Virtualization architecture. Refer to the Enterprise Network Virtualization - Path Isolation System Assurance Guide for more information on implementing MPLS/VPN Path Isolation.

Enterprise customers require virtualized and secure network access for partners, vendors, contractors, and guests in order to increase productivity, collaboration, and optimize the return on the investment of their IT infrastructure. While there are a number of advanced technologies under development to address market needs more comprehensively, Network Virtualization is capable of meeting a number of key requirements today while maintaining our competitive position.

The business value provided to our Enterprise customers will be their ability to tightly integrate with their vendors and partners by:

- extending network services to guests and partners.
- extending access anywhere and anytime.
- securing the access through the segmentation of users and resources.

The Cisco Validated Design Program (CVD) consists of systems and solutions that are designed, tested, and documented to facilitate faster, more reliable and more predictable customer deployments. These designs incorporate a wide range of technologies and products into a broad portfolio of solutions that meet the needs of our customers. For more information on the Cisco CVD program, refer to:

http://cisco.com/en/US/partner/netsol/ns741/networking_solutions_program_home.html

The test activity on which this document is based supports the goals of the Cisco Validated Design program by extending coverage of CVDs, combining CVDs, and exploring interactions between them, as well as developing sustaining, to extend the lifecycle of the Network Systems in a customer representative environment. The extended coverage of designs, combined with sustaining capability result in recommended releases that ensure improved quality and a successful customer deployment experience.

The test program was executed by following a formal test process that ensures consistency of operation, quality of results and value for our customers.

The following are the key aspects of the test process:

- All collateral is reviewed and updated for general deployment.
- Solution requirements are tested and results are documented according to a formal process that includes a cross-functional team of stakeholders.

- High quality standards are met (Zero observable operationally impacting defects within the given test parameters, that is, no defects that have not been resolved either outright through software change, redesign, or workaround (refer to reference test plan for specific details)

- A detailed record of the testing conducted is available to customers and field teams, which provides:

    – Design baseline which provides a foundational list of test coverage to accelerate a customer deployment.

    – Software baseline recommendations that are supported by successful testing completion and product roadmap alignment.

- Detailed record of the associated test activity that includes configuration, traffic profiles, memory and CPU profiling, and expected results as compared to actual testing results. Design recommendations and test results undergo detailed review by Subject Matter Experts (SMEs) within each technology area.

As an integral part of the CVD System Assurance program, an automated sustaining validation model was created for on-going validation of this design for any upcoming IOS software release on the targeted platforms. This model significantly extends the life of the design, increases customer confidence, and reduces deployment time.

**C H A P T E R** **2**

# Network Virtualization Solution Overview

Network Virtualization is one component of the overall Cisco Service Oriented Network Architecture (SONA) that provides guidelines to accelerate applications, business processes, and profitability. Network Virtualization is a cohesive, extensible architecture that allows customers to logically partition their network infrastructure (as shown in Figure 2-1). Network Virtualization simplifies network operations by enabling customers to securely share a common network infrastructure between groups of users, applications and devices. The use of a common infrastructure places an increased emphasis on security in order to protect assets and satisfy regulatory and privacy concerns.

*Figure 2-1        Network Virtualization Overview*
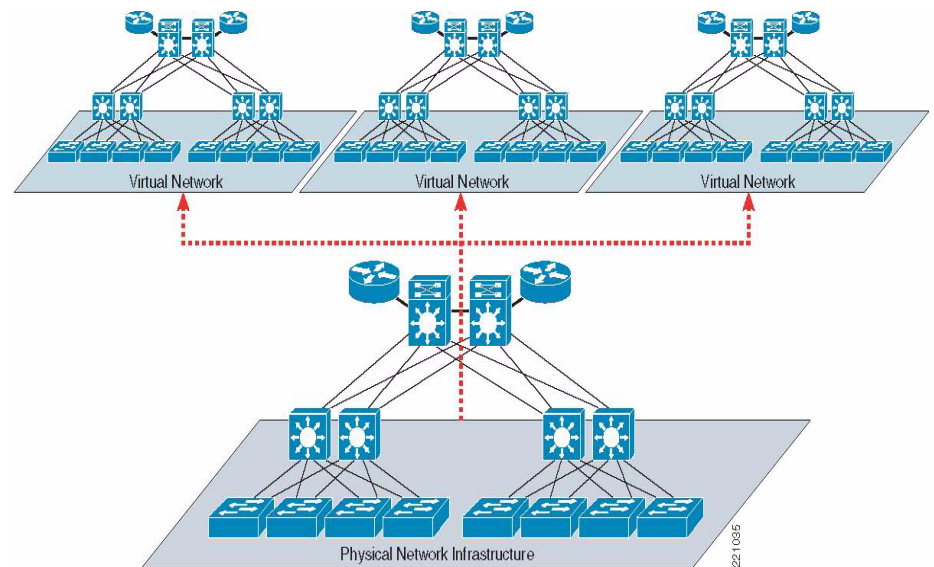


The Network Virtualization architecture has three main components: Access Control, Path Isolation and Services Edge. The components highlighted in Figure 2-2 are dedicated to specific functional areas.

*Figure 2-2        Network Virtualization Framework*
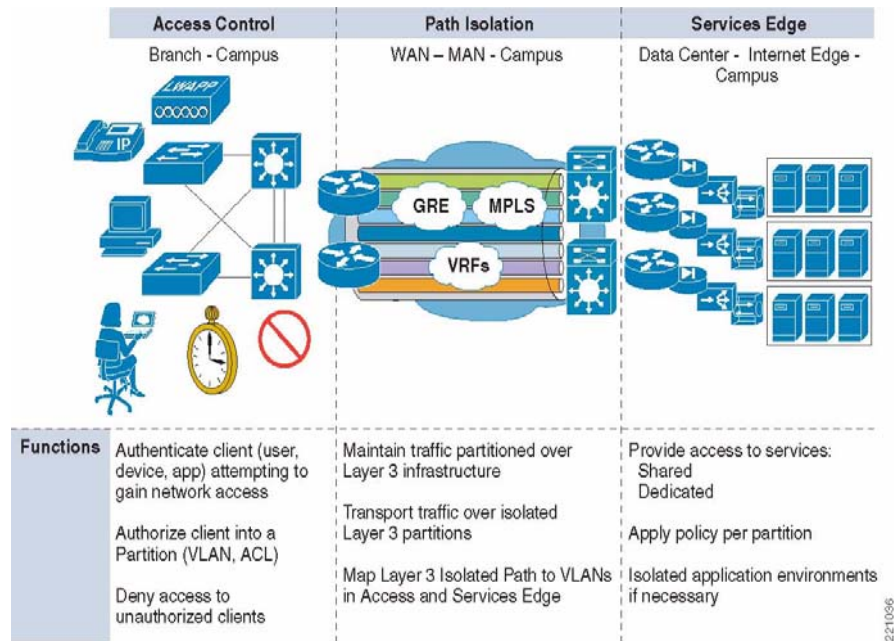


Services Edge is responsible for centralizing policy enforcement points where it is possible to control and restrict communications between separate logical partitions or access to services that can be dedicated or shared between virtual networks.

Path Isolation is an overlay network and refers to the creation of independent logical traffic paths to isolate traffic between users belonging to separate groups (example: Guest and Partners) over a shared physical network infrastructure.

There are two approaches to achieve Path Isolation in the Network Virtualization architecture: Policy based and Control Plane based. The following technologies can be used to achieve Path Isolation: GRE, VRF-Lite, and MPLS VPN. MPLS/VPN technology was implemented due to its scalability and flexibility.

Campus MPLS VPN is an overlay network in a Multilayer Campus environment. MPLS functional roles and positioning of network devices are defined below:

- Provider Edge (PE): Distribution Devices

- Provider (P): Core Devices

- Route Reflector (RR): New Devices with respect to Multilayer Campus Network

- Customer edge (CE): There are actually no true CE devices, because the only devices connecting to the PE are Access Layer switches that perform only L2 functions.

Details about MPLS VPN technology and how to deploy Network Virtualization Path Isolation using MPLS VPN in the Campus can be found in the Network Virtualization – Path Isolation Design guide.

The Access Control function identifies users or devices logging into the network so they can be successfully assigned to the corresponding groups. There are two steps involved in Access Control: (a) Authentication, which is the process of establishing and confirming the identity of the client requesting services. (b) Authorization, in which an endpoint is activated and configured with certain characteristics and policies. When the endpoint is authorized, it will be mapped to an end-to-end virtual network.

# 2.1 Network Virtualization - Access Control Solution

The purpose of access control is to identify different users and device network access requests and to place each endpoint in their respective User groups based on their credentials. Authentication and authorization are the two key mechanisms to provide network based access control. The most efficient and secure technology for both authentication and authorization is IEEE 802.1x. IEEE 802.1x offers an efficient framework to protect a network by authenticating endpoints and administering user traffic. It is an end-to-end solution comprised of multiple components integrated together within the solution. The following are the 802.1x components:

**Supplicant:** A supplicant is an 802.1x enabled client that runs on a device such as a Desktop, Laptop, IP Phone or any workstation. The main function of the supplicant is to send a request to gain access to the network. It also responds to the requests from the switch that is attached to the network. Examples of supplicants are the 802.1x client offered by Microsoft Windows operating system and Cisco Secure Services Client (CSSC).

- Microsoft offers an integrated 802.1x supplicant as part of its XP operating system. The supplicant's behavior is partially configured on the Network Properties page for each interface and partly configured via Registry Settings.

- The Cisco Secure Services Client (CSSC) is Cisco's 802.1x supplicant. CSSC supports user and machine authentication for wired and wireless clients. CSSC is a fully supported 802.1x supplicant with broad Extensible Authentication Protocol (EAP) support and an easy-to-use client interface. CSSC also offers an Enterprise deployment mechanism in which user profiles can be distributed to the entire organization through a single Extensible Markup Language (XML) file.

**Authenticator:**   The authenticator is a device (typically an access switch) that provides connectivity to the Supplicant device based on the authentication status of the device. The authenticator acts as a proxy between the supplicant and the authentication server to exchange EAP messages.

The network solution implemented in this guide uses three Catalyst devices in the Access Layer – Cat 3750 Stackwise, Cat4500 and Cat6500.

The Authenticator is also referred as the "Network Access Device (NAD)".

**Authentication server:**   The authentication server is responsible for authenticating the supplicant. The server receives EAP messages from the supplicant (which are relayed by the authenticator), validating its identity, and based on the identity information, the authentication status is passed on to the supplicant. An example of an authentication server is the Cisco Access Control Server (ACS) that acts as the RADIUS server.

**User database:** The user database is where the user credentials for 802.1x authentication are stored. The database can reside locally on the authentication server or remote to it and both options are supported by ACS. An example of a typical external database server is Microsoft's Active Directory (AD).

For more information related to AD setup, refer to the following link:

Domain Controller Role: Configuring a domain controller

EAP is used to integrate the 802.1x framework components. First, 802.1x defines encapsulation for the transport of EAP traffic between supplicant and authenticator (EAP over LAN, called EAPoL). The authenticator then relays the EAP information to authentication server (EAP over RADIUS). Therefore, EAP provides a way for client and authentication server to negotiate the authentication methods.

There are various EAP methods supported: EAP-Transport Layer Security (EAP-TLS), PEAP-CHAPv2 and Message Digest 5 (MD5). Each EAP method makes different demands on the organization's Public Key Infrastructure (PKI). EAP-TLS requires the most complex PKI and provides highest security to the network. It requires both Certificate Authority's (CA) Root Certificate and Personal Certificate signed by CA. Personal Certificates have two types – machine and user certificates. The 802.1x client can be

setup for machine, user or both authentication requests. PEAP-CHAPv2 requires CA Root Certificate, which requires moderately complex PKI. PEAP-CHAPv2 is the most commonly applied method in today's network. MD5 does not require certificates and is the simplest method and least secure of all.

In summary, 802.1x is a security technology to provide network access solution for Employee, Managed Partner and Guest.

# 2.2  Network Virtualization – Employee, Managed Partner and Guest Access Solution

For today's Enterprise customers the need for secure network access has become more important than ever. In today's diverse workplaces, end-users can be partners, consultants, contractors, vendors and guests who require access to network resources over the same physical media connection as regular employees. As data networks become increasingly indispensable in day-to-day business operations, the potential for unauthorized people will gain access to controlled or confidential information also increases.

One of the most vulnerable points of the network is the Access Layer. The Access Layer is where end users connect to the network. In the past, Enterprise customers have largely relied on physical security to protect this part of the network i.e., (a) authorized users had unlimited network access and (b) unauthorized users were not allowed to enter a secure building where they could plug into the network.

In today's network, users demand network access anywhere and anytime. Once the user is attached to the network, they are granted full access to network resources. An efficient way to secure network access is to use the IEEE 802.1x protocol.

Based on end-user types, Access Control solution provides:

- Employee Access Deployment
- Managed Partner Access Deployment
- Guest Access Deployment

An Employee Access deployment provides unlimited access to the entire network in the Enterprise. Since the 802.1x protocol provides port based security to the access layer, no traffic can pass through the port except EAP traffic. Other traffic can pass through the port only if 802.1x authentication is successful. Any user providing valid employee credentials and is authenticated by the RADIUS server will be authorized and assigned to the employee VLAN which has access to all network resources. The employee network subnets are propagated through the global routing table, and the routes are isolated from other user types (Guest and Partner).

The Managed Partner Access deployment provides network access similar to Employee access. Ports will be dynamically assigned to the Partner VLAN based on the client's credentials. Downloadable ACLs are used with a pre-mapped security policy to provide granular access. There are two differences between Managed Partner Access and Employee Access:

*Table 2-1        Employee and Managed Partner Features*

| Features\User type | Employee | Managed Partner |
|---|---|---|
| Networks | Employee user networks are placed in global routing table. | Partner user networks are placed in Partner VPN. |
| Access levels | Unlimited access: To all the resources in the network including Internet access. | Limited access: To network resources, servers in the data center and Internet access. |

The Guest VLAN functionality provides network access to clients that are not equipped with an 802.1x supplicant. Similar to the Partner VLAN, the Guest VLAN is mapped to a secured MPLS VPN. The Guest VPN will only be granted Internet access.

The Employee and Managed Partner deployment scenarios are validated with the following combinations:

- Auth-failed VLAN

- With IP Phone (Employee Access deployment only)

- Fallback to MAC Authentication Bypass (MAB)

The Auth-failed VLAN provides limited services to clients. These clients are 802.1x compliant and cannot access the employee or partner network due to invalid credentials, resulting in failed authentication. Similar to the Guest VLAN, the Auth-failed VLAN is mapped to a secured MPLS VPN and is only allowed Internet access.

An endpoint could attach to an access switch via an IP phone. Depending on its type, an IP phone will register with the Cisco Unified Communications Manager (CUCM) using different procedures:

- Non-802.1x capable IP phones use CDP to communicate through the voice VLAN configured on a switch.

- 802.1x capable IP phones, which only support MD5 authentication, require the access switch to have "multi-domain" enabled so that both voice and data VLAN can perform 802.1x authentication independently. IP phones are first authenticated against the RADIUS server by an EWAPOL request. After they are authenticated, the IP Phones can communicate with the CUCM.

MAB provides a way to authorize users based on MAC address identity. There are various reasons why MAB is suited for Network Virtualization – Access Control: (a) to provide a supplemental authentication method using EAP standards (b) to provide a supplemental authentication method to integrate and function with 802.1x and (c) some devices in the wired network do not support 802.1x. Therefore, if the device does not have 802.1x software installed, the authentication will timeout. At this point, the MAB authentication process initiates. If the device's MAC address matches with the RADIUS's MAB database, the port will be authorized and assigned to the VLAN based on the MAB database user group association.

The detailed flowchart of 802.1x with combinations of MAC-Auth Bypass (MAB), Auth-Failed VLAN and Guest VLAN are described in each of the following deployment chapters.

**C H A P T E R** **3**

# Network Virtualization - Employee Access Deployment

This section discusses the solution implementation of Network Virtualization – Employee Access deployment in different combinations (Fallback to MAB, Auth-failed VLAN and with IP Phone) in a Multi-layer MPLS/IP Campus environment.

This deployment includes the following components:

- Access control: 802.1x authentication and optional items such as 8021.x Auth-fail VLAN and Fallback to MAC-Auth Bypass (MAB)

- Path Isolation: MPLS/IP

- Services Edge: Dedicated Services of ACS, DNS and Microsoft AD servers.

*Figure 3-1*        *Employee Access Topology*
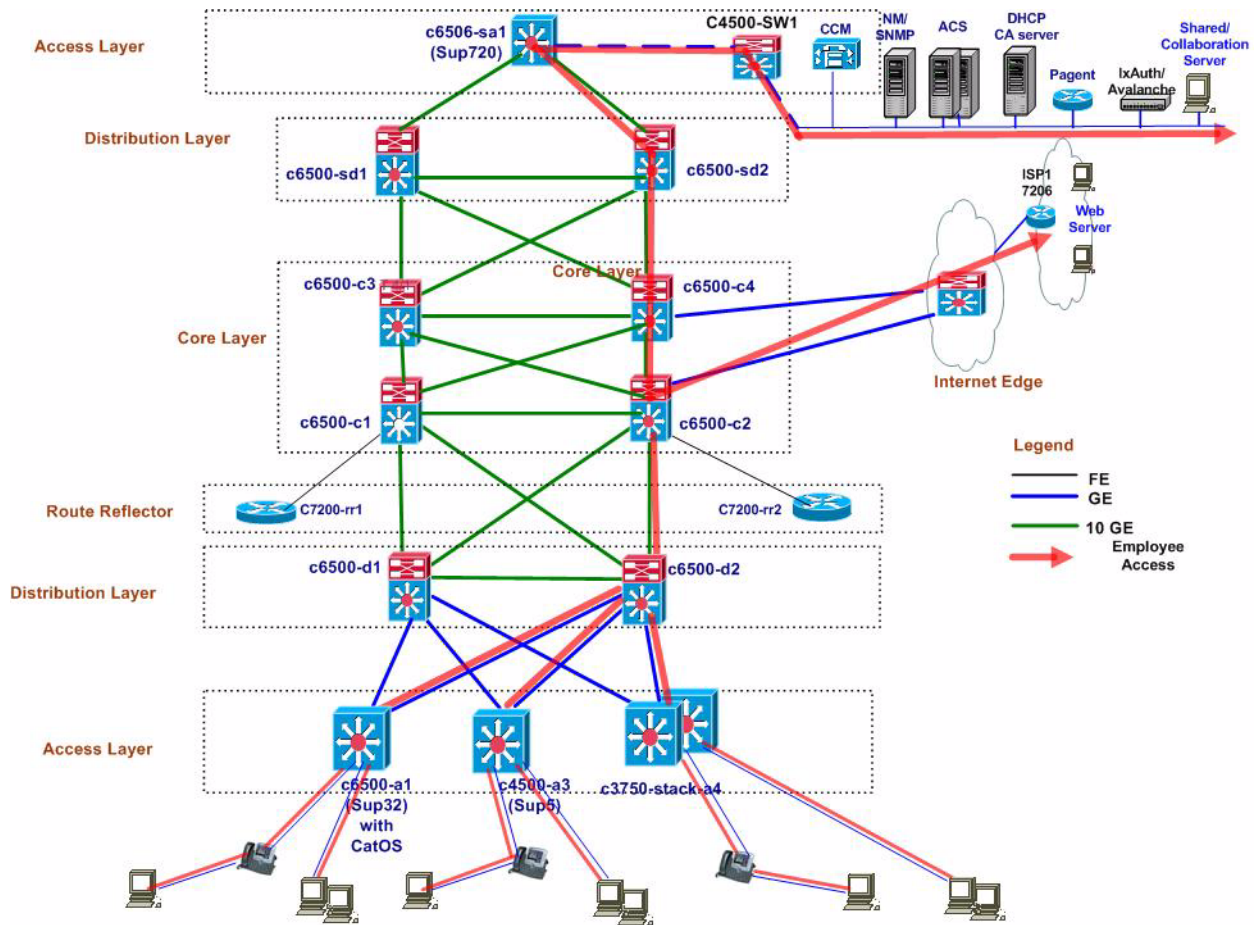


> **Note**    The traffic path that is highlighted in Figure 3-1 indicates one of the paths that users in the employee group can access in the Enterprise Network. The routes for the Employee VLANs are part of the Global routing table. Users and their phones are in Global network for minimal disruption and migration purposes. Only Partners and Guest are in VPN network, making this more evolutionary for network changes.

Figure 3-2 describes the access control flow when users in the Employee group request access to the network.

*Figure 3-2*          ***Flow Chart for Employee Access Deployment***

**802.1x flow in Employee Access Deployment**
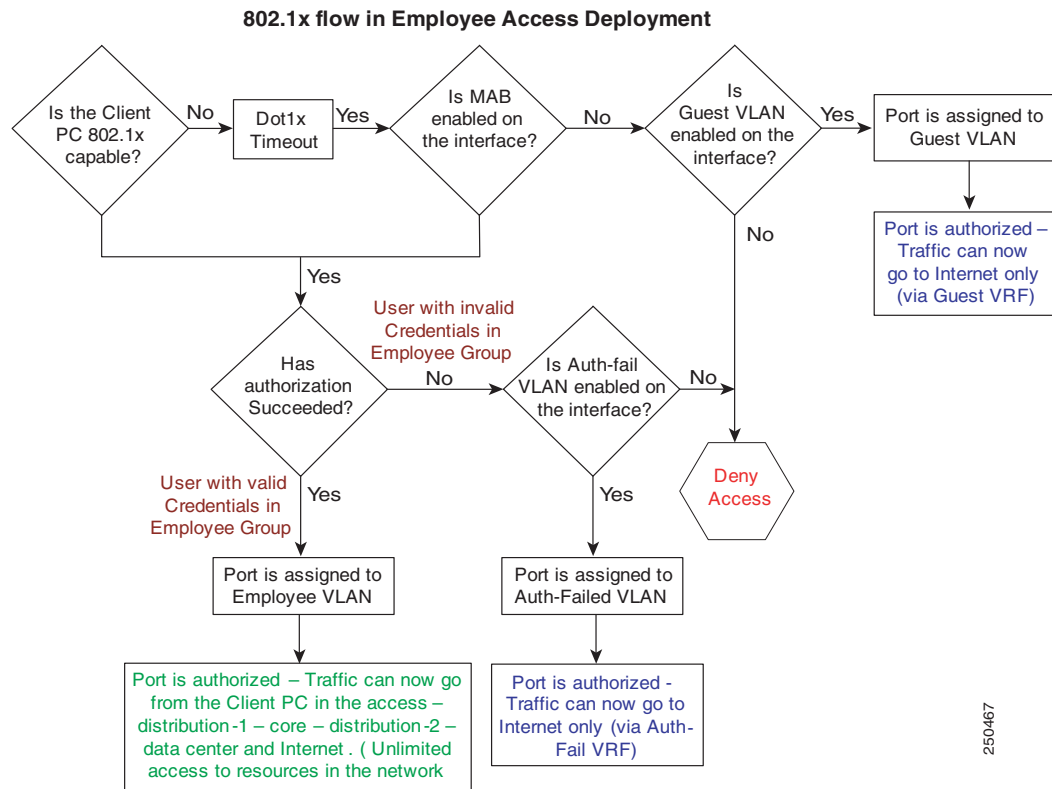
# 3.1  Employee Access Deployment Configuration

The following are assumed to be in place for the successful deployment of Employee Access control solution:

1. Basic network connectivity:

   a. The Access switch (the authenticator) is able to access the ACS server (the authentication server) in the Datacenter.

   b. The necessary NV – Path Isolation configurations are assumed to be in place based on the recommendations from the Enterprise Network Virtualization – Path Isolation System Assurance Guide

2. Authentication servers:

   Two ACS servers (one primary and one secondary) are used to provide fault tolerance for Remote Authentication Dial-In User Service (RADIUS) based authentication. If only one RADIUS server is configured and it becomes unavailable, wired clients cannot connect.

3. Client machines (Wired media):

   a. Windows XP has built-in support for IEEE 802.1X authentication using the Extensible Authentication Protocol (EAP). Windows 2000 supports IEEE 802.1X authentication when the Windows 2000 Service Pack4 (SP4) is installed.

   b. Client machines with Cisco Secure Services Client (CSSC) supplicant enabled.

The following is a summary of the steps required to correctly deploy the Employee Access Control scenario:

1. ACS Server Configuration: There are three basic steps that are needed to be configured in ACS server – Global authentication setup, AAA client setup and user configuration.

2. Microsoft Active Directory (AD) Configuration: User configuration of the Active Database and attaching the user to the domain are the two steps involved in AD.

3. Network Connectivity:   The following configuration must be done in the distribution routers:

   a. L3 configuration for users in the Employee group

   b. HSRP configuration for the L3 interface

   c. Routing protocol configuration for VLANs in the employee group

   d. DHCP configuration

**Note**    The above set of configurations in the distribution routers are additional configurations on top of the ones mentioned in the Enterprise Network Virtualization – Path Isolation System Assurance Guide

4. Access Switch Configuration:

   a. 802.1x configurations on the access ports connected to end device (PC/Mobile device).

   b. AAA configuration

   c. RADIUS configuration

The following are some of the optional configurations that were validated in Employee Access Control Deployment:

### Fallback to MAC Auth Bypass (MAB)

When the user in the employee group has an outdated version of the supplicant software, the user cannot access the network even though the user provides valid credentials. But at the same time, the user has to gain access to get the new version of the supplicant software. To avoid this situation, MAB can be configured. The following steps are necessary to deploy this optional step.

1. On the access switch, enable MAB on the access port.

2. On the ACS, three steps need to complete to create the MAB database associating different users: shared Radius Authorization Component (RAC) and network access profile.

**Note**   The above scenario for MAB was used for validation in the test environment. MAB also provides support for controlled access to the network for non-responsive devices such as printers, video conferencing units, faxes, etc.

### Authentication-Fail VLAN

When the user in the employee group has his/her credentials expired, the user cannot access the network. At the same time, the user has to gain access to update the password. To avoid this situation, Auth-failed VLAN can be configured. The following steps are necessary to deploy this optional step.

1. Distribution router configuration:
   a. VRF configuration
   b. Layer 3 (L3) configuration
   c. DHCP configuration
   d. HSRP configuration for the L3 interface.
   e. Mapping of VRF to the L3 interface.
   f. Exporting VRF through MP-iBGP

2. Access Switch configuration:
   a. RADIUS configuration
   b. 802.1x configurations on the access ports connected to end device (PC/Any mobile device) AAA configuration

### IP Phone interaction in Employee Access Deployment

#### Case 1: non 802.1x supplicant phone

1. On the access switch, enable voice VLAN and support for 802.1x. Configure the interface to support 802.1x multi-host mode.

2. On the distribution router, propagate the voice vlan network into the global routing table. Setup the IP helper address to broadcast traffic to become unicast traffic to Cisco Unified Communications Manager.

**Case 2: 802.1x supplicant phone**

1. On the access switch, enable voice vlan and support 802.1x. Configure the interface to support multi-domain.

2. On the distribution router, propagate the voice vlan network into the global routing table. Setup the IP helper address for broadcast traffic to become unicast traffic to the Cisco Unified Communications Manager.

3. Define the user in the ACS for IP phone.

4. Enable 802.1x on the IP phone

Following are the detailed steps required to properly deploy the Employee access scenario:

### ACS Server Configuration

1. Setup the global authentication method. As part of the EAP negotiation, both authentication server and client will select the first method that they both support.

**2.** Define the AAA client. In order for the access switch to communicate with the ACS server, access switch must be an AAA client for the ACS server.

**Note** This step must be done for each 802.1x enabled access switch.



**3.** Create a group: A group is created and users having the same characteristics are assigned to the same group. A group is a collection of similar users. For example, (a) All users in employee status are assigned and attached to a group named – Employee and (b) All users other than employee status are assigned and attached to a different group – Non-Employee.

a. Radius Attributes selection – There are three Radius attributes that need to be selected:

- Tunnel type – VLAN

- Tunnel Medium – 802

- Tunnel private group-id – Vlan ID (e.g. 201)

4.  Create a user:

    a.   A user is created and a password is selected for this user. (e.g. – 37-emp-md5)

    b.  The authentication method for this user is selected to be – ACS.

    c.  The user is then assigned to the particular group that was created in step1. In this case, the user is assigned to Employee group.

    d.  The rest of the options in the creating the user are left as default.
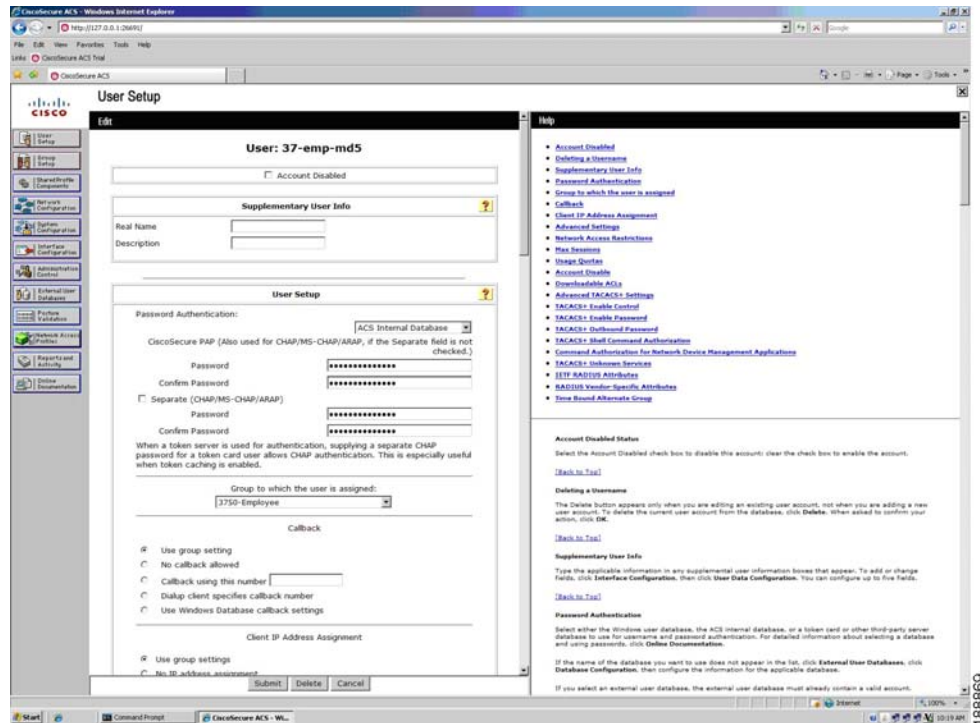


**Note**    User settings override the Group level settings.

**Note**    The preceding configurations are done when the ACS internal database is used to store the user information. Besides the ACS internal database, an external database, such as Microsoft Active Directory (AD), can be used to store user information. The ACS database can be configured to use an external database server in the "User setup" menu under "Password Authentication"; see the preceding screenshot. Microsoft AD configurations are beyond the scope of this document.

**Network Connectivity**

Distribution Switch Configuration:

1.  L2/L3 configuration:

    a.  Map the employee VLAN to its corresponding L3 interface. Following is the configuration:

```
vlan 201
    name employee
    interface vlan201
        description for 6500 employee pc
        ip address 191.0.1.2 255.255.255.0
```

```
standby 201 ip 191.0.1.3
standby 201 timers msec 250 msec 750
standby 201 priority 150
standby 201 preempt
```

2. Routing Protocol configuration:

   a. After the L3 interface is created, the networks should be advertised via an IGP. In this case, EIGRP is configured on the distribution device and so, the network is advertised under EIGRP process.

```
router eigrp 1
network 191.0.1.0 0.0.0.255
```

**Note**    Only configurations relevant to this deployment scenario are mentioned here.

**Note**    DHCP configurations (network address pool assignment) are done in the DHCP server. The DHCP server can be a Windows server running DHCP server services. During system validation, DHCP server feature is configured and enabled on the distribution router (D1, D2). Discussion on detailed DHCP configurations relevant to Microsoft DHCP server is beyond the scope of this document.Only configurations relevant to this deployment scenario are mentioned here.

3. Access Switch Configuration:

   Radius Server configurations:

   a. Enable Authentication, Authorization and Accounting access control model on the switch:

```
aaa new-mode1
```

   b. Specify one or more authentication methods for use on interfaces running IEEE 802.1x:

```
aaa authentication dot1x default group radius
```

   c. Configure ACS server parameters:

```
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key Cisco

aaa new-mode1
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key Cisco
radius-server host 2.2.2.2 auth-port 1812 acct-port 1813 key Cisco1
```

   IEEE 802.1x configurations

   a. Enable IEEE 802.1x port-based access control on the switch:

```
dot1x system-auth-control or set dot1x system-auth-control(CatOS)
```

   b. Set the port access indicator (PAE) type to authenticator:

```
dot1x pae authenticator
```

   c. Enable manual control of the authorization state of a controlled port:

```
dot1x port-control auto or set port dot1x <mod/port> port-control auto(CatOS)
```

   d. Global IOS configuration:

```
dot1x system-auth-control
```

    **e.**  Interface IOS configuration:

```
dot1x pae authenticator
dot1x port-control auto
```

**4.**  Global CatOS configuration:

```
set dot1x system-auth-control
```

Port-level CatOS configuration:

```
set port dot1x 3/20 port-control auto
```

The final interface configuration on the access device for the Employee Access deployment is show below:

IOS configuration:

```
interface GigabitEthernet2/0/1
description testcase emp-3k connect to 3750
    switchport mode access
    dot1x pae authenticator
    dot1x port-control auto
    spanning-tree portfast
    spanning-tree bpduguard enable
end
```

CatOS configuration:

```
#radius
set radius server 191.101.1.111 auth-port 1812
set radius key cisco
#dot1x
set dot1x quiet-period 30
set dot1x tx-period 10
set dot1x radius-accounting enable
set port dot1x 3/47 port-control auto
set spantree portfast 3/47 enable
set spantree bpdu-guard 3/47 enable
set port channel 3/47 mode off
set port dot1x 3/47 guest-vlan 241
```

**5.**  Fallback to MAC Auth Bypass (MAB) configuration (optional):

The following detailed steps enable MAB on the access port on the access switch:

    **a.**  Enable MAB global, this only is only required on CATOS

```
set mac-auth-bypass enable
```

    **b.**  Enable MAB on the access port

On the 6500 CATOS switch

```
Set port mac-auth-bypass <mod/port> enable
```

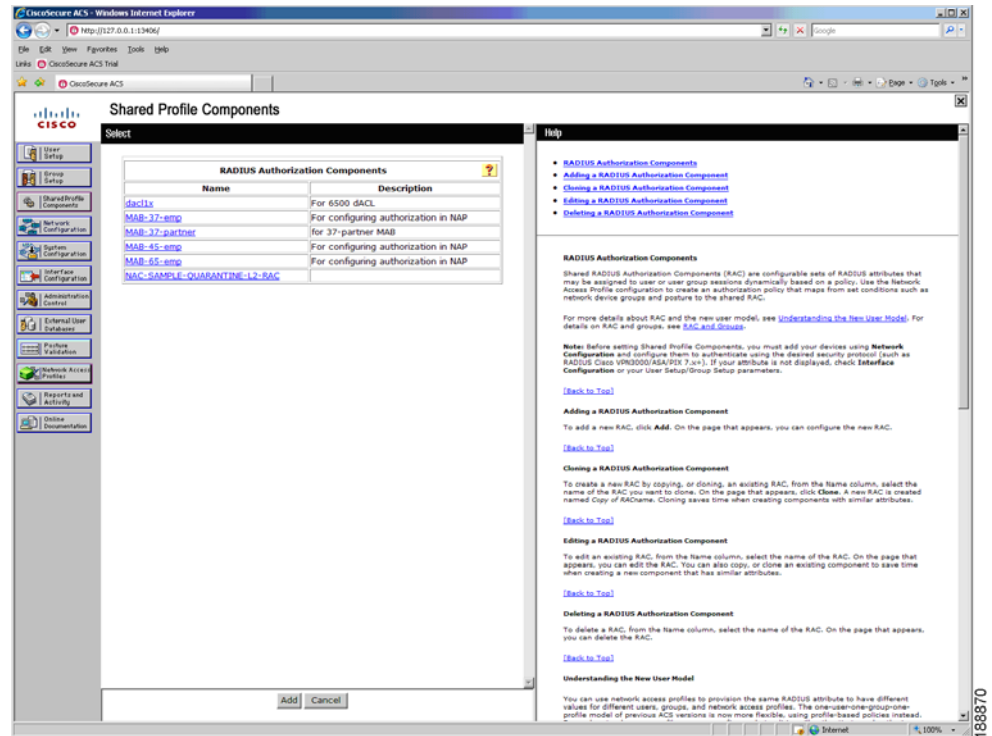On the IOS switch

```
Interface <type> <slot>
    dot1x mac-auth-bypass
```

**MAB Authentication**

Following are the details for setting-up MAB authentication in the ACS:

1.  Set up the shared RAC

    Add the shared RAC by navigating from Shared Profile Components. > Radius Authorization Components. After RAC is created, a new entry will show under the Shared Profile Components.

**2.** After the shared RAC is created, add and submit the following attributes:

```
Tunnel-Type (64) = VLAN
Tunnel-Medium-Type (65) = 802
Tunnel-Private-Group-ID (81) = VLAN ID for Employee
```

The following example shows three attributes that belong to RAC named "MAB-37-emp"

**3.** Set up the network access profile for MAB.

  **a.** Add the network access profile by navigating to Network Access Profile. After the Network Access profile is created, set the MAB to active:

b. Add and submit the following components in the policies inside the network access profile:
Protocols: select the radius (Cisco IOS/PIX6.0) as the protocol type



**Note**    Confirm that the Allow-Agentless-Request-Processing box is checked. (The Allow-Agentless-Request-Processing box is checked in ACS Server settings to indicate that the end-point device (PC/laptop) that is connected to the switchport does not have the supplicant software and the client is using MAB for authentication purposes.)
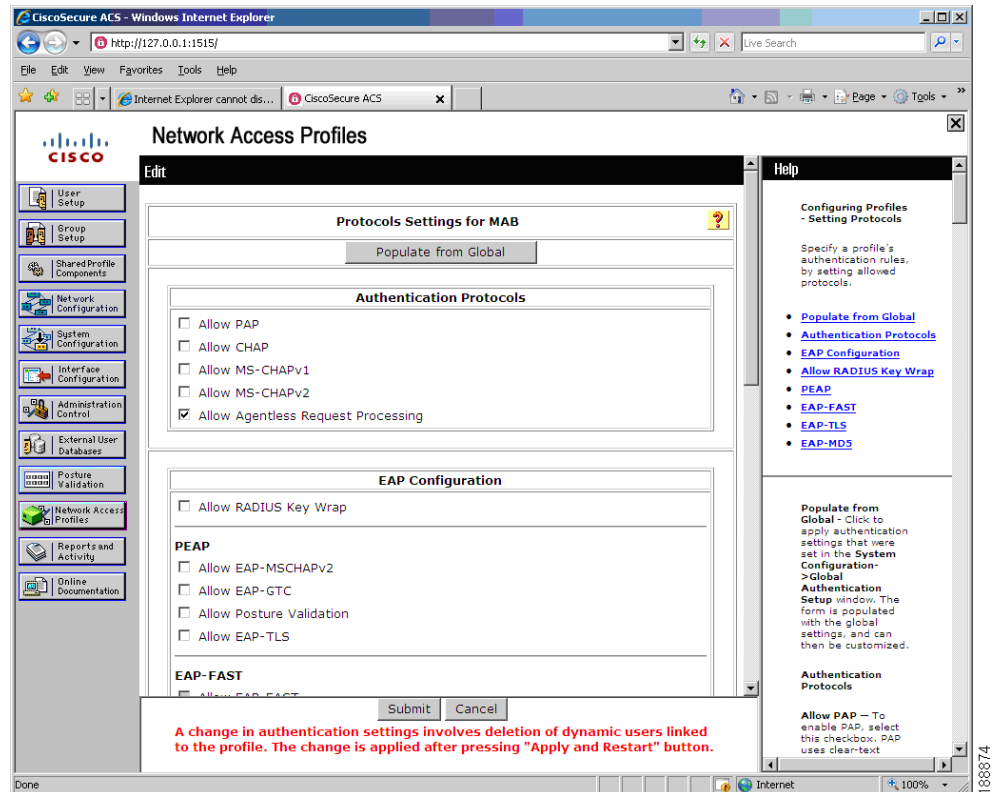
Authentication: The purpose of authentication is to create the MAC DB and associate it with the user group so that MAC address can be authenticated:

- select Authentication MAC to be internal ACS database (ACS DB)

- create each end host MAC entry in the internal ACS DB

- associate the user group for each MAC entry

Authorization: The major purpose of authorization is to create a link between the user group and the RAC that was created in step 1 by adding authorization rules so that once authentication is passed, the user is granted the network access.
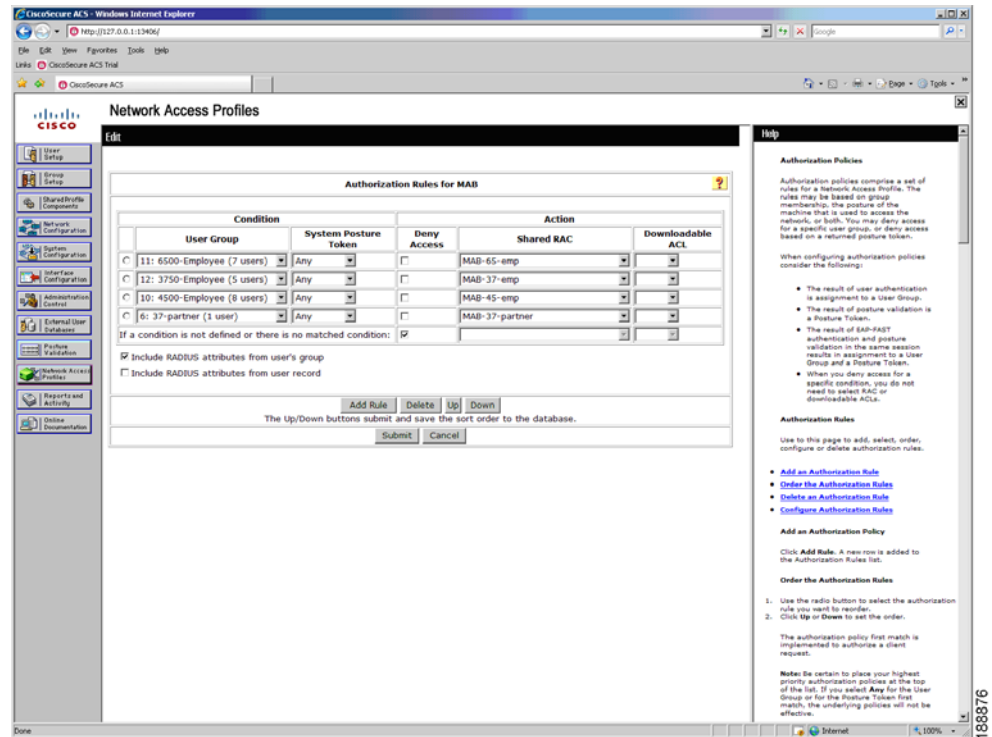
After all components of the policies in a network access profile have been created, add and submit the network access profile. At this point, MAB is ready in the ACS.

The final interface configuration on the access device for Employee Access deployment (with MAC Auth Bypass enabled) is shown below:

IOS configuration:

```
interface GigabitEthernet2/0/1
description testcase emp-3k connect to 3750
    switchport mode access
    dot1x pae authenticator
    dot1x port-control auto
     dot1x mac-auth-bypass
    spanning-tree portfast
    spanning-tree bpduguard enable
end
```

CatOS configuration:

```
set trunk 3/47 off negotiate 1-4094
set port dot1x 3/47 port-control auto
set port dot1x 3/47 guest-vlan 241
set port mac-auth-bypass 3/47 enable
set spantree portfast 3/47 enable
set spantree bpdu-guard 3/47 enable
set port security-acl 3/47 port-based
set security acl map dacl1x 3/47
set port channel 3/47 mode off
```

c.  Authentication-Fail VLAN Configuration (optional): The following are detailed steps involved in the successful deployment of Auth-Fail VLAN option in the Employee Access scenario.

**Network Connectivity**

**Distribution Switch Configuration**

1. VRF configuration:

   a. Create VRF for guest VLAN. The following is the configuration:

   ```
   ip vrf auth-fail-pc
    rd 107:107
    route-target export 107:107
    route-target import 107:107
   ```

**L3 configuration**

1. Map the Auth-Fail VLAN to its corresponding L3 interface.

   ```
   interface Vlan273
    description for 4500 auth-fail-pc
    ip vrf forwarding auth-fail-pc
    ip address 195.0.2.1 255.255.255.0
    standby 233 ip 195.0.2.3
    standby 233 timers msec 250 msec 750
    standby 233 priority 150
    standby 233 preempt
   ```

   After creating the L3 interface for the corresponding Auth-Fail VLAN, the VRF that was created in the previous step is mapped to this interface. Also HSRP is configured under this interface. The router in which the command `standby 245 priority 150` was configured will make it take the role as Active HSRP router, provided the HSRP priority was left as the default for the other distribution router in the topology.

2. Exporting VRF through MP-iBGP: After the L3 interface is created, the networks should be advertised through MP-iBGP protocol.

   ```
   router bgp 64000
    bgp router-id 10.255.254.6
    bgp log-neighbor-changes
    bgp graceful-restart-time 120
    bgp graceful-restart stalepath-time 360
    bgp graceful-restart
    neighbor 10.255.254.9 remote-as 64000
    neighbor 10.255.254.9 update-source Loopback0
    neighbor 10.255.254.10 remote-as 64000
    neighbor 10.255.254.10 update-source Loopback0
    maximum-paths ibgp 2

   address-family ipv4 vrf auth-fail-pc
       redistribute connected
       redistribute static
       no synchronization
       exit-address-family
   ```

**Note**   Configurations necessary for Auth-Fail VLAN deployment are highlighted in a different color.

3. DHCP configuration:

**Note**   DHCP configurations (e.g. network address pool assignment) are done in the DHCP server. The DHCP server can be a Windows server running DHCP server services. During the system validation, the DHCP server feature is configured and enabled on the distribution router (D1,D2). Discussion on detailed DHCP configurations relevant to Microsoft DHCP server is beyond the scope of this document.

**Access Switch Configuration:**

**Interface level IOS configuration**

Enable IEEE 802.1x restricted VLANon the port:

```
dot1x auth-fail-vlan 273
vlan <vlan#> OR set port dot1x <mod/port> auth-fail-Evangeline#> (in CATOS)
```

The final interface configuration on the access device for Employee Access deployment (with Authentication Failed VLAN) is:

**IOS configuration:**

```
interface GigabitEthernet3/20
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x auth-fail vlan 273
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

**CatOS configuration:**

```
set trunk 3/47 off negotiate 1-4094
set port dot1x 3/47 port-control auto
set port dot1x 3/47 guest-vlan 241
set port dot1x 3/47 auth-fail-vlan 271
set spantree portfast 3/47 enable
set spantree bpdu-guard 3/47 enable
set port security-acl 3/47 port-based
set security acl map dacl1x 3/47
set port channel 3/47 mode off
```

**IP Phone configuration (optional)**

The following are the detailed steps needed to ensure proper deployment of supplicantless and 802.1x supplicant IP Phones in the Employee Access scenario:

**Case 1. Non 802.1x supplicant phone:**

1. On the access switch, enable voice VLAN and set the 802.1x mode to multi-domain on the access port.

```
interface GigabitEthernet3/47
 switchport access vlan 203
 switchport mode access
 switchport voice vlan 262
 qos trust cos
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-domain
 spanning-tree portfast
 spanning-tree bpduguard enable
```

2. On the distribution router, propagate the voice VLAN network into the global routing table. Configure IP helper address in the distribution router for the IP Phone to reach the Cisco Unified Communications Manager.

```
interface Vlan262
    ip address 194.0.2.2 255.255.255.0
    ip helper-address 191.101.1.201
 standby 222 ip 194.0.2.3
```

```
standby 222 timers msec 250 msec 750
standby 222 priority 150
standby 222 preempt
```

3. Connect the supplicant PC to IP Phone PC port.

**Case 2. 802.1x supplicant phone:**

1. On the access switch's interface, enable voice VLAN and the 802.1x mode is set to multi-domain.

```
switchport voice vlan 262
dot1x host-mode multi-domain
```

2. On the distribution router, propagate the voice VLAN network into the global routing table. Configure IP helper address in the distribution router for the IP Phone to reach the Cisco Unified Communications Manager.

```
interface Vlan262
    ip address 194.0.2.2 255.255.255.0
    ip helper-address 191.101.1.201
    standby 222 ip 194.0.2.3
    standby 222 timers msec 250 msec 750
    standby 222 priority 150
    standby 222 preempt
```

3. Define the user in the ACS for the IP phone by creating the IP Phone group and edit settings:

   a. Click "Group Setup" in the main menu.

   b. Select an existing group from the drop down list and then select "Rename Group." Rename group to "4500-ip-phone."

   c. Define the IP address pool for the IP Phone under the "IP Assignment" section (pool was previously defined in the distribution router) and enable the "cisco-av-pair" attribute. Select "Edit Settings" and enter "device-traffic-class=voice" as the value for the attribute.

**Create the IP Phone user.**

    **a.** Click on "User Setup" in the main menu.

    **b.** Enter the user name in the 'User' box and click the Add/Edit button.



> **Note**    The user name format should be as follows: *CP-<IP phone type>-SEP<MAC>*

    **c.** Add the newly created user to the "4500-ip-phone" group.

**Enable 802.1x on the IP Phone.**

    **a.** Choose Settings > Security Configuration > 802.1X Authentication > Device Authentication

    **b.** Set the Device Authentication option to Enabled

    **c.** Press the Save softkey

**Specify a password to use with 802.1X authentication on the IP Phone.**

    **a.** Choose Settings > Security Configuration > 802.1X Authentication > Device Authentication > EAP-MD5 > Shared Secret

    **b.** Enter the shared secret

    **c.** Press the Save softkey

Following is the final interface configuration (IOS) on the access device for Employee Access deployment with IP Phone enabled:

```
interface GigabitEthernet3/47
 switchport access vlan 203
 switchport mode access
 switchport voice vlan 262
 qos trust cos
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-domain
 spanning-tree portfast
 spanning-tree bpduguard enable
```

# 3.1.1 Employee Access Deployment Observations

Once the supplicant is connected to the port of the access device (IOS or CatOS) with the above configuration, the following were observed:

1. Upon valid credentials, the end-user is authenticated by the authentication server.

2. The port (in the Access Layer device) connected to the supplicant is granted the VLAN ID based on the attributes in Radius (Dynamic VLAN assignment). The following three RADIUS attributes are used: IETF 64 (Tunnel Type)= VLAN, IETF 65 (Tunnel Medium Type) = 802, and IETF 81 (Tunnel Private Group ID = VLAN ID)

3. The DHCP server will then assign an IP address for this supplicant, which belongs to network (defined in the distribution layer) in the global routing table.

4. Once IP address is obtained, the supplicant can gain access to the all the resources of the network as the credentials match with the employee status.

Employee Access deployment observations with Fallback to MAB enabled: Once the end device (supplicant) gains physical connectivity to the port of the access device (IOS or CatOS) with the MAB configuration listed in the detailed steps section, the following results are observed:

1. After the 802.1x authentication request times out, MAB will be in effect.

2. Once the MAC address that the end device provides matches the entry in the ACS MAC database, the port will be assigned to the Employee VLAN.

3. The DHCP server will then assign an IP address for this supplicant, which belongs to network (defined in the distribution layer) in the global routing table.

4. Once IP address is obtained, the supplicant can gain access to the all the resources of the network as the credentials match with the employee status.

Employee Access Deployment observations with Auth-Failed VLAN option enabled: Once the end device (supplicant) gains physical connection to the port of the access device (IOS or CatOS) with the Auth-Failed VLAN configuration listed in the detailed steps section, the following results are observed:

1. Supplicant will be prompted for credentials, by default every 60 seconds 3 consecutive times.

2. Due to lack of valid credentials or omission of credentials, the supplicant access port will be placed into the Auth-Fail VLAN.

3. The DHCP server will then assign an IP address for this device, which belongs to network (defined in the distribution layer) in the Auth-Fail VPN.

4. Once IP address is obtained, the end device gains limited network access (e.g. Internet access) as defined by Auth-Fail VLAN policy.

Employee Access Deployment observations with IP Phone option enabled: Once the end device (supplicant) gains a physical connection to the port of the access device (IOS or CatOS) with the configuration listed in the detailed steps section, the following results are observed:

### Case 1. Non 802.1x supplicant phone

1. When valid credentials are provided, the end-user (supplicant) is authenticated by the authentication server (ACS) and granted access to network resources.

2. The non 802.1x supplicant IP Phone successfully registers with the Cisco Unified Communications Manager.

   3. Both the Data and Voice VLANs are granted network access.

**Case 2. 802.1x supplicant phone**

1. Upon valid authentication of the end-user and IP Phone by the authentication server (ACS), access is granted to network resources.

2. The 802.1x supplicant IP Phone successfully registers with the Cisco Unified Communications Manager.

3. Both the Data and Voice VLANs are granted network access.

## 3.1.2  Employee Access Deployment Recommendations

1. EAP type selection: The choice of EAP method depends on the customer and is based on the complexity and the level of security needed in the network. See 2.1  Network Virtualization - Access Control Solution for various types of EAP methods.

2. AAA access: Any device with the CLI – "aaa new model requires authentication. This means this command could potential block the access to the device. Two situations can happen: (a) When the session is lost to this router (b) The Radius server is not available. In both of these situations, the administrator will not be able to login to the switch. To prevent this situation from happening, Cisco recommends the following is added to the router configuration

   ```
   aaa authentication login local default group radius enable
   ```

   For more details on this command line usage, refer to Cisco documentation using the link provided: Cisco IOS Security Command Reference

3. RADIUS timer tuning: When using two or more RADIUS servers, CATOS and IOS switches exhibit different behaviors. CATOS supports primary and secondary RADIUS servers. By default, a CatOS access switch sends a periodical keepalive packet to the RADIUS servers every 300 seconds (the default Keepalive Timer). When a keepalive packet gets no response, the following parameters are used to determine the RADIUS server is unreachable: (A) Retransmit, (B) Timeout. When the Retransmit and Timeout expire (the default Retransmit is 2 and Timeout is 5 seconds), the CATOS switch moves the RADIUS server to dead state. Any subsequent access request is then sent to a Secondary/Backup RADIUS server. By default, the dead timer is set to 0, which means the RADIUS server is not marked as dead even it does not respond to any authentication requests. This can cause supplicants to continue to send authentication requests to the dead RADIUS server, and supplicants eventually fail to be authenticated. To reduce convergence through a faster detection of RADIUS servers, the RADIUS Keepalive Timer should be set to 60 seconds.

   In the IOS switch configuration, there is no concept of a primary or secondary RADIUS server. Instead, the switch chooses the best RADIUS server (usually the first configured server). The IOS access switch does not send a periodic keepalive packet by default. When a RADIUS access request gets no response, a Dead-Criteria is used to determine when a RADIUS server is unreachable. The Dead-Criteria has two values: (A) time and (B) tries. After the Dead-Criteria time and tries expire, the RADIUS state is moved to dead. Any subsequent access request is then sent to the second configured RADIUS server. By default, the dead timer is set to 0, which means the RADIUS server is not marked as dead even it does not respond to any authentication requests. This can cause supplicants to continue to send authentication requests to the dead RADIUS server, and supplicants eventually fail to be authenticated. To reduce convergence by faster detection and effective RADIUS server use, automatic testing of the RADIUS server status and RADIUS load balancing should be enabled, and the following timers adjusted: (A) Dead-Criteria time is set to 5 seconds and (B) The Dead-Criteria tries is set to 3. Use the following command to enable automatic server testing and RADIUS load-balance:

   ```
   radius-server host A auth-port aaa acct-port bbb test username testing key 7 XXXXXXXX
   radius-server load-balance method least-outstanding
   ```

4. 802.1x timer tuning: When DHCP and 802.1x authentication is configured (with default DHCP and 802.1x timers), the maximum time it takes for a Microsoft client to get an IP address from the DHCP server may be around seven minutes or longer. This situation is caused by the DHCP timeout that takes place after 60 seconds. In order to get a valid IP address, the dot1x transit timer (tx-timeout) is reduced from 30 seconds (the default) to 10 seconds.

5. Dynamic VLAN assignment: Cisco recommends same configuration on the access port for all different user types, so the port will be dynamically assigned a VLAN ID based on the user credentials.

6. IP Phone Firmware version: Use IP phones running a firmware version that enables them to send the EAPOL-Logoff. Proxy EAPOL – Logoff was introduced in the Cisco 7940 and 7960 phones with firmware 7.2(2) and the Cisco 7911, 7941, 7961, 7970 and 7971 phones in firmware 7.0(1). For more information, refer to:

   http://www.cisco.com/en/US/partner/products/hw/phones/ps379/prod_release_note09186a008046 1f84.html

**Note** When accessing the network by connecting to the port on an IP Phone, no link-down event occurs on the switch port when the PC is later removed. Therefore, the switch is unaware of this event, which poses security vulnerabilities. The capability of the IP phone to send an EAPOL-Logoff message on behalf of the client after it detects a link-down event on the PC port is called proxy EAPOL-Logoff.

# Network Virtualization - Managed Partner Access Deployment

This section discusses the solution implementation of Network Virtualization – Managed Partner Access deployment in different combinations (Fallback to MAB and Auth-failed VLAN) in a Multi-layer MPLS/IP Campus environment.

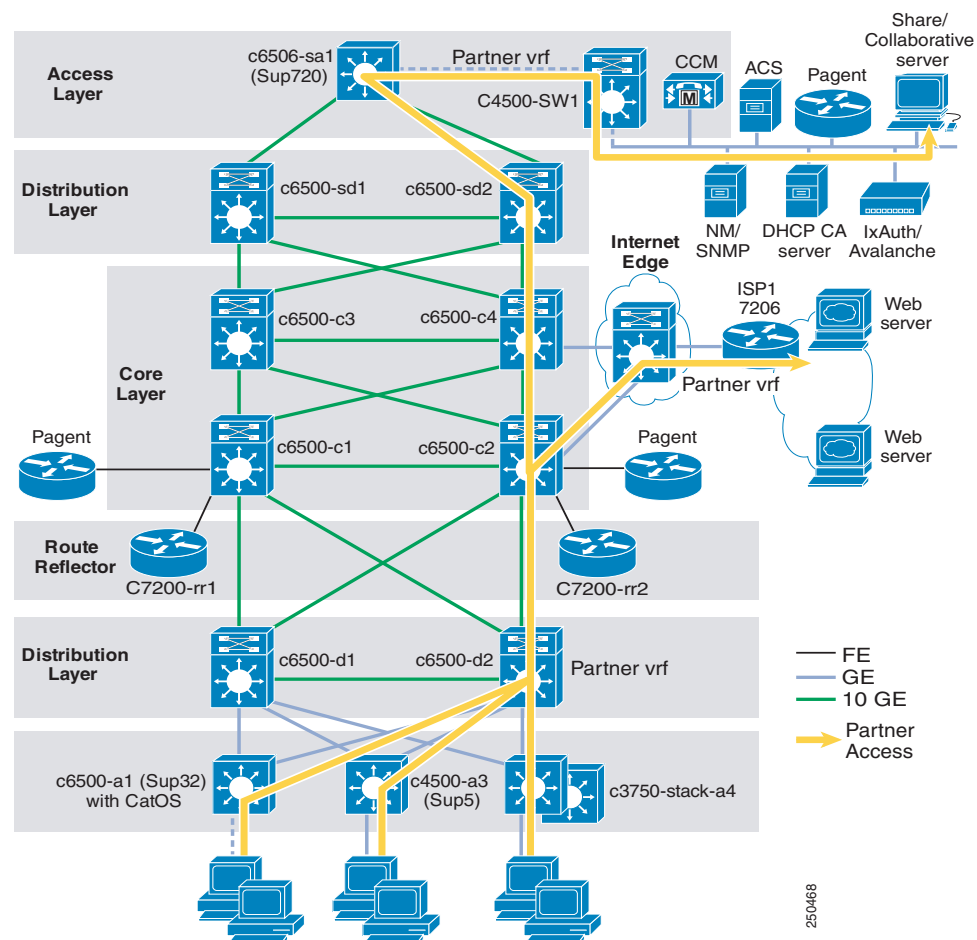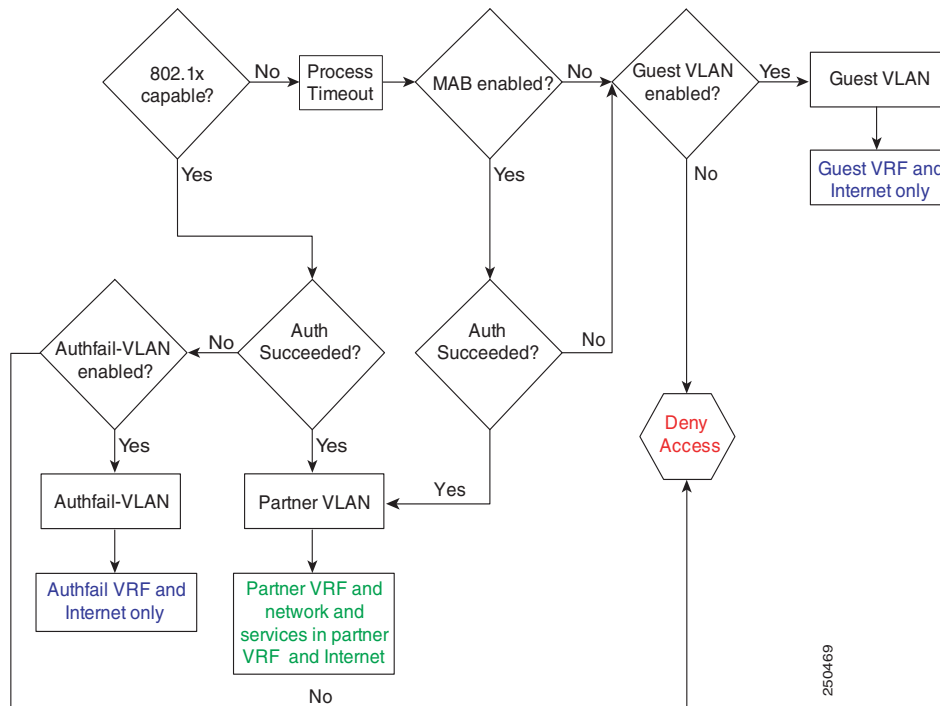*Figure 4-1*      *Managed Partner Access Topology*

*Figure 4-2*        *Managed Partner Access Flowchart*



# 4.1  Managed Partner Access Deployment Configuration

The following steps are assumed to be in place for a successful Managed Partner Access deployment.

1. Network connectivity: campus distribution layer can access the ACS server in the datacenter.

2. 802.1x enabled on the access switch: uniform configuration with 802.1x enable cross all the access ports. This means any access port can be attached by an employee, partner, or guest.

3. Wired Supplicant Client: 802.1x supplicant software are installed in the client pc or laptop.

In addition, partner access requires that the network has MPLS VPN enabled, because Partner networks will only exist in MPLS VPN (VRF) which are separated from Employee's networks that are placed in the global routing table. All the core routers are the P function router and all the distribution routers and Internet Edge routers are the PE function router. Route reflector is recommended for the MPLS VPN in order to separate the data plane and control plane. For detail of MPLS VPN deployment in enterprise campus, refer to Enterprise Network Virtualization - Path Isolation System Assurance Guide.

As was mentioned in Chapter 2, managed partner access is similar to employee access with additional security requests. Therefore, deployment for managed partner access has the same steps as employee access. In addition, one of the major goals of this document is to provide a uniform setup for easy network management. This means that, on the access switch, regardless of whether the end user type is employee, partner or guest, as long as endpoint attaches to an access port, the access switch and Radius server will be sufficiently intelligent to identify the endpoint by its unique credential and only authorize the port to the appropriate privilege.

The following are the summary steps for deploying Managed Partner Access, including the full steps of access control. This procedure deploys managed partner access regardless of whether the network has implemented employee access or not. Meanwhile, this procedure can also be treated as employee access's expansion to managed partner access (both employee access and managed partner access will coexist):

1. Create DHCP scope (pool) for partner access network user in the same employee DHCP server or separate DHCP server.

2. Map the partner access network into Partner VPN in all PE routers and propagate the routes to RR.

3. Inject Internet routes into partner VPN

4. Enable 802.1x authentication on the access switch

5. Create a partner user in the ACS

6. Create a security policy on the 6500 CATOS only

7. (optional) Create dACL in the ACS for the 6500 CATOS access switch

8. (optional) Enable auth-fail VLAN and guest VLAN on the access port of the access switch

9. (optional) Enable MAB on the access port of the access switch

10. (optional) Enable MAB on the ACS

Following are the detailed steps to deploy Managed Partner Access:

1. Create a network address pool for partner access network in the DHCP server.

2. Map the partner network into the partner VRF in all PE routers (include campus distribution routers and Internet edge router) and propagate the routes. Following is an example to map the partner access network "192.0.1.0 /24" into MPLS VRF "partner-pc" on the campus distribution router. Then PE router advertises the routes via Mi-BGP.

```
interface Vlan221
    ip vrf forwarding partner-pc
    ip address 192.0.1.2 255.255.255.0
    standby 221 ip 192.0.1.3

router bgp 64000
address-family ipv4 vrf partner-pc
    redistribute connected
    redistribute static
    no synchronization
    exit-address-family
```

3. Inject Internet route into partner VRF. There are many ways to inject the Internet route into the partner. The following configuration is done on the Internet Edge router to generate a default route into the partner VRF.

```
Router bgp 64000
    Address-family ipv4 vrf partner-pc
        neighbor <neighbor's IP address> default-originate
```

4. Enable the 802.1x authentication on the access switch. Following is the configuration to enable 802.1x authentication, which includes radius server, AAA and 802.1x configurations on the port.

   a. Enable Authentication, Authorization and Accounting access control model on the switch:

```
aaa new-mode1
```

   b. Specify one or more authentication methods for use on interfaces running IEEE 802.1x:

```
aaa authentication dot1x default group radius
```

**c.** Configure ACS server parameters:

```
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key Cisco
```

**d.** Enable IEEE 802.1x port-based access control on the switch:

```
dot1x system-auth-control or set dot1x system-auth-control(CatOS)
```

**e.** Set the port access indicator (PAE) type to authenticator:

```
dot1x pae authenticator
```

**f.** Enable manual control of the authorization state of a controlled port:

```
dot1x port-control auto or set port dot1x <mod/port> port-control auto(CatOS)
```

On CATOS:

```
#radius
set radius server 191.101.1.111 auth-port 1812
set radius server 191.101.1.101 auth-port 1812 primary
set radius auto-initialize enable
set radius key cisco
#dot1x
set dot1x quiet-period 30
set dot1x tx-period 10
set dot1x radius-accounting enable
set port dot1x 1/1 port-control auto
set port dot1x 1/1 multiple-host enable
On the IOS based switch
aaa new-model
!
aaa authentication login default local group radius enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
interface GigabitEthernet3/0/2
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x timeout quiet-period 30
 dot1x timeout tx-period 10
 dot1x reauthentication
 spanning-tree portfast
```

**5.** Create the Partner user in the ACS. This procedure is very similar to the one performed for the user in the Employee group (refer to Chapter 3). The only difference is the value of the attribute - Tunnel-Private-Group-ID (81). The Tunnel-Private-Group-ID should match with the partner network's VLAN ID or VLAN name that is defined in the access switch (e.g. VLAN ID "221") or VLAN name "partner-vlan").

**6.** (Optional) Because managed partner access must be more restricted in its access to available resource, dACL can granularize access policy within a Partner VPN, which can fit for this purpose. Create the security policy on the 6500 CATOS only. dACL is a port based security policy. There are four sub-steps to create the dACL on the 6500 CATOS.

**a.** Configure the basic security ACL with the keyword "downloaded-acl." The following example lists the limited entries that are required:

```
set security acl ip <ACL name> permit arp
set security acl ip <ACL name> permit arp-inspection any any
set security acl ip <ACL name> permit dhcp-snooping
```

```
set security acl ip <ACL name> include downloaded-acl dot1x
```

**Note**    Keyword "downloaded-acl" with "dot1x" as the option, will allow the dACL to merge with basic security ACL on the port, once the authentication is successful.

**b.** Commit the security ACL into the config

```
commit security acl all
```

**c.** Set the access port to port based security ACL

```
set port security-acl <mod/port> port-based
```

**d.** Apply the security ACL on the access port

```
set security acl map <ACL name> <mod/port>
```

Following is an example for implementing dACL on the CATOS Switch:

```
#security ACLs
set security acl comp-opt enable
clear security acl all
set security acl ip dacl1x permit arp
set security acl ip dacl1x permit arp-inspection any any
set security acl ip dacl1x permit dhcp-snooping
set security acl ip dacl1x include downloaded-acl dot1x
commit security acl all
set port security-acl 3/20,3/26,3/47 port-based
set security acl map dacl1x 3/20,3/26,3/47
```

**7.** (Optional) Creating the dACL on the ACS includes two major steps – creating a shared profile component and applying the dACL to the user setup or group setup.

Two components in the shared profile components are involved for setting up the dACL: downloadable IP ACLs and network access filtering.
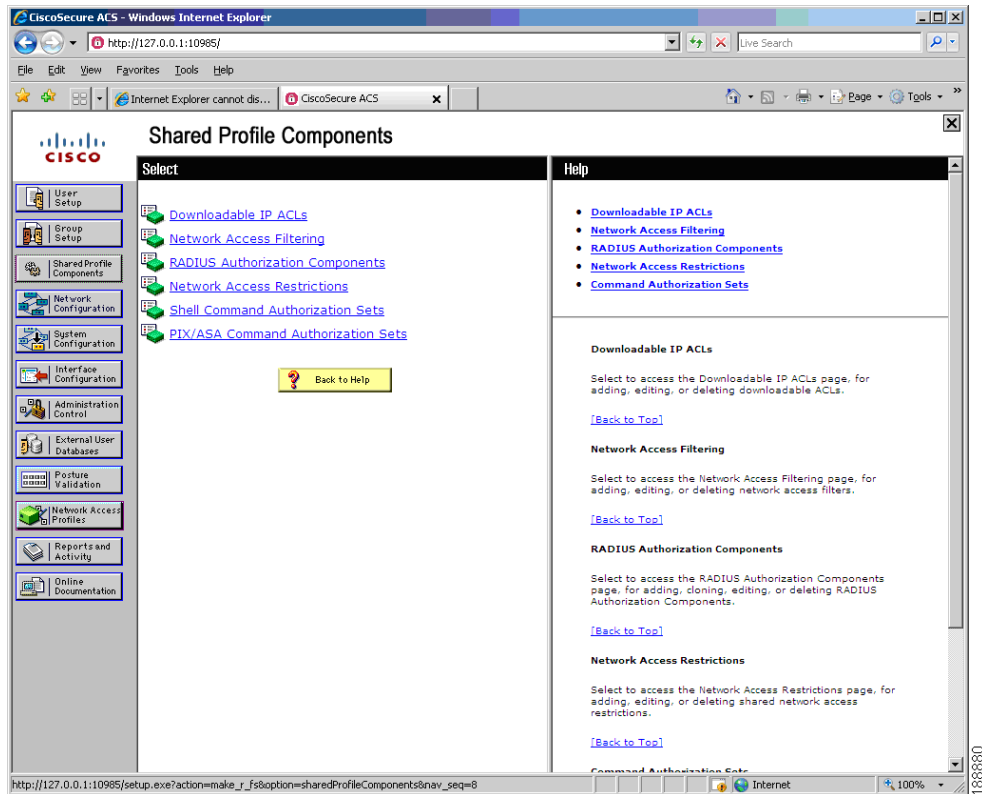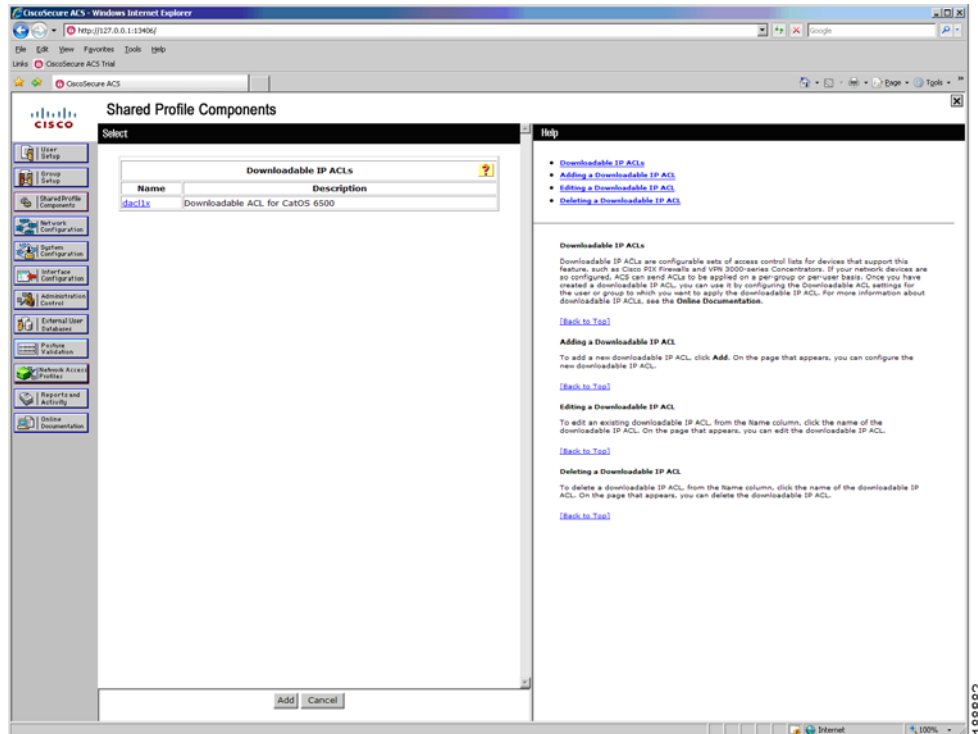
a. Add and submit the dACL by navigating from the shared profile components to the Downloadable IP ACLs. This name needs to match the ACL name that is defined in the 6500 CATOS.
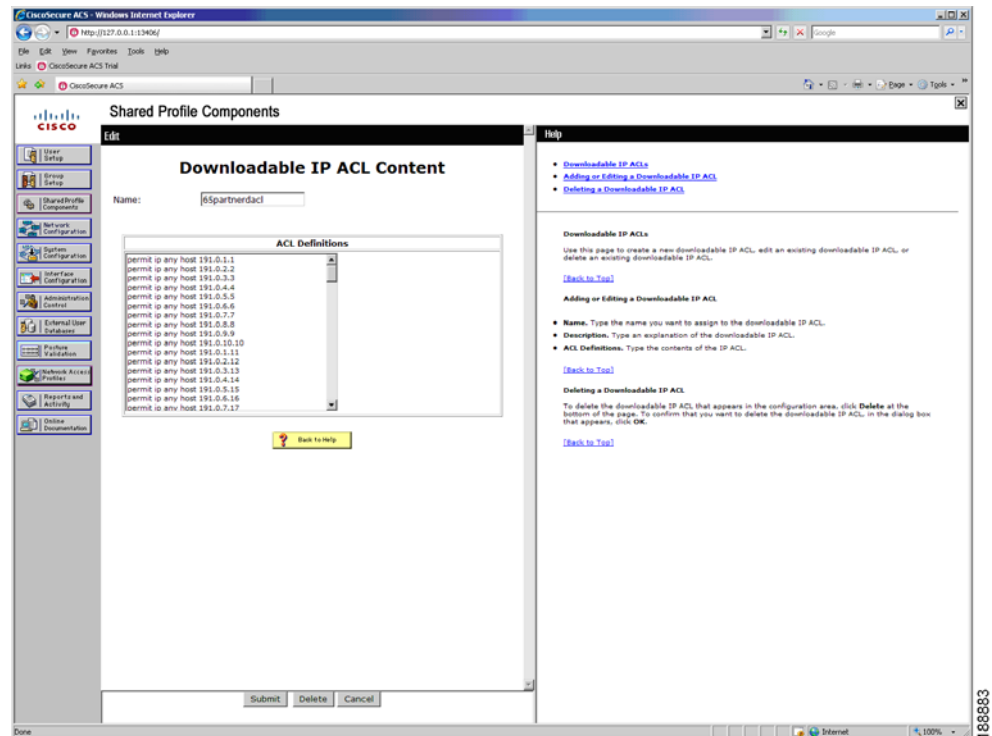
The following screen shot is a sample of the output in ACS server after the downloadable IP ACLs is created:

    **b.** Add the ACE in the downloadable ACL content (click the dACL name will pop up the ACE content page).
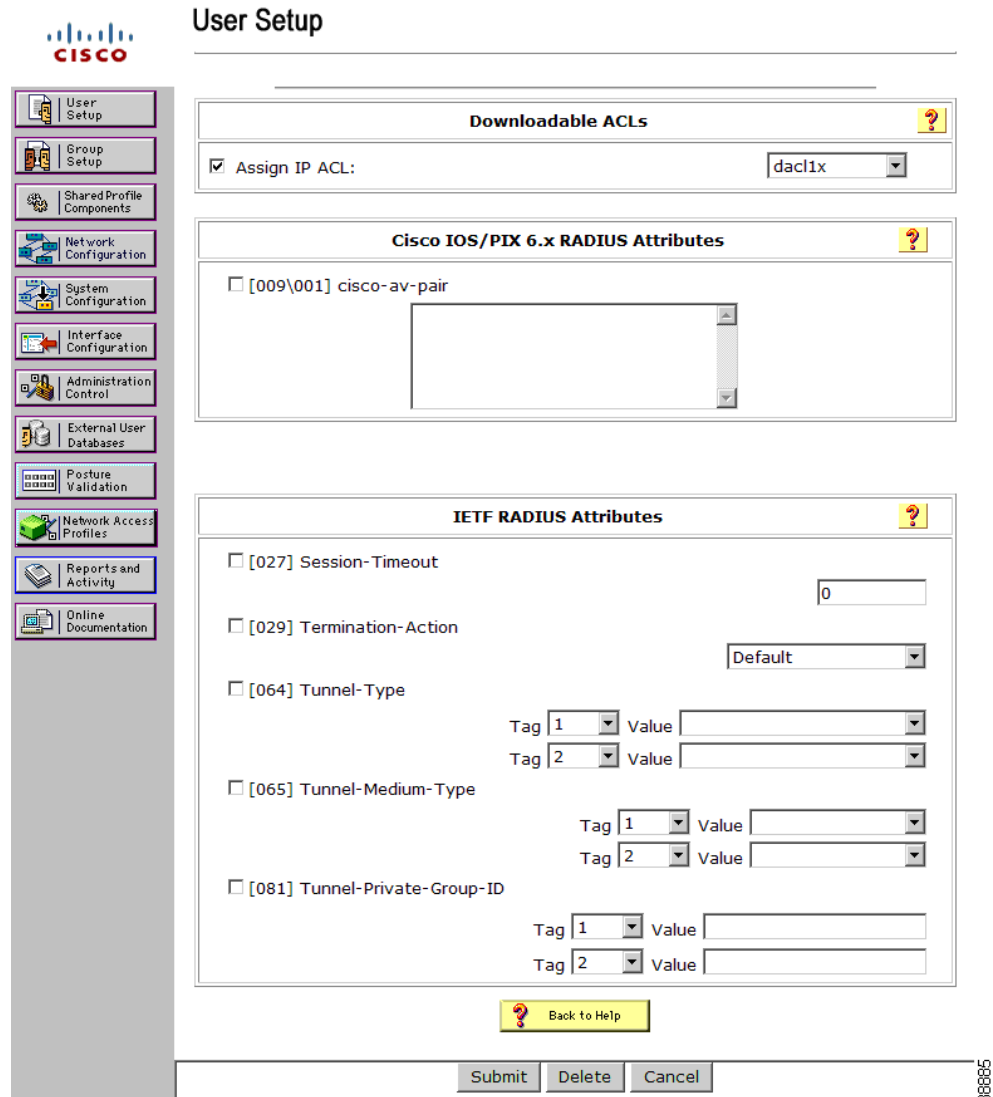
c.  Add and submit network access filter. In the network access filter, define which AAA client will use the dACL function.
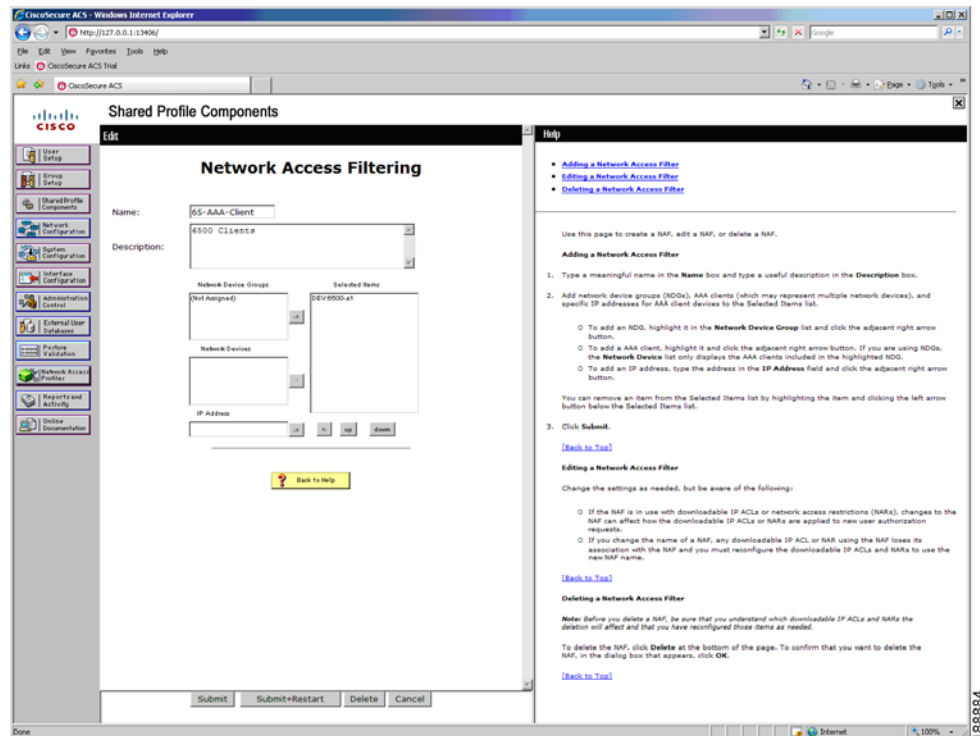


d.  AAA filter is mapped to dACL

e.  Restart the system by navigating from network configuration to Service control.

f.  Apply the dACL to the user setup or group setup.

8. Enable Auth-failed VLAN on the switch. This is an optional step, to provide limited access to the Partner user when invalid credentials are provided.

   a. Enable Auth-Failed VLAN on the access port

   Cat OS configuration:

   ```
   Set port dot1x <mod/port> auth-fail-vlan <vlan#>
   ```

   IOS configuration:

   ```
   dot1x auth-fail vlan 275
   ```

9. Enable MAB on the access switch. This is an optional step, only if MAB is enabled as fallback solution. It includes following sub steps:

   a. Enable MAB global, this only requires on CATOS

   ```
   set mac-auth-bypass enable
   ```

**b.** Step 2. Enable MAB on the access port

On the 6500 CATOS switch

```
Set port mac-auth-bypass <mod/port> enable
```

On the IOS switch

```
Interface <type> <slot>
       dot1x mac-auth-bypass
```

The final configuration on the access device for Managed Partner Access deployment (with MAC Auth Bypass enabled) is shown below:

On CATOS:

```
set trunk 3/47 off negotiate 1-4094
set port dot1x 3/47 port-control auto
set port dot1x 3/47 guest-vlan 241
set port dot1x 3/47 auth-fail-vlan 271
set port mac-auth-bypass 3/47 enable
set spantree portfast 3/47 enable
set spantree bpdu-guard 3/47 enable
set port security-acl 3/47 port-based
set security acl map dacl1x 3/47
set port channel 3/47 mode off
```

On IOS:

```
interface GigabitEthernet4/0/24
 switchport mode access
 dot1x mac-auth-bypass
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x timeout quiet-period 30
 dot1x timeout tx-period 10
 dot1x reauthentication
 dot1x guest-vlan 245
 dot1x auth-fail vlan 275
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping trust
```

**10.** (Optional) Set up MAB on the ACS. This step applies only if MAB is enabled for fallback access. There are two major steps – setup network access profile and setup RAC.

Following are the sub steps for set up the RAC.

**a.** Add and submit the RAC by navigating from shared profile component to RAC
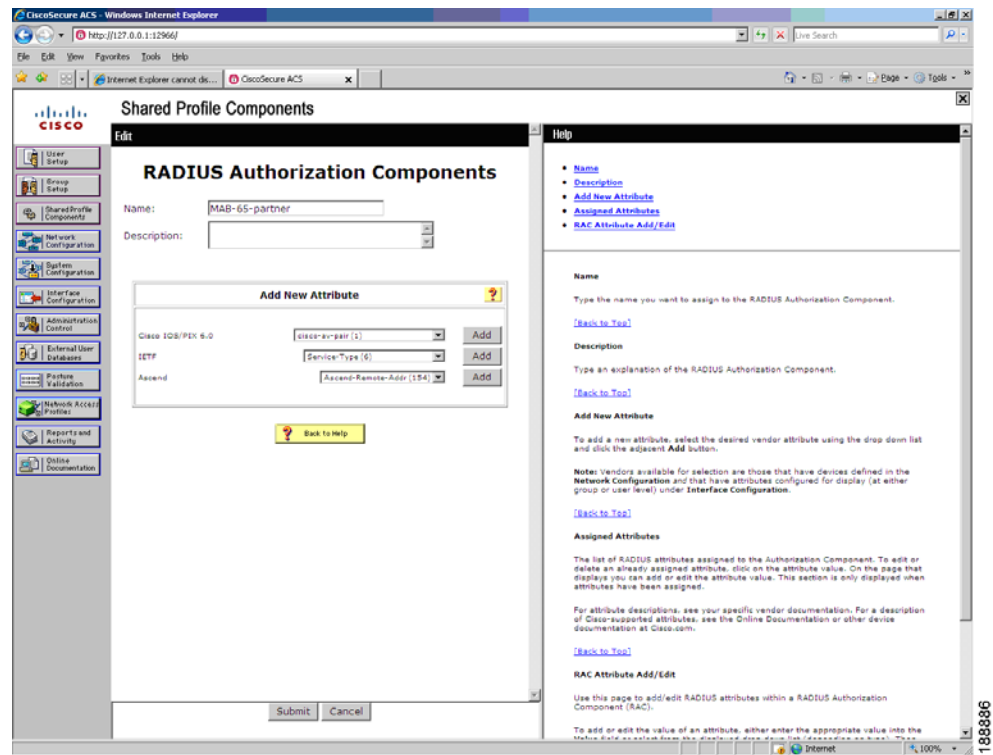
**b.** Add and submit the attributes to RAC (clicking the RAC name will bring the attribute window). Following attributes are required attributes

Tunnel-Type (64) = VLAN

Tunnel-Medium-Type (65) = 802

Tunnel-Private-Group-ID (81) = VLAN ID for partner (e.g.: 221)

Following is the RAC screen shot from the ACS server after the above attributes are added:



Following are the sub steps for setting up network access profile on ACS:

**a.** Create the network access profile and set MAB to active.

**b.** Add and submit the following components in the policies inside the network access profile:

Protocols: select the radius (Cisco IOS/PIX6.0) as the protocol type

After the network access profile is created, the following entry will be displayed:
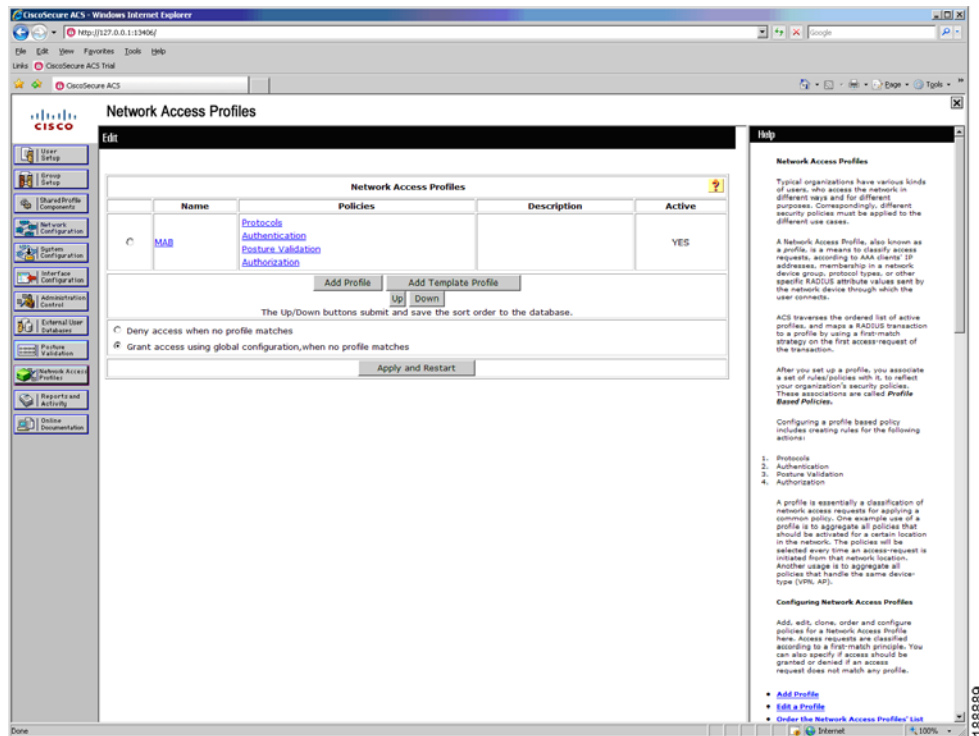


**c.** Make sure that Allow Agentless Request Processing box is checked. (The Allow Agentless Request Processing box is checked in the ACS Server settings, to indicate that the end-point device (PC/laptop) connected to the switchport does not have the supplicant software and the client is using MAB for authentication purposes.)
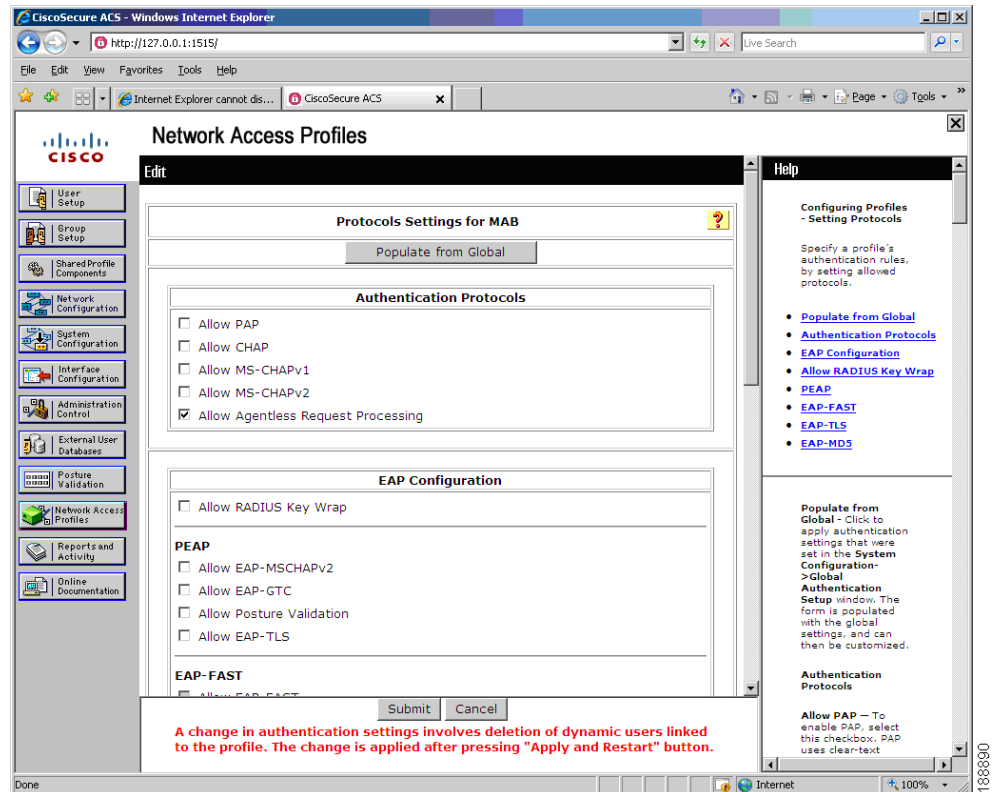
**11.** Define the MAC address for authentication for each partner user and map it to the partner user group.
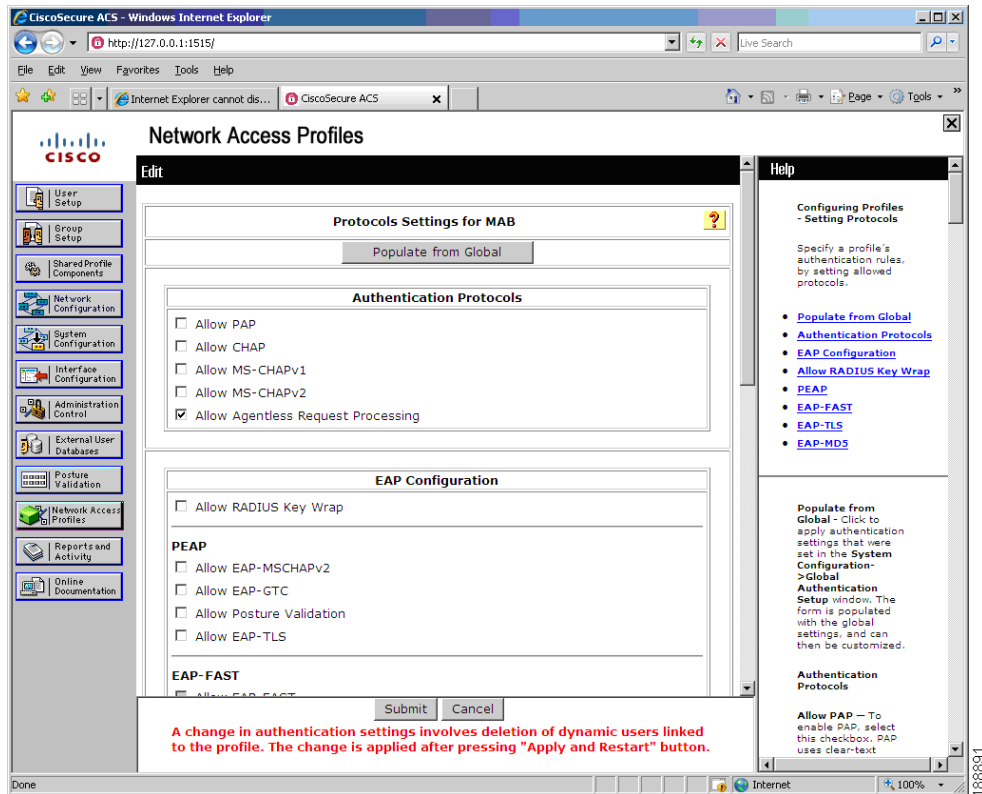
**12.** Add the authorization rule - Map the user group to RAC and dACL.
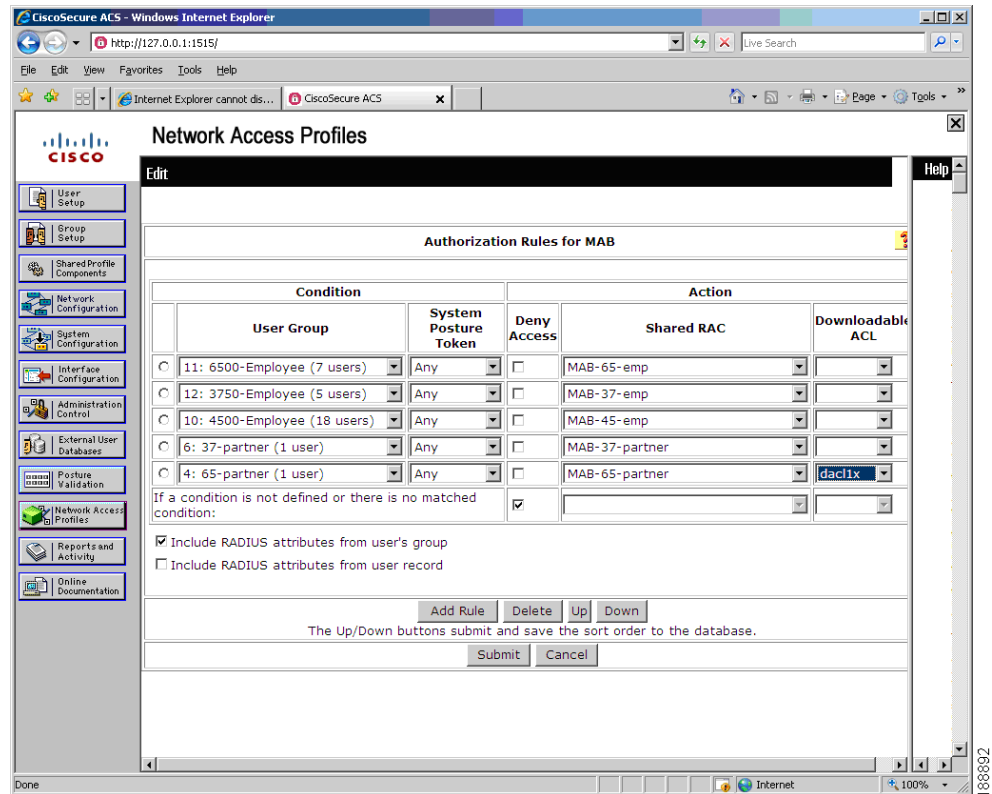


# 4.1.1 Partner Access Deployment Observations

Once the Partner user connects to the access port and enters valid credentials, authentication will be successful and the following results are observed:

**1.** Users can access Partner Servers and the Internet.

**2.** From the access switch, the port should be "AUTHORIZED" by Dot1x and assigned to the Partner VLAN.

**3.** On the CatOS, the downloadable ACL gets attached to the access port to provide an access policy.

**4.** On the DHCP server, a Partner IP address will be assigned to the partner user.

Managed Partner Access deployment observations with Fallback to MAB enabled:  Once the end device (supplicant) gains physical connectivity to the port of the access device (IOS or CatOS) with the MAB configuration listed in the detailed steps section, the following results are observed:

**1.** User can reach partner servers and reach the Internet.

**2.** From the access switch, the port should indicate it has been "AUTHORIZED" by MAB authentication and assigned to the Partner VLAN.

**3.** On the CatOS, the downloadable ACL gets attached to the access port to provide an access policy.

**4.** On the DHCP server, a Partner IP address will be assigned to the partner user.

Managed Partner Access Deployment observations with Auth-Failed VLAN option enabled: Once the end device (supplicant) gains physical connection to the port of the access device (IOS or CatOS) with the Auth-Failed VLAN configuration listed in the detailed steps section, the following results are observed:

1. Users can only access the Internet.

2. On the access switch, the port should indicate it has been "AUTHORIZED" and assigned to the Auth-Failed VLAN.

3.  On the DHCP server, an Auth-fail network IP address will be assigned to the user.

If the partner user does not have supplicant software and the MAC address does not match in the ACS database, the following results are observed:

• Users can only access the Internet.

• On the access switch, the port should indicate it has been "authorized" and assigned to the Guest VLAN.

• On the DHCP server, a Guest network IP address will be assigned to the user.

## 4.1.2  Partner Access Deployment Recommendations

1. Dynamic VLAN assignment: Cisco recommends the same configuration on the access port for all different user types, so the port will be dynamically assigned a VLAN ID based on the user credential.

2. Granularized access policy: dACL can be used to provide Granularized access policy within a Partner VPN. Currently, this feature is only supported on CatOS.

3. 802.1x timer tuning: When DHCP and 802.1x authentication is configured (with default DHCP and 802.1x timers), the maximum time it takes for an user to get an IP address from the DHCP server may be around seven minutes or longer. This situation is caused by the DHCP timeout that takes place after 60 seconds. In the current validation, the dot1x transmit timer (tx-timeout) is reduced from 30 seconds (the default) to 10 seconds.

4. RADIUS timer tuning: When using two or more RADIUS servers, CATOS and IOS switches exhibit different behaviors. CATOS supports primary and secondary RADIUS servers. By default, a CatOS access switch sends a periodical keepalive packet to the RADIUS servers every 300 seconds (the default Keepalive Timer). When a keepalive packet gets no response, the following parameters are used to determine the RADIUS server is unreachable: (A) Retransmit, (B) Timeout. When Retransmit and Timeout expire (by default, Retransmit is 2 and Timeout is 5 seconds), the CATOS switch moves the RADIUS server to dead state. Any subsequent access request is sent to a Secondary/Backup RADIUS server. By default, the dead timer is set to 0, which means the RADIUS server is not marked as dead even it does not respond to any authentication requests. This can cause supplicants to continue to send authentication requests to the dead RADIUS server, and supplicants eventually fail to be authenticated. To reduce convergence through a faster detection of RADIUS servers, the RADIUS Keepalive Timer should be set to 60 seconds.

In the IOS switch configuration, there is no concept of a primary or secondary RADIUS server. Instead, the switch chooses the best RADIUS server (usually the first configured server). The IOS access switch does not send a periodic keepalive packet by default. When a RADIUS access request gets no response, a Dead-Criteria is used to determine when a RADIUS server is unreachable. The Dead-Criteria has two values: (A) time and (B) tries. After the Dead-Criteria time and tries expire, the RADIUS state is moved to dead. Any subsequent access request is then sent to the second configured RADIUS server. By default, the dead timer is set to 0, which means the RADIUS server is not marked as dead even it does not respond to any authentication requests. This can cause

supplicants to continue to send authentication requests to the dead RADIUS server, and supplicants eventually fail to be authenticated. To reduce convergence by faster detection and effective RADIUS server use, automatic testing of the RADIUS server status and RADIUS load balancing should be enabled, and the following timers adjusted: (A) Dead-Criteria time is set to 5 seconds and (B) The Dead-Criteria tries is set to 3. Use the following command to enable automatic server testing and RADIUS load-balance:

```
radius-server host A auth-port aaa acct-port bbb test username testing key 7 XXXXXXXX
radius-server load-balance method least-outstanding
```

**4.1.2   Partner Access Deployment Recommendations**

# Network Virtualization - Guest Access Deployment

This section discusses the solution implementation of Network Virtualization – Access Control – Guest Access deployment in a Multi-layer MPLS/IP Campus environment.

This deployment includes the following components:

- • Access control: IEEE 802.1x with Guest VLAN support
- • Path Isolation: MPLS/VPN
- • Services Edge: Internet access

*Figure 5-1*      ***Guest Access Deployment Topology***
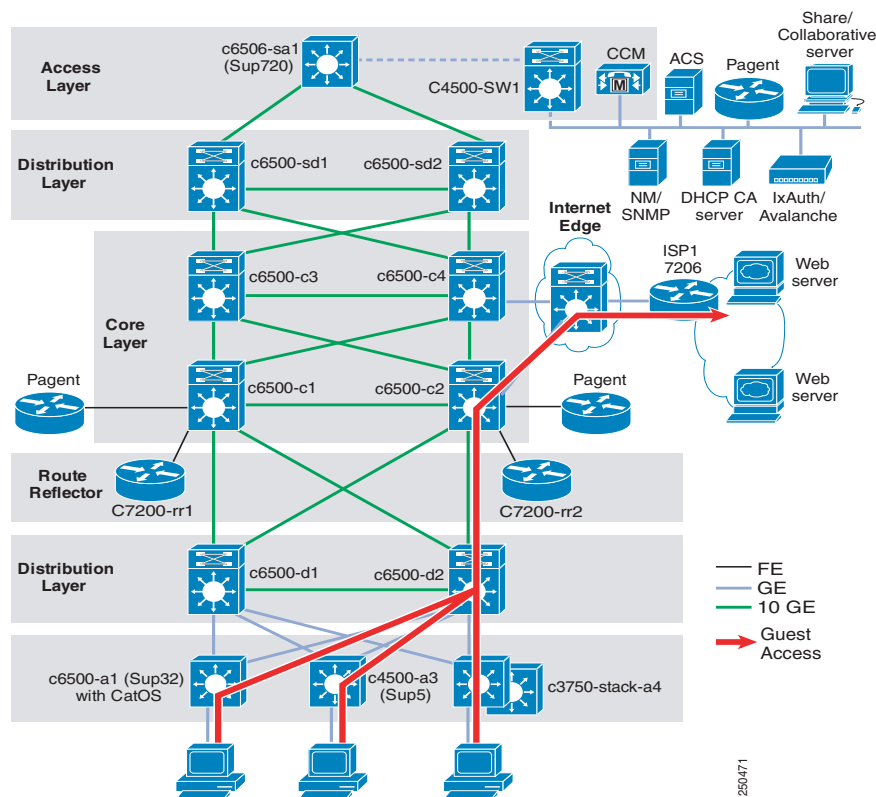
*Figure 5-2*          *802.1x Flow Guest Access Deployment*

802.1x Flow for Guest Access Deployment

```
┌─────────────────────────────────┐
│   802.1x Enabled on the Access   │
│  Switch Interface connected to   │
│          the Client PC           │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────┐
│                                  │
│   Client not IEEE 802.1x capable │
│                                  │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────┐
│   IEEE 802.1x authentication     │
│        process times out         │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────┐
│    Port is assigned to Guest VLAN │
└─────────────────────────────────┘
                 │
                 ▼
┌─────────────────────────────────┐
│        Port Authorized           │
│  Traffic can now go from the     │
│  Client PC in the access layer   │
│  to the local distribution layer │
│  to the core layer and to        │
│  Internet Edge . Access is       │
│  limited to Internet only .      │
└─────────────────────────────────┘
```
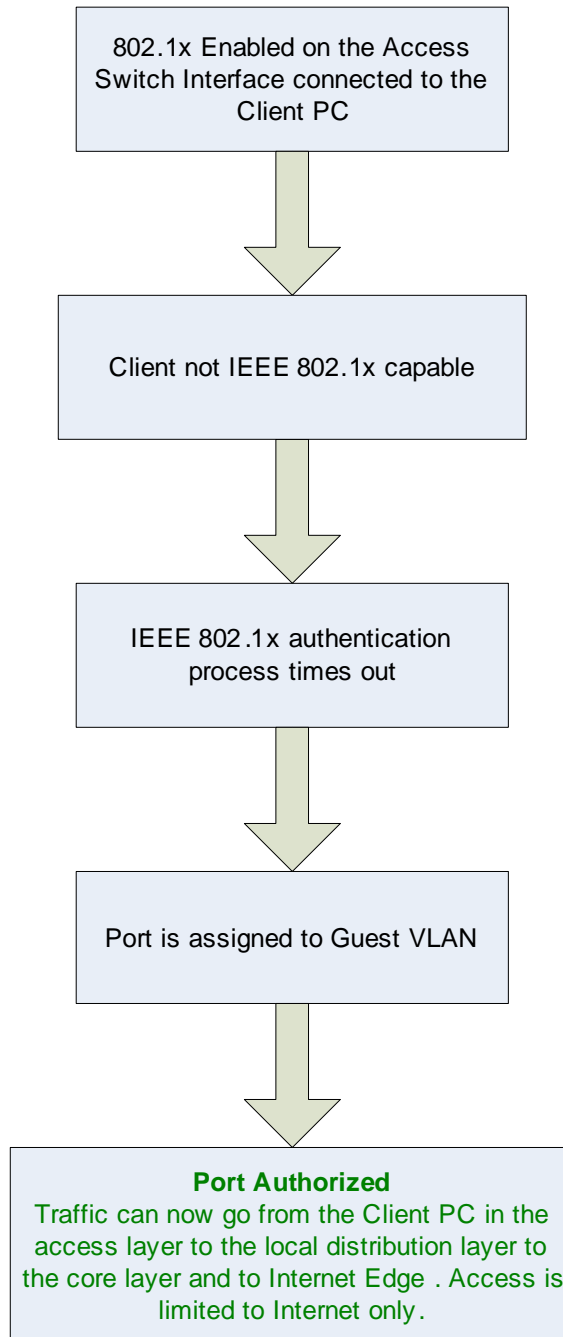
# 5.1  Guest Access Deployment Configuration

For a successful deployment of this scenario, the following are assumed to be in place:

- Basic network connectivity exists.
- DHCP servers are operational.
- Non-802.1x capable host machines (wired media).

The following is the summary of steps needed to ensure proper deployment of the Guest Access scenario in the Network Virtualization – Path Isolation solution.

1. Network Connectivity: Apart from the basic network connectivity from the access device to the device connected to the datacenter and the Internet Edge. The following configurations must be done in the distribution routers for the Guest Access deployment:
    a. Layer 3 (L3) configuration
    b. HSRP configuration for the above Layer 3 (L3) interface.
    c. VRF configuration
    d. Exporting VRF through MP-iBGP
    e. DHCP configuration
2. Access Switch Configuration
    a. 802.1x configurations on the access ports connected to end device (e.g. PC)
    b. AAA configuration.
    c. RADIUS configuration

The following are the detailed steps needed to ensure proper deployment of the Guest Access scenario in the Network Virtualization – Path Isolation solution.

**Network Connectivity**

**Distribution Switch Configuration:**

VRF configuration:

1. The first step in configuring the Guest VLAN deployment in the distribution router is to create VRF for guest VLAN. The following is the configuration:

```
ip vrf guest-pc
    rd 103:103
    route-target export 103:103
    route-target import 103:103
```

Layer 3 (L3) configuration: The second step of configuration in the distribution router is to map the Guest VLAN to its corresponding Layer 3 (L3) interface. The following is the configuration:

```
interface Vlan245
 description for 3750-guest-pc
 ip vrf forwarding guest-pc
 ip address 193.0.3.2 255.255.255.0
 standby 245 ip 193.0.3.3
 standby 245 timers msec 250 msec 750
 standby 245 priority 150
 standby 245 preempt
```

After creating the L3 interface for the corresponding Guest VLAN, the VRF that was created in the previous step is mapped to this interface. Also, HSRP is configured under this interface. The router in which the command "standby 245 priority 150" was configured will be the Active HSRP router, provided that the HSRP priority was set to default for the other distribution router in the topology.

**Note**    The configuration shown above can be extended to different VLANs from different access devices.

Exporting VRF through MP-iBGP: After the Layer 3 interface is created, the networks should be advertised through MP-iBGP protocol.

```
router bgp 64000
 bgp router-id 10.255.254.6
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.255.254.9 remote-as 64000
 neighbor 10.255.254.9 update-source Loopback0
 neighbor 10.255.254.10 remote-as 64000
 neighbor 10.255.254.10 update-source Loopback0
 maximum-paths ibgp  2

address-family ipv4 vrf guest-pc
  redistribute connected
 no synchronization
 exit-address-family
```

### DHCP configurations:

1. The DHCP server provisioned to assign network addresses to supplicants in the corresponding VLAN.

2. Access Switch Configuration

   a. Enable Authentication, Authorization and Accounting access control model on the switch:

      ```
      aaa new-mode1
      ```

   b. Specify one or more authentication methods for use on interfaces running IEEE 802.1x:

      ```
      aaa authentication dot1x default group radius
      ```

   c. Configure ACS server parameters:

      ```
      radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key Cisco
      ```

   d. Enable IEEE802.1xport-based access control on the switch

      ```
      dot1x system-auth-control
      aaa authentication dot1x default group radius
      aaa authorization network default group radius
      ```

   e. Set the Port Access Entity (PAE) type to authenticator:

      ```
      dot1x pae authenticator
      ```

   f. Enable manual control of the authorization state of a controlled port:

      ```
      dot1x port-control auto
      ```

### Radius Server configurations:

RADIUS is the protocol that the Access Layer devices use to communicate with the ACS server for 802.1x authentication. So some RADIUS commands are required to configure on this device:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

These commands indicate that RADIUS is chosen as the default protocol for IEEE 802.1x authentication.

The following command configures RADIUS server parameters (IP address of the radius server and the password).

```
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key Cisco
radius-server host 2.2.2.2 auth-port 1812 acct-port 1813 key Cisco
```

IEEE 802.1x configurations:   IEEE 802.1x must be enabled globally on the IOS switch.

```
dot1x system-auth-control
dot1x pae authenticator

dot1x port-control auto
```

The following command configures the dot1x port to be on the guest-vlan

```
dot1x guest-vlan 253
```

The final interface configuration on the access device is:

```
interface GigabitEthernet2/0/4
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 253
 spanning-tree portfast
 spanning-tree bpduguard enable
end
```

# 5.1.1 Guest Access Deployment Observations

Once the end device connected to the port of the access device with the above configuration, the following results are observed:

1. Upon EAP time-out, the end-user is placed into the Guest VLAN by the access switch.

2. The DHCP server will then assign an IP address for this device, which belongs to the network in the Guest VPN.

3. Once IP address is obtained, the end device is granted access to the Internet.

# 5.1.2 Guest Access Deployment Recommendations

1. Employees and Partner users can use the Guest VLAN as a last resort network access.

2. 802.1x timer tuning: When DHCP and 802.1x authentication is configured (with default DHCP and 802.1x timers), the maximum time it takes for an user to get an IP address from the DHCP server may be around seven minutes or longer. This situation is caused by the DHCP time-out that takes place after 60 seconds. In the current validation, the dot1x transmit timer (tx-time-out) is reduced from 30 seconds (default) to 10 seconds.

# References

*Network Virtualization -- Access Control Design Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008084985f.pdf

*Network Virtualization – Guest and Partner Access Deployment Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080849883.pdf

*Network Virtualization -- Path Isolation Design Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080851cc6.pdf

*Cisco-recommended Campus Network Design Guides*

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2

*Network Virtualization -- Path Isolation System Assurance Guide*
http://www.cisco.com/en/US/docs/nsite/network_virtualization/nv_pi_sag.pdf

# Network Virtualization Access Control Solution Validation Strategy

The Network Virtualization – Access Control Solution Validation Strategy was to build End-to-End MPLS VPN Campus network (with Path Isolation) and to validate Access Control services at the edge of the network. The solution was validated in manual and automated regression testing.

## B.1  Network Topology

The Network Virtualization Access control solution was validated in the MPLS VPN - High Availability Multilayer Campus network and based upon the following Campus design guides:

*Network Virtualization -- Access Control Design Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008084985f.pdf

*Network Virtualization – Guest and Partner Access Deployment Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080849883.pdf

*Network Virtualization -- Path Isolation Design Guide*
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a0080851cc6.pdf

*Cisco-recommended Campus Network Design Guides*

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2

In validating the Network Virtualization – Access control Design, a High Availability (HA) MPLS VPN multilayer Campus Path Isolation network was built as shown in Figure A-1 with different Access Layer devices used for validation.

In the core layer, Cat6500 platforms with dual chassis, dual supervisor (SUP-720-BXL) and ten gigabit Ethernet (10GE) links played a role of Provider (P).

The Route Reflector role with fast Ethernet links to core devices was deployed on a C7200-VXR with NPE-G1 processor.

In the Distribution Layer, Cat6500 platforms with dual chassis, dual supervisor (SUP-720-BXL) and ten-gigabit Ethernet (10GE- uplink to the core) links played a role of Provider Edge (PE). Emulated distribution blocks were created using IXIA tools in order to scale EIGRP routes

In the Access Layer, Cat6500, Cat4500, and Cat3750E (StackWise – Total of four switches) played a role of Layer2 switches.

*Figure B-1        Network Virtualization - Access Control Topology*
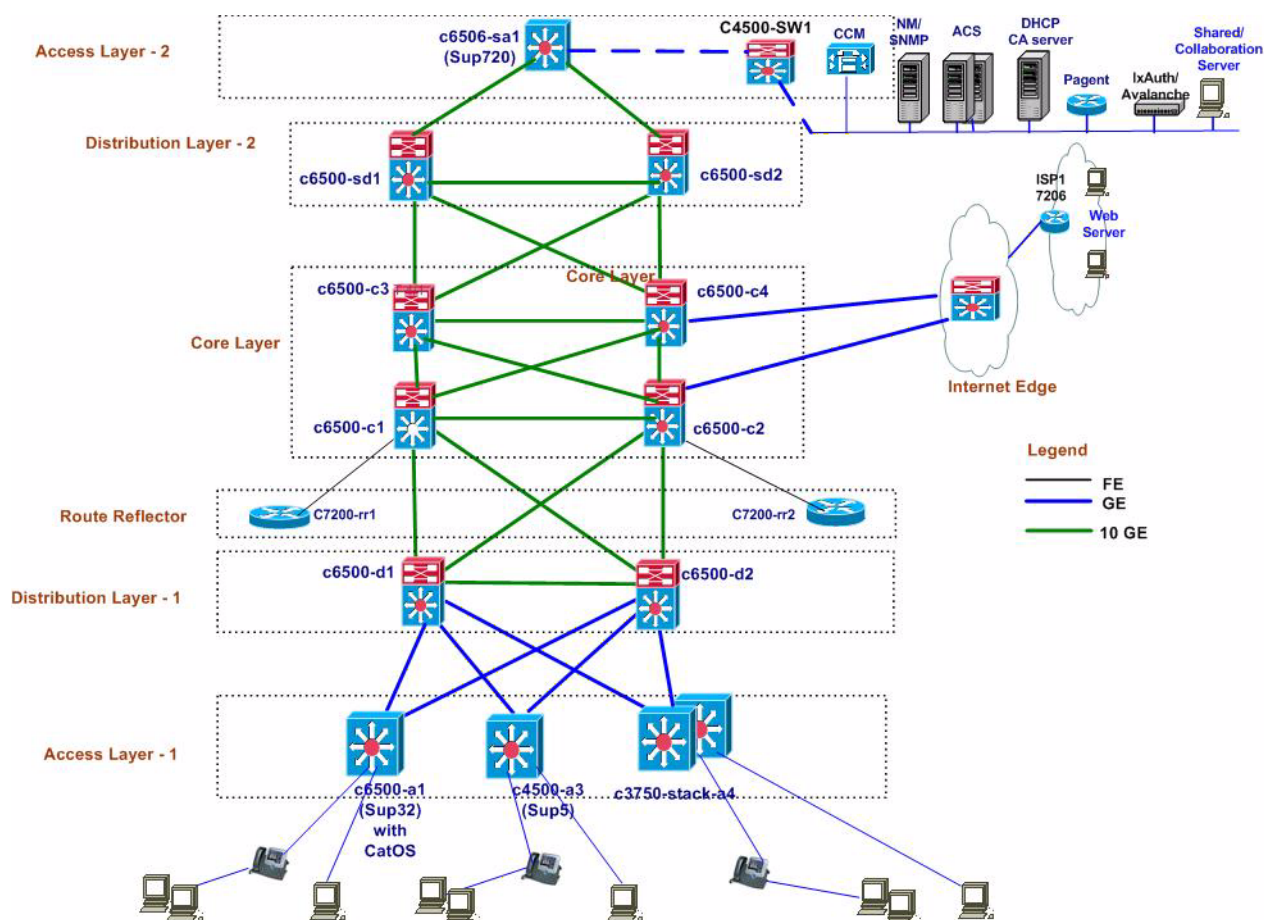


# B.2  Traffic Profile

## B.2.1  Baseline Traffic

The following constitutes "Baseline traffic" that ran for every test that was executed.

- 5000 EIGRP routes (10% rate)
- 5000 Multicast routes (10% rate)
- 5000 VPN routes   (10% rate)
- QoS Traffic includes Stateful traffic for Voice call, Video, Call Control, SAP, HTTP, FTP, POP3, etc (20% rate).

QoS traffic is based on the recommendations from *Enterprise QoS Solution Reference Network Design Guide:*

http://www.cisco.com/univercd/cc/td/doc/solution/esm/qossrnd.pdf

The following table shows the details of QoS Traffic:

***Table B-1          Qos Traffic***

| Class (BW %) | Application | DSCP | Packet size (Byte) | BW |
|---|---|---|---|---|
| | Voice | EF | 64 | 18% |
| **Real Time (33%)** | Messenger | AF41 | 100~1k | 15% |
| | SAP | AF21 | 1024 | 20% |
| | stream video | CS4 | 256 | 10% |
| | call signaling | CS3 | 64 | 4% |
| **Critical Data (37%)** | SNMP | CS2 | 64 | 3% |
| **Best Effort (25%)** | HTTP | 0 | EMIX | 25% |
| **Scavenger/Bulk (5%)** | FTP | AF11 | 1500 | 3% |

**Test tools:**   IxNetwork v5.30.40.50 (IXIA) is used for EIGRP, Multicast and VPN routes. Avalanche (Spirent) is used for Stateful QoS Traffic

# B.2.2  Test Traffic

The following constitutes "Test Traffic" for validating the deployment scenarios discussed in the next section:

- 150 (802.1x) supplicants across three access devices.
- HTTP Traffic flows (on all 150 supplicants).

Avalanche is used for emulated 802.1x supplicants. After the emulated supplicant is authenticated, the switch port will grant the access for either employee in the global table or partner in the MPLS VRF. A HTTP traffic flows between the emulated supplicant and dedicated server depending the user type – employee or partner. When emulated the supplicant with wrong password, the port will be authorized in auth-fail-VLAN. Auth-fail-VLAN is routed to Internet Edge router with the Internet service. And HTTP traffic will flow the Internet server in this case.

**Test tools:**   Avalanche (Spirent) is used for emulating multiple 802.1x supplicants as well as HTTP traffic across those supplicants.

*Table B-2        Hardware and Software and Device Information*

| Role | Hardware | | Software |
|------|----------|---|----------|
| | **Platform** | **Line Card** | |
| Access L2 | C3750E-24TD | StackWise (Four 3750E) | 12.2(44)SE |
| | C4507R | WS-X4516-10GE<br>WS-X4548-GB-RJ45V | 12.2(46)SG |
| | C6506 | WS-SUP32<br><br>WS-F6700-CFC<br>WS-F6K-PFC3BXL<br>WS-SUP720 (MSFC3)<br>WS-X6704-10GE<br>WS-X6148A-GE-45AF<br><br>WS-X6548-GE-TX | 8.7(1) |
| Distribution (PE) L2 / L3 | C6506 | WS-SUP720-3BXL (Dual)<br>WS-F6700-DFC3BXL<br>WS-F6K-PFC3BXL<br>WS-SUP720 (MSFC3)<br>WS-X6704-10GE<br>WS-X6748-GE-TX | 12.2(33)SXH2a |
| Core (P) L3 | C6509 | WS-SUP720-3BXL (Dual)<br>WS-F6700-DFC3BXL<br>WS-F6K-PFC3BXL<br>WS-SUP720 (MSFC3)<br>WS-X6704-10GE<br>WS-X6748-GE-TX | 12.2(33)SXH2a |
| Route Reflector (RR) | C7206VXR | NPE-G1 | 12.4(15)T5 |
| ACS | Access Control Server | N/A | 4.2 |
| CCM | Cisco Call Manager | N/A | 6.1 |

# B.3  Test Types

Validation tests are divided into the following categories:

- System Integration
- Scalability
- Reliability

# B.4  System Integration

System Integration has two major components: feature combination and feature interaction. Feature combination focuses on testing a feature when various combinations of other features are enabled. Feature interaction tests were conducted to verify dependencies between features.

The System Integration Tests combines all the features required for multiple features inter-operability. End-to-End traffic (stateful and stateless) is validated for data, voice and video using IXIA and SmartBit tools.

Health checks were performed before and after tests. These checks included memory and CPU utilization, tracebacks, memory alignment errors, interface errors, line card status and syslog messages.

*Table B-3        Device Role and Feature Information*

| Role | Feature / Technology |
|------|---------------------|
| Access L2 | Rapid PVST+ Loopguard |
| | BPDU Guard Portfast UDLD Vlan Trunking StackWise (3750E) |
| | AAA |
| | 802.1x |
| | Auth-Failed VLAN |
| | Guest VLAN |
| | Mac-Authentication Bypass (MAB) |
| Distribution L2 | PVRST+ Loopguard Portfast UDLD Vlan Trunking |

*Table B-3        Device Role and Feature Information*

| Distribution (PE) L3 | HSRP<br>EIGRP<br>EIGP hello/hold timers tuning<br>EIGRP Graceful Restart<br>MPLS LDP<br>MPLS LDP Graceful Restart<br>MPLS LDP Session Protection<br>BGP, MP-iBGP<br>BGP Graceful Restart<br>BGP Next-Hop Tracking<br>BGP VPNv4 scan timer<br>ECMP IGP/BGP<br>NSF/SSO support of MPLS VPN<br>DHCP<br><br>Multicast<br><br>QoS |
|---|---|
| Core (P) L3 | EIGRP<br>EIGP hello/hold timer tuning<br>EIGRP Graceful Restart<br>MPLS LDP<br>MPLS LDP Graceful Restart<br>MPLS LDP Session Protection<br>ECMP IGP<br>NSF/SSO support of MPLS LDP |
| Route Reflector (RR) | EIGRP<br>MP-iBGP<br>BGP Next-Hop Tracking<br>BGP VPNv4 scan timer<br>BGP IPv4 Unicast Multipath iBGP |
| ISP Router | EIGRP<br>EIGRP hello/hold timers tuning<br>EIGRP Graceful Restart<br>MP-iBGP<br>Static routes |

# B.5  Scalability

As part of the solution validation, the MPLS/VPN Campus network was scaled by simulating a large number of distribution blocks. For EIGRP, the network was scaled up to 50 neighbors and 3000 routes. For MPLS VPN, the network was scaled up to 5000 VPN prefixes. End-to-End traffic (stateful and stateless) was validated for data, voice and video using IXIA. Further traffic details are described in B.2.1  Baseline Traffic.

*Table B-4        Device Role and Network Scalability Information*

| Role | Network Scalability |
|------|---------------------|
| Access L2 | 100 Vlans |
| Distribution L2 | 100 Vlans |
| Distribution (PE) L3 | 3000 EIGRP routes<br>50 VRFs<br>100 HSRPs<br>5000 VPN prefixes |
| Core (P) L3 | 50 EIGRP neighbors<br>3000 EIGRP routes |

Access Control scale included the simulation of 150 aggregate 802.1X supplicant clients equally distributed across the access layer platforms (3750, 4500, and 6500) using the Spirent Avalanche test tool. Within each access platform, various user types were simulated, which included: Employee, Partner and Guest supplicants. End-to-End HTTP traffic flows are generated across each supplicant to their respective servers based on supplicant types. Further supplicant details are described in Table B-5.

*Table B-5        802.1x Supplicant Scalability Information*

| Platform | Supplicant Scale and Type | Traffic Destination | Route Path |
|----------|---------------------------|---------------------|------------|
| 3750 | 43 Employee | Employee Server | Global Table |
|      | 5 Partner | Partner Server | MPLS VPN |
|      | 2 Guest | Internet Access | |
| 4500 | 43 Employee | Employee Server | Global Table |
|      | 5 Partner | Partner Server | MPLS VPN |
|      | 2 Guest | Internet Access | |
| 6500 | 43 Employee | Employee Server | Global Table |
|      | 5 Partner | Partner Server | MPLS VPN |
|      | 2 Guest | Internet Access | |

**Downloadable ACL Scalability (CATOS):**

The scale of dACL is determined by TCAM ACL storage usage. There are two components that use the storage: number of independent ACEs, and number of ports that the ACEs are mapped to. Following are three scenarios that are validated:

- a) 750 independent ACEs with a single dot1x access port
- b) 600 independent ACEs with 42 dot1x access ports
- c) 500 independent ACEs with 47 dot1x access ports

# B.6 Reliability

The 150-hour reliability test was executed for the entire testbed to ensure that the various solutions interoperate without memory or CPU issues or any operationally impacting defects. Devices were monitored for tracebacks, alignment and interface errors, and syslogs for any error messages. End-to-End connectivity was maintained during this test.

# B.7 Sustaining Coverage

On going automated regression testing provides consistent, repeatable customer representative coverage.

Sustaining test coverage includes the following components:

- Automated test scripts for each automated test case
- Common scripts library for managing the testbed, collecting and reporting test results
- Automated procedures to capture the manual execution results

# C

# Test Case Descriptions and Results

## C.1 Employee Access Test Suite

| Test | Manual Test Case | Defects | Automation Test Case | Defects |
|---|---|---|---|---|
| NV – Access Control Employee Access Deployment Suite: This test suite validates the employee access deployment, where a client with dot1x supplicant (with a valid userame and password) can be placed in Global network and have unlimited access to resources on the network. This test suite includes various options: <br>– Client with Dot1x supplicant – no IP Phone. <br>– Client with Dot1x Supplicant - with supplicant IP Phone. <br>– Client with Dot1x supplicant – with supplicantless IP Phone. <br>– Client with Dot1x supplicant – Fallback to MAC auth Bypass (MAB) – no IP Phone. <br>– Client with Dot1x supplicant – Fallback to MAC auth Bypass (MAB) – with supplicant IP Phone. <br>– Client with Dot1x supplicant – Fallback to MAC auth Bypass (MAB) – with supplicantless IP Phone. | | | | |
| With Dot1x Supplicant (no IP phone) | --- | --- | Passed | --- |
| With Dot1x Supplicant (with supplicant IP phone) | Passed | --- | --- | --- |
| With Dot1x Supplicant (with supplicantless IP Phone) | Passed | --- | --- | --- |
| With Dot1x supplicant - Fallback to MAB (no IP Phone) | Passed | --- | --- | --- |
| With Dot1x supplicant - Fallback to MAB (with supplicant IP phone) | Passed | --- | --- | --- |
| With Dot1x supplicant - Fallback to MAB ( with supplicantless IP phone) | Passed | --- | --- | --- |

# C.2  Partner Access Test Suite

| Test | Manual Test case | Defects | Automation test case | Defects |
|------|------------------|---------|----------------------|---------|
| – NV – Access Control Partner Access Deployment Suite: This test suite validates the Partner Access Deployment, where a client with dot1x supplicant (with a valid username and password) can be placed in Partner VRF network and have limited access to resources on the network.  This test suite includes various options: <br> – Client with Dot1x supplicant – no IP Phone. <br> – Client with Dot1x supplicant – Fallback to MAC Auth Bypass (MAB) – no IP Phone. | | | | |
| With Dot1x Supplicant – no IP Phone | --- | --- | Passed | --- |
| With Dot1x Supplicant – Fallback to MAB- no IP Phone. | Passed | --- | --- | --- |

# C.3  Guest Access Test Suite

| Test | Manual Test case | Defects | Automation test case | Defects |
|------|------------------|---------|----------------------|---------|
| NV – Access Control Guest Access Deployment Suite: This test suite validates the Guest Access deployment, where a client without the dot1x supplicant will be placed in Guest network and have access to only Internet connection on the network. This test suite includes the following option: <br> – Client without Dot1x supplicant – no IP Phone. | | | | |
| With no Dot1x supplicant | --- | --- | Passed | --- |

**APPENDIX D**

# Defects

There were 24 defects encountered during the validation of the Network Virtualization – Access Control solution. These defects were resolved and verified during the validation of this solution.

**The following are two outstanding defects:**

## D.1  CSCsr07134

Description: Memory leak for qos const_get_private_ipc_buffer_pak on 6k, 12.2(33)SXH02a.

 Workaround:  None.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(33)SXH3.

## D.2  CSCsr07615

Description: Memory leak for pak_pool_cache_item_get on 6k,12.2(33)SXH02a.

Workaround: This defect is observed once when the distribution router (PE) reloads. This is not observed under normal conditions.

Severity: Moderate.

Status: Resolved in IOS version 12.2(33)SXH3.

**The following are defects that were resolved:**

## D.3  CSCsq96691

Description: Whitney: Memory leak in update_memory_histroy

Severity: Moderate.

Status: Resolved in IOS version 12.2(33)SXH2a.

# D.4 CSCsq66364

Description: Dot1x authentication not working for 44 SG image, scale of supplicants.

Severity: Severe.

Status: Resolved in IOS version 12.2(46)SG.

# D.5 CSCsm69762

Description: WI08: Random dot1x users do not authenticate throughout my network.

Severity: Severe.

Status: Resolved in IOS version 12.2(46)SG.

# D.6 CSCsm44028

Description:  Port a couple of CMFI ICC issues from autobahn76 to sierra.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(33)SXH.

# D.7 CSCsl90751

Description:  Dot1x critical:  Re-auth of MAB kicks security violation.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SG.

# D.8 CSCsl83010

Description:  dot1x critical:  phones cannot be recovered.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE2.

# D.9 CSCsl82998

Description:  dot1x critical:  Traffic allowed blindly on the Voice-VLAN.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE2.

# D.10  CSCsl77063

Description:  3rd party phones are incorrectly err-dis w/ cisco ip-phone detect.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE2.

# D.11  CSCsl48111

Description:  7960/40 EAPOL-Logoff functionality.

Severity:  Moderate.

Status:  Resolved in 8.0(9)

# D.12  CSCsk63889

Description:  802.1x:  CDP is processed and transmitted.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE2.

# D.13  CSCsk59128

Description:  802.1x:  VLAN-Assignment and RFC 4436.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE.

# D.14  CSCsk59124

Description:  802.1x:  Accounting contains IP of 0.0.0.0.

Severity:  Moderate.

Status:  Resolved in 8.7(0)

# D.15  CSCsk38616

Description:  Mac-auth-Bypass generates incorrect accounting records.

Severity:  Severe.

Status:  Resolved in 8.7(0.116).

# D.16 CSCsk35014

Description:  Doc:  Incorrect 802.1x timer/value definitions.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2S

# D.17 CSCsk14571

Description:  802.1x Accounting:  Attributes [49] has incorrect value.

Severity:  Moderate.

Status:  Resolved in 8.7(0.91)LAR

# D.18 CSCsk14521

Description:  802.1x Accounting:  Missing attribute{6} in the START record.

Severity:  Moderate.

Status:  Resolved in 8.7(0.82)LAR

# D.19 CSCsk14482

Description:  802.1x Missing attribute [30].

Severity:  Moderate.

Status:  Resolved in 8.7(0.82)LAR

# D.20 CSCsk14465

Description:  MAB:  RADIUS Attribute [12] not sent.

Severity:  Moderate.

Status:  Resolved in 8.7(0.82)LAR

# D.21 CSCsk14456

Description:  802.1x:  Radius attribute 12.

Severity:  Moderate.

Status:  Resolved in 8.7(0.82)LAR

# D.22  CSCsi85257

Description:  MDA:  Cannot be enabled on the flly with MAB and Cisco-Phone.

Severity:  Moderate.

Status:  Resolved in IOS version 12.2(44)SE2

# D.23  CSCsi31046

Description:  DHCP-Snooping:  Entries are purged on link-down.

Severity:  Severe.

Status:  Resolved in 8.7(0.1)LAR

# D.24  CSCsq14606

Description: To Handle code review comments regarding Base code issues.

Severity:  Moderate.

Status:  Resolved in IOS versioin 12.2(33)SXH.

**D.24   CSCsq14606**