



Enterprise Network Virtualization – Access Control System Assurance Guide Cisco Validated Design

Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883 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

ſ

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
НТТР	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
Р	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

Γ

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.



CONTENTS

1

Γ

Executive Summary 1-1			
Network Virtualization Solution Overview 2-1			
2.1 Network Virtualization - Access Control Solution 2-3			
2.2 Network Virtualization – Employee, Managed Partner and Guest Access Solution 2-4			
Network Virtualization - Employee Access Deployment 3-1			
3.1 Employee Access Deployment Configuration 3-4			
3.1.1 Employee Access Deployment Observations 3-24			
3.1.2 Employee Access Deployment Recommendations 3-25			
Network Virtualization - Managed Partner Access Deployment 4-1			
4.1 Managed Partner Access Deployment Configuration 4-2			
4.1.1 Partner Access Deployment Observations 4-19			
4.1.2 Partner Access Deployment Recommendations 4-20			
Network Virtualization - Guest Access Deployment 5-1			
5.1 Guest Access Deployment Configuration 5-3			
5.1.1 Guest Access Deployment Observations 5-5			
5.1.2 Guest Access Deployment Recommendations 5-5			
References A-1			
Network Virtualization Access Control Solution Validation Strategy B-1			
B.1 Network Topology B-1			
B.2 Traffic Profile B-2			
B.2.1 Baseline Traffic B-2			
B.2.2 Test Traffic B-3			
B.3 Test Types B-4			
D.3 163(1)/p63 B-4			
B.4 System Integration B-5			

B.7 Sustaining Coverage B-8

Test Case Descriptions and Results C-1

C.1 Employee Access Test Suite C-1

1

- C.2 Partner Access Test Suite C-2
- C.3 Guest Access Test Suite C-2

Defects D-1

- D.1 CSCsr07134 D-1
- D.2 CSCsr07615 D-1
- D.3 CSCsq96691 D-1
- D.4 CSCsq66364 **D-2**
- D.5 CSCsm69762 D-2
- D.6 CSCsm44028 D-2
- D.7 CSCsI90751 D-2
- D.8 CSCsl83010 D-2
- D.9 CSCsl82998 D-2
- D.10 CSCsI77063 D-3
- D.11 CSCsI48111 D-3
- D.12 CSCsk63889 D-3
- D.13 CSCsk59128 D-3
- D.14 CSCsk59124 D-3
- D.15 CSCsk38616 D-3
- D.16 CSCsk35014 D-4
- D.17 CSCsk14571 D-4
- D.18 CSCsk14521 D-4
- D.19 CSCsk14482 D-4
- D.20 CSCsk14465 D-4
- D.21 CSCsk14456 D-4
- D.22 CSCsi85257 D-5
- D.23 CSCsi31046 D-5
- D.24 CSCsq14606 D-5



FIGURES

- *Figure 2-1* Network Virtualization Overview **2-1**
- *Figure 2-2* Network Virtualization Framework 2-2
- Figure 3-1Employee Access Topology3-2

ſ

- *Figure 3-2* Flow Chart for Employee Access Deployment **3-3**
- Figure 4-1Managed Partner Access Topology4-1
- Figure 4-2Managed Partner Access Flowchart4-2
- *Figure 5-1* Guest Access Deployment Topology **5-1**
- *Figure 5-2* 802.1x Flow Guest Access Deployment **5-2**

Figures

1



TABLES

Table 1	Modification History 1-iii
Table 2-1	Employee and Managed Partner Features 2-5
Table B-1	Qos Traffic B-3
Table B-2	Hardware and Software and Device Information B-4
Table B-3	Device Role and Feature Information B-5
Table B-4	Device Role and Network Scalability Information B-7
Table B-5	802.1x Supplicant Scalability Information B-7

Γ

Tables

1



CHAPTER

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.



ſ

снарте 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.



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:

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.

Table 2-1 Employee and Managed Partner	r Features
--	------------

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.

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





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

ſ

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







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.

ſ



Figure 3-2 Flow Chart for 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



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.



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.
- 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:

Γ

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.

li il i	System Configuration	
User Setup	Edit	
	Global Authentication Setup	
Group Setup		
Shared Profile Components	EAP Configuration]
Network Configuration	РЕАР	
System	Allow EAP-MSCHAPv2	
Configuration	Allow EAP-GTC	
Interface Configuration	Allow Posture Validation	
Administration Control	Allow EAP-TLS	
External User	Select one or more of the following options:	
Databases	Certificate SAN comparison	
Posture Validation	Certificate CN comparison	
Network Access Profiles	Certificate Binary comparison	
	EAP-TLS session timeout (minutes): 120	
Reports and Activity	Cisco client initial message:	
Online Documentation	PEAP session timeout (minutes): 120	
	Enable Fast Reconnect:	
	EAP-FAST EAP-FAST Configuration	
	Select one or more of the following options:	
	LEAP Allow LEAP (For Aironet only)	
	EAP-MD5 ☑ Allow EAP-MD5	
	AP EAP request timeout (seconds): 20	
	MS-CHAP Configuration	
	Allow MS-CHAP Version 1 Authentication	
	Allow MS-CHAP Version 2 Authentication	
	Back to Help	-

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.



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

Network Configuration		
Select		
% Q	(Not Assigned) AAA Clients	?
AAA Client Hostname	AAA Client IP Address	Authenticate Using
	Add Entry Search	
% ⊲	(Not Assigned) AAA Server	s <u>?</u>
AAA Server Name	AAA Server IP Address	AAA Server Type
w2k3-acs2	127.0.0.1	CiscoSecure ACS
	Add Entry Search	
	P Back to Help	18838966
	Select Select Select AAA Client Hostname AAA Client Hostname AAA Server Name	Select

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.

ahaha	Group Setup		
cisco	Select		
User Setup			-1
Group Setup	Group :	0: Default Group (6 users)	
	Users in Group	20: Group 20	
Shared Profile Components	- Osers in Group	21: Group 21	
		22: Group 22	
Network Configuration		23: Group 23	
		24: Group 24	
System		25: Group 25	
Configuration		26: Group 26	
Interface		27: Group 27	
Configuration		28: Group 28	
_ 90 Administration		29: Group 29	
Administration Control		30: Group 30 31: Group 31	
- External User		32: Group 32	
Databases		33: Group 33	
		34: Group 34	
Posture Validation		35: Group 35	
		36: Group 36	
Network Access Profiles		37: Group 37	
- Promes		38: Group 38	
Reports and		39: Group 39	
🛛 💓 🛛 Activity		40: Group 40	
🚌 🔁 Online		41: Group 41	
Documentation		42: Group 42	
		43: Group 43	
		44: Group 44	
		45: Group 45	
		46: Group 46	
		47: Group 47	\sim
		48: Group 48	88
	l L	49: Group 49	188867

1

Enterprise Network Virtualization Access Control System Assurance Guide

Γ

- 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)

ahaha	Group Setup					
CISCO	Jump To Access Restrictions					
User Setup	[028] Idle-Timeout	<u>Р</u>				
Group Setup		0				
Shared Profile Components	[029] Termination-Action					
Network Configuration	Default Default Default	<u> </u>				
System Configuration	[034] Login-LAT-Service [
Configuration	[035] Login-LAT-Node					
External User Databases Posture Validation	[036] Login-LAT-Group					
Network Access Profiles	[037] Framed-AppleTalk-Link (065535)	0				
Reports and Activity	[038] Framed-AppleTalk-Network (065535)					
Documentation	[039] Framed-AppleTalk-Zone	0				
	[062] Port-Limit	0				
	[063] Login-LAT-Port					
	☑ [064] Tunnel-Type					
	Tag 1 Value VLAN Tag 2 Value	• •				
	I ag ∠ Value					
	Tag 1 Value 802 Tag 2 Value	▼ ▼				
	I ag [Value]					
	Tag 1 Value					
	Tag 2 🔽 Value					
	Submit Submit + Restart Cancel	▼				
	Cancer Cancer	88868				

- 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.

	daws Internet Explorer	s internet and the second s
😋 🕘 • 🔘 http://12	7.0.0.1.2669U	• (*) × (**** (*)
Ne Edit View Pavori	ies Taals Help	
nis O Continue ACS h	nd	
Coosteoure	AS E	🖓 • 🗋 - 📾 • 🖓 fagt • 🕲 fagt •
	User Setup	x
CISCO		
	Edit	• http
Setas	User: 37-emp-md5	Account Disabled
1177	user. Sy emp mus	Deleting a Username
G Shared Brothe	C Account Disabled	Supplementary liner Info Desseard Authentication
		· Group to which the sour is assigned
Confriguration	Supplementary User Info	Callack Class IP Address Assignment
Carlingention	Real Name	Advanced Settings
	Description	Instaurk Access Restrictions
Configration		Has Sessions Usage Quitas
Control		Account.Double
0G External liner	User Setup ?	Downlandship AGLa Advanced TACACS+ Settings
the state of the s		TACACS + Enable Control
Validation	Password Authentication: ACS Internal Database	TACACS+ Enable Password
Parties	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not	TACACS+ Outboard Passaurd TACACS+ Shell Command Authorization
Co. I Beautrant	checked.)	Command Authorization for Network Device Hasagement Applications
Reports and Activity	Password	TACACE+ Unknown Services ETF RADIUS Attributes
Distant	Confern Password	RADIUS Vender Specific Attributes
	Separate (CHAP/MS-CHAP/ARAP)	Time Bound Alternate Group
	Password	Letter transfer
	Confirm Password	Account Disabled Status
	When a token server is used for authentication, supplying a separate CH4P password for a token card user allows CH4P authentication. This is especially useful when token caching is enabled.	Select the Assount Disabled sheck box to disable this assount: clear the check box to enable the assount.
		[Hack to Tau]
	Group to which the user is assigned:	Deleting a Veename
	3750-Employee	The Delete bottom appears only often you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When axied to confert your among click DK.
	Calback	[Back to Toul]
	# Use group setting	Supplementary User Jafo
	C No calback allowed	Type the applicable information in any supplemental user information house that appear. To add or shange
	C Callback using this number	fields, slick Interface Configuration, then click User Data Configuration. You can configure up to five fields.
	C Dialup client specifies callback number	[Back to Tau]
	O Use Windows Database callback settings	Password Authentication
	Client IP Address Assignment	Select alther the Windows user database, the ACS Internal database, or a taken raid or other third-party server database to use for usersman and passed authentication. For database devices a selecting a database and using passentials, click Onten Concentration .
	Use group settings C. No. 10 address, associated	If the name of the database you want to use does not appear in the fait, dick External Oser Databases, cick Database Configuration, then configure the information for the applicable database.
	Submit Delete Cancel	If you salect an external user database, the external user database must already contain a valid account.
	44.1 20	2 100% *

<u>Note</u>

User settings override the Group level settings.



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



Only configurations relevant to this deployment scenario are mentioned here.



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-model
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 Ciscol

IEEE 802.1x configurations

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

dot1x system-auth-control OI set dot1x system-auth-control(CatOS)

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

dotlx 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:

dotlx 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

ſ

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.

CiscoSecure ACS - Win	dows Internet Explorer		
• •	27.0.0.1:13406/		💌 🔩 🗶 Google 🖉 🖓 🛀
Ele Edit View Fgvorit	tes <u>T</u> ools Help		
Links O OscoSecure ACS Tr	Hal		
😭 🕸 👩 OscoSecure	AG		💁 • 🖸 - 📾 • 🕑 Bage • 🎯 Tgols • "
abab	Shared Profile Components		×
CISCO -	Select .		E Help
User Setup			
	RADIUS Authori	zation Components	RADIUS Authorization Components
Breve Setap	Name	Description	Adding a RADIUS Authorization Component Cloning a RADIUS Authorization Component
Shared Profile Components	dacl1x	For 6500 dACL	Editing a RADIUS Authorization Component
	MAB-37-emp	For configuring authorization in NAP	Deleting a RADIUS Authorization Component
Network Configuration	MAB-37-partner	for 37-partner MAB	
System Configuration	MAB-45-emp	For configuring authorization in NAP	
	MAB:65-emp	For configuring authorization in NAP	RADIUS Authorization Components
Configuration	NAC-SAMPLE-QUARANTINE-L2-RAC		Shared RADIUS Authorization Components (RAC) are configurable sets of RADIUS attributes that may be assigned to user or user group sessions dynamically based on a policy. Use the Network
Administration Control			Access Profile configuration to create an authorization policy that maps from set conditions such as network device groups and posture to the shared RAC.
Deternal User Dutabases			For more details about RAC and the new user model, see <u>Understanding the New User Model</u> . For details on RAC and groups, see <u>BAC and Octube</u> .
Posture Validation			Notes Before setting Shared Profile Components, you must add your devices using Network Configuration and configure them to authenticate using the desired security protocol (such as RADUS Class VPR0200/RAS/VPIX 2xx). If your attribute is not displayed, check Interface
Nebrock Access Profiles			Configuration or your User Setup/Group Setup parameters.
Reports and Activity			(Back to Top)
-Children			Adding a RADIUS Authorization Component
Documentation			To add a new RAC, click Add. On the page that appears, you can configure the new RAC.
			[Back to Top]
			Cloning a RADIUS Authorization Component
			To create a new RAC by copying, or closing, an existing RAC, from the layer column, select the name of the RAC you want to close. On the page that appears, click Glose , a new RAC is created named Copy of RAChame. Closing saves time when creating components with similar attributes.
			[Back to Top]
			Editing a RADIUS Authorization Component
			To edit an existing RAC, from the trame column, select the name of the RAC. On the page that appears, you can edit the RAC. You can also copy, or come an existing component to save time when creating a new component that has attributes.
			[Back to Top]
			Deleting a RADIUS Authorization Component
			To delete a RAC, from the Name column, select the name of the RAC. On the page that appears, you can delete the RAC.
			[Back to Top]
			understanding the New User Hodel
	Ad	d Cancel	Two uses use autored, assess provides to providence the same. Additional distribution to have efficient based for different and
			💊 🚱 Internet 🔍 100% 🔹 😡

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"

CiscoSecure ACS - W	Indows Internet Explor	er		x O x
G . Mp://	127.0.0.1:13406/			🗶 🏘 🗶 Google 🖉 P
Ble Edit Yew Fgvo	anites ∐ools Help			
Links 👩 OscoSecure ACS	Trial			
🚖 🐟 🛛 👩 OscoSecur	re ACS			🐴 + 🖸 - 📾 + 🕑 Bage + 🎯 Tgols + 🤎
	Shared Profi	le Components		×
cisco		le componenta		
	Edit			A Help
User Setup	RAI	DIUS Authorizatio	n Components	• Name
Broup Setup			. componento	Description
Shared Profile Components	Name:	MAB-37-emp		Add New Attribute Assigned Attributes
			on in 👘	RAC Attribute Add/Edit
Network Configuration	Description:	NAP	on in 💌	
Sutem Configuration				Name
Interface		Add New Attribut	e 🤶	
Configuration		Add New Attribut	• <u>I</u>	Type the name you want to assign to the RADIUS Authorization Component.
Administration Centrel	Cisco 105/PIX 6-	.0 cisco-av-	pair (1) Add	[Back to Top]
Deternal User	LETF		PType (6) Add	Description
				Type an explanation of the RADIUS Authorization Component.
Posture Validation	Ascend	[A)	cend-Remote-Addr (154) 💌 Add	[flack to Top]
Network Access Profiles				Add New Attribute
Reports and				To add a new attribute, select the desired vendor attribute using the drop down list and dick the
Activity		Assigned Attribute	es 🤶	to add a new attribute, select the desired vendor attribute using the drop down list and click the adjacent Add button.
Documentation	Vendor	Attribute	Value	Note: Vendors available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at either group or user level) under
	18TF	Tunnel-Private-Group-ID (81) Tunnel-Type (64)	[T11 205 [T11 VLAN (13)	Interface Configuration.
	IETF	Tunnel-Hedium-Type (65)	[TT11402 (6)	[Back to Too]
				Assigned Attributes
		P Back to Help		The list of RADIUS attributes assigned to the Authorization Component. To edit or delete an already assigned attribute, citic on the attribute value. On the paper that displays you can add or edit the attribute value. This section is not/displayed what mattributes have been assigned.
				For attribute descriptions, see your specific vendor documentation. For a description of Cisco- supported attributes, see the Online Documentation or other device documentation at Cisco.com.
				(Back to Top)
				RAC Attribute Add/Edit
				Use this page to add/edit RADIUS attributes within a RADIUS Authorization Component (RAC).
				To add or edit the value of an attribute, either enter the appropriate value into the Value field or select from the displayed drop down list (depending on type). Then click Subenit.
				For value ranges, see your specific vendor documentation.
l l		Submit Clone Delet	e Cancel	Retex Vendors and attributes available for exelection are those test have devices defined in the Retex Konfiguration and the how attributes configured for display(at either group or user Ired) under Interface Canfiguration. To device the attribute from the RAC, click Delete at the bottom of the page. To conform that you To device the attribute from the RAC, click Delete at the bottom of the page. To conform that you
				To delete the attribute from the RAC, click Delete at the bottom of the page. To confirm that you I delete the attribute from the RAC, click Delete at the bottom of the page. To confirm that you I delete the attribute from the RAC, click Delete at the bottom of the page.

Γ

- **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:

CiscoSecure ACS - W	Vindows Inter	net Explorer					
🕒 🕤 • 🚺 http:/	/127.0.0.1:134	06/				💌 🍕 🗙 Google	P -
Ele Edit Yew Fgv		Beb					
Links O CiscoSecure AC	5 Trial		1				
🚖 🔷 👩 OscoSecu	ze ACS					🔄 • 🖸 🗸 📾 • 🔂 Bage •	
diala	Netwo	rk Access Profi	iles			Hab	×
User Setup	Con					Network Access Profiles	
Group Setup			Network Access Profiles		?	Typical organizations have various kinds of users, who access the network in	
Shared Profile Components		Name	Policies	Description	Active	different ways and for different purposes. Correspondingly, different security policies must be applied to t	
Network Configuration	0	MAB	Protocols Authentication		YES	different use cases. A Network Access Profile, also known	
System Configuration			Posture Validation Authorization			a profile, is a means to classify acces requests, according to AAA clients' IP addresses, membership in a network	
Configuration			Add Profile Add Template P	rofile		device group, protocol types, or othe specific RADIUS attribute values sent the network device through which the user connects.	t by
Deternal User		access when no pro	The Up/Down buttons submit and save the sort of	order to the database.		ACS traverses the ordered list of acti- profiles, and maps a RADSUS transac	tion
Perfuse Validation			I configuration, when no profile matches			to a profile by using a first-match strategy on the first access-request of the transaction.	× 1
Network Access Profiles			Apply and Restart			After you set up a profile, you associ	ate
Reports and Activity						a set of rules/policies with it, to refle your organization's security policies. These associations are called Profile Based Policies.	
Documentation						Configuring a profile based policy includes creating rules for the followin actions:	na 👘
						1. Protocols 2. Authentication 3. Posture Validation 4. Authorization	
						A profile is essentially a disatification network access requests for applying common policy. One example used profile is to aggregate all policies this to the network. The policies will be selected every time an excess-result initiated from that network location. Another usage is to aggregate all policies that handle the same device type (PM, Ap).	it iton st is
						Configuring Network Access Profiles	
						Add, edit, clone, order and configure policies for a treducti Access Profile here. Access requests are classified according to a first-match principle. Y can also specify if access should be granted or denied if an access request does not match any profile.	fow
						Add Profile Edit a Profile	188872
						Order the Network Access Profiles' I	<u>⊾</u> _ 28
Done						🕞 😜 Internet	100% • 2

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

CiscoSecure ACS - W	indows Internet Explorer		
• •	127.0.0.1:13406/		• + X Google P •
Ele Edit Yew Fgvo			
Links O CiscoSecure ACS			
🙀 🔗 👩 CiscoSecu	e ACS		🏠 + 🔂 - 📾 + 🕞 Bage + 🎯 Tgols + 🎽
cisco	Network Access Profi	les	E Help
User Setup			
		Profile Setup	Profile Setup
Group Setup			Use to this page to add, edit, clone, or delete a Network Access Profile.
Shared Profile Components	Name:	MAB	Set Profile Name and Status
Network Configuration		2	Set Up the Profile
			Clone a Profile
Sustem Configuration	Description:		Set Profile Name and Status
Configuration		Y I	1. Type the Name you want to assign to the
Administration Centrel	Active:	R	profile. 2. Enter a Description. 3. Use the Active checkbox to activate or
Deternal User Databases	C		 Use the Active checkbox to active or deactivate the profile. An inactive profile is ignored, and can be activated later.
	Network Access Filter:	(Any)	[Beck to Top]
Californian Validation		16e4V	Set Up the Profile
Network Access Profiles	2		Three conditions are used to determine
Reports and Activity	Protocol types		how an access-request is classified and mapped to a profile. The profile is
	C Allow any Protocol type		selected when all three conditions match. For each condition, you can
Documentation	Allow Selected Protoco		substitute the value "Any" to always match the condition.
		Addite () deas Addite () deas Addite () deas Addite () dease Addite ()	The profile determines the policies that ACS uses to process the accessivequest. If there is no matching profile, ACS fails by the global configuration settings.
		AACUU (Colum VP 300) Macoo Bockward Macoo Bockward AACUU (Colum Ashang) AACUU (Colum Ashang)	The following three ARD/set conditions are used to determine how an access request is classified and mapped to a profile.
		x x = 4 x	 Network Access Filters - NATs are groupings of AAA client configurations (which may represent multiple network devices), network device groups (NDGB), or 1P addresses of specific AAA client devices. NATs are configured in Shared Profile Components section.
	Advanced Filtering		
	Advanced Filtering	ACS compares the NAS-IP-Address of the access-request with the selected NAF. If it is found then the condition matches.	
		IO36/I000001 sizco-se-pair nol-exipt asa:service IO36/IO6enrice-Type = 10	Select a NAF from the drop down list.
		In the second se	[Back to Top]
		Submit Clone Delete Cancel	2. Protocol Type- Use this condition to select the AAA client vendor types from which access- requests are allowed. AAA clients are macced
Done			C (100%)



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.)
ſ

🔏 CiscoSecure ACS - Wi	ndows Internet Explorer		
😋 🕞 👻 🚺 http://:	127.0.0.1:1515/	• +7 ×	Live Search
Eile Edit ⊻iew Favor	rites Iools Help		
🚖 🏟 🔡 🕇 🍎 In	ternet Explorer cannot dis 1 CiscoSecure ACS 🗙	6	} ▼ 🗟 → 🖶 ▼ 🔂 Page ▼ 🍈 Tools ▼ 🎽
cisco	Network Access Profiles		Help
User Setup	Protocols Settings for MAB	<u></u> ?	Configuring Profiles - Setting Protocols
Setup	Populate from Global		Specify a profile's authentication rules, by setting allowed
Network Configuration	Authentication Protocols		protocols.
System Configuration	Allow PAP Allow CHAP		Populate from Global Authentication Protocols EAP Configuration
Configuration	Allow MS-CHAPv1 Allow MS-CHAPv2		Allow RADIUS Key Wrap PEAP
Administration Control	Allow Agentless Request Processing		<u>EAP-FAST</u> <u>EAP-TLS</u> EAP-MD5
External User Databases	EAP Configuration		
Network Access Profiles	Allow RADIUS Key Wrap		Populate from Global - Click to apply authentication
Reports and Activity	PEAP		settings that were set in the System Configuration-
Documentation	Allow EAP-GTC Allow Posture Validation		>Global Authentication Setup window. The form is populated
	Allow EAP-TLS		with the global settings, and can then be customized.
	EAP-FAST		Authentication Protocols
	Submit Cancel A change in authentication settings involves deletion of dynamic use to the profile. The change is applied after pressing "Apply and Restar		Allow PAP — To enable PAP, select this checkbox. PAP uses clear-text
Done			S Internet

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.

CiscoSecure ACS - Wi	ndows Internet Explorer					× O ×
G O http://1	27.0.0.1:13406/					💌 69 🗙 Google 🖉 P 1
Ble Edit View Favor	ites <u>I</u> ools Help					
Links 👩 OscoSecure ACS	Trial					
🚖 🕸 👩 OscoSecure	ACS					A * D * H * O Engel * O Tgols * **
atata	Network Access Profiles					×
cisco	Edit					Holp
User Setup						
						Authorization Policies
Group Setup		Authoriza	tion Rules fo	r MAB	?	Authorization policies comprise a set of rules for a Network Access Profile. The
Shared Profile Components						rules may be based on group membership, the posture of the machine that is ured to access the
Network Configuration	Condition		_	Action	Downloadable	network, or both. You may deny access for a specific user proup, or deny access
	User Group	System Posture Token	Access	Shared RAC	ACL	based on a returned posture token.
System Configuration	C 11: 6500-Employee (7 users)	Any		MAB-65-emp		When configuring authorization policies consider the following:
Configuration	C 12: 3750-Employee (5 users)	Any 💌		MAB-37-emp		The result of user authentication
Administration Control	C 10: 4500-Employee (8 users)			MAB-45-emp		is assignment to a User Group. • The result of posture validation is
Diternal User Databases	C 6: 37-partner (1 user)	Any 💌		MAB-37-partner		a Posture Token. • The result of SAP-FAST
	If a condition is not defined or there is	s no matched condition:	R	×	E	The result of BAP-PAST authentication and posture validation in the same session
Patienten	Include RADIUS attributes from use					results in assignment to a User Group and a Posture Token.
Nebwork Access Profiles	Include RADIUS attributes from use	r record				 When you deny access for a specific condition, you do not
Reports and Activity		Add Rule	Delete I	Up Down		need to select RAC or downloadable ACLs.
Documentation	The U			e sort order to the database.		Authorization Rules
Decumentation		S	ubmit Cano	el		Use to this page to add, select, order,
						configure or delete authorization rules.
						Add an Authorization Rule
						Order the Authorization Rules Delete an Authorization Rule
						Configure Authorization Rules
						Add an Authorization Policy
						Click Add Rule. A new row is added to the Authorization Rules list.
						Order the Authorization Rules
						Use the radio button to select the authorization rule you want to reorder. Click Up of Down to set the order.
						The authorization policy first match is implemented to authorize a client request.
						Note: Be certain to place your highest
						priority authorization policies at the top
						Group or for the Posture Token first match, the underlying policies will not be
Done						effective.
						1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

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:

ſ

```
set trunk 3/47 off negotiate 1-4094
set port dotlx 3/47 port-control auto
set port dotlx 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
bop 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
```



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

3. DHCP configuration:



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 dac11x 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:

 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
```

I

```
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
dotlx 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.



Cisco IOS/PIX 6.x RADIUS Attributes	?
<pre> [009\001] cisco-av-pair device-traffic-class=voice </pre>	85627

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.

U	ser List				
	User	Status	Group	Network Access Profile]စ္
	CP-7942G-SEP001E4A921AC9	Enabled	4500-ip-phone (1 users)	(Default)	



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.
- 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

- 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 XXXXXXX 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



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

I

Enterprise Network Virtualization – Access Control System Assurance Guide



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-model

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 OY set dot1x system-auth-control(CatOS)

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

dotlx pae authenticator

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

dot1x port-control auto OT 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
1
interface GigabitEthernet3/0/2
switchport mode access
dot1x pae authenticator
dot1x port-control auto
dot1x host-mode multi-host
dot1x timeout guiet-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



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.



Γ

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.

CiscoSecure ACS - 1	Windows Internet Explorer	
🕒 🔾 🔻 🚺 http:	://127.0.0.1:12966/	💌 4 🗙 Uve Search 👂 -
Ele Edit Yow Fa	vorites Ilools Help	
🚖 🕸 💠 🍎	Internet Explorer cannot dis O OscoSecure ACS 🗙	🛐 + 🔝 - 🖶 + 🕞 Bage + 🎯 Tgols + 🎽
cisco	Shared Profile Components	الله المان 🗵
CISCO Barry Barry Barry Barry Barry Construction Co	Contents Note: Act. Contents Noticat Notica	Plop Provide addition 10 PACL Adding or Editing a Downloadable 10 PACL Control addition 10 PACL Developed addition 10 PACL Develop
	Submit Cancel	

The following screen shot is a sample of the output in ACS server after the downloadable IP ACLs is created:

CiscoSecure ACS - W	Indows Internet Explorer	
(3) • (0) http://	[127.0.0.1:13406/	💌 🏘 🗙 Google 🖉 -
Ble Edit Yew Fav	orites Iools Help	
Links 👩 OscoSecure ACS	5 Trial	
🚖 🐟 👩 OscoSecu	re ACS	🖓 + 🖸 - 📾 + 🕑 Bage + 🎯 Tgols - 🤎
cisco	Shared Profile Components	160p
Error Error	Downloadable IP ACIS Image: Constraint of the sector of the	<text><list-item><list-item><list-item><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></list-item></list-item></list-item></text>
		🛛 🔽 🖓 🖓 Internet 🔍 💐 100% 🔹 📈

Γ

b. Add the ACE in the downloadable ACL content (click the dACL name will pop up the ACE content page).

CiscoSecure ACS - W	Vindows Internet Explorer	x D.s.
🕒 🕒 + 🚺 http://	(127.0.0.1:13406/	💌 fg 🗙 Google 🖉 r
Ele Edt Yew Favo	orites Iools Help	
Links 👩 OscoSecure ACS	5 Trial	
🙀 🔗 🛛 👩 Osco Secu	ze ACS	🛐 + 🖸 - 📾 + 🕑 Base + 🎯 Tgols + 🧮
cisco	Shared Profile Components	150p
		<text><list-item><list-item><list-item><list-item><section-header><section-header><list-item><list-item><list-item><section-header><section-header><section-header></section-header></section-header></section-header></list-item></list-item></list-item></section-header></section-header></list-item></list-item></list-item></list-item></text>
Done		🖌 🚺 Internet 👘 🔧 100% 🔹 🖉

c. Add and submit network access filter. In the network access filter, define which AAA client will use the dACL function.

CiscoSecure ACS - V	Vindows Internet Expl	arer 🛛				ĸ
• •	/127.0.0.1:13406/				• • • × Google /• •	
	orites <u>I</u> ools <u>H</u> elp					
Links O OscoSecure AC		1	-			
😪 🐼 👩 OscoSeo.	ire ACS				🖓 + 🖸 - 🕅 Age - 🕜 Tgols - '	
obob	Shared Prof	file Compone	nts		LX III III III III III III III III III I	8
CISCO	Edit			×	Help	1
User Setup						
Group Setup		Netwo	rk Access Filteri	ng	Adding a Network Access Filter Editing a Network Access Filter	
					Deleting a Network Access Filter	
Shared Profile Components	Name:	65-AAA-Client				
Network Configuration		6500 Clients		8	Use this page to create a NAF, edit a NAF, or delete a NAF.	
System Configuration	Description:				Adding a Network Access Filter	
				2	 Type a meaningful name in the Name box and type a useful description in the Description box. 	
Configuration		Network Device Oros		_		
Administration Control		(Net Assigned)	DEV:0500-a1		Add network device groups (NDGs), AAA clients (which may represent multiple network devices), and specific IP addresses for AAA client devices to the Selected Items list.	
Diternal User Dutabases			-3		O To add an NDG, highlight it in the Network Device Group list and click the adjacent right arrow button.	
Posture Validation		Network Devices			O To add a AAA client, highlight it and click the adjacent right arrow button. If you are using NDGs, the Network Device list only displays the AAA clients included in the highlighted NDG.	
Nebvock Access Profiles			-		O To add an IP address, type the address in the IP Address field and click the adjacent right arrow button.	
Reports and			12		You can remove an item from the Selected Items lat by highlighting the item and clicking the left arrow	
Activity		IP Address			button below the Selected Items list.	
Documentation			.s c up down		3. Click Submit.	
					[Back to Top]	
					Editing a Network Access Filter	
			P Back to Help		Change the settings as needed, but be aware of the following:	
					O If the NAF is in use with downloadable IP ACLs or network access restrictions (NARs), changes to the NAF can affect how the downloadable IP ACLs or NARs are applied to new user authorization requests.	
					O If you change the name of a NAF, any downloadable IP ACL or NAR using the NAF loses its association with the NAF and you must reconfigure the downloadable IP ACLs and NARs to use the new NAF name.	
					[Back to Top]	1
					Deleting a Network Access Filter	
					Noter Before you delete a NAP, be sure that you understand which downloadable IP ACLs and NARs the deletion will affect and that you have reconfigured those items as needed.	
					To delete the NAF, click Delete at the bottom of the page. To confirm that you want to delete the NAF, in the dialog box that appears, click OK .	
				-	[Beck to Top]	
		Submit 5	iubmit+Restart Delete C	Cancel		5
						000
Done					🕞 🚱 Internet 🔍 100% -	0

- 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.

cisco	User Setup	
User Setup	Downloadable ACLs	<u>?</u>
Group Setup	Assign IP ACL:	•
Shared Profile Components		
Network Configuration	Cisco IOS/PIX 6.x RADIUS Attributes	?
System Configuration	[009\001] cisco-av-pair	
Interface Configuration		
Administration Control	×	
Databases	1	
Posture Validation		
Network Access Profiles	IETF RADIUS Attributes	?
Reports and Activity	[027] Session-Timeout	
Online Documentation	[029] Termination-Action	
	Default	•
	[064] Tunnel-Type	
	Tag 1 💌 Value Tag 2 💌 Value	- -
	[065] Tunnel-Medium-Type	
	Tag 1 Value	•
	Tag 2 💌 Value	•
	[081] Tunnel-Private-Group-ID	
	Tag 1 🔽 Value	
	Tag 2 🔽 Value	
	Back to Help	
	Submit Delete Cancel	

- **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:

I

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

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

CiscoSecure ACS - Windows Internet Explorer	
G Nttp://127.0.0.1:12966/	💌 🌆 🗙 Live Search 🖉 -
Ele Edit View Favorites Iools Help	
🔆 🏟 🔃 🗙 🍎 Internet Explorer cannot dis 👩 OscoSecure ACS 🗙	🛅 + 🔝 - 🖶 Eage + 🎯 Tgols + 🎽
Shared Profile Components	×
CISCO Edit	A Help
RADIUS Authorization Components	• Name
Braup Setup	Description Add New Attribute
BaredProfile Name: MAB-65-partner	Assigned Attributes
Description:	BAE Attribute Add/Edit
Buten Configuration	Name
Configuration Add New Attribute	Type the name you want to assign to the RADIUS Authorization Component.
Cisco 105/PDX 5-0 (sisce-av-pair (s) Add	(Back to Top)
Databases IETF Service:Type (6) V Add	Description
Pastere Ascend Ascend-Remote-Addr (154) V Add	Type an explanation of the RADIUS Authorization Component.
	[Back to Top]
Pottie	Add New Attribute
Reports and Statistics	To add a new attribute, select the desired vendor attribute using the drop down list and click the adjacent Add button.
Della Constantation	Note: Vendors available for selection are those that have devices defined in the network for figuration and that have attributes configured for display (at either group or user level) under Interface Configuration.
	(Back to Top)
	Assigned Attributes
	The list of ADDUG stributes assigned to the Automization Component. To add or delete an already assigned attribute, click on the attribute value. On the gage that displays you can add or edit the attribute value. This section is only displayed when attributes have been assigned.
	For attribute descriptions, see your specific vendor documentation. For a description of Caso-supported attributes, see the Online Documentation or other device documentation at Casocom.
	[Back to Top]
	RAC Attribute Add/Edit
Submit Cancel	Use this page to add/edit RADIUS attributes within a RADIUS Authorization Component (RAC).
	Component (RAC). To add or add the value of an attribute, either enter the appropriate value into the Verse of the value of an attribute.
	📊 😼 🖓 🖓 Internet

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

ſ

Tunnel-Medium-Type (65) = 802

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

CiscoSecure ACS - V	Windows Interne <mark>t Exp</mark>	lorer			
🕒 🗸 🔹 🚺 http:	//127.0.0.1:12966/				💌 🔩 🗶 Uve Search 🖉 🖉
Ele Edit View Fax	vorites Iools Help				
🚖 🕸 🖾 🗸 🏉	Internet Explorer cannot	ds 👩 CiscoSecure ACS 🛛 🗙			🚱 - 🔝 - 🖶 Eage - 🎯 Tgols - 🎽
abab	Shared Pro	ofile Components			×
CISCO	Edit				Help 🗖
User Setup Setup Setup Setup		US Authorization		ents	Name Description Add New Attribute Assigned Attribute Roc Attribute Roc Attribute
Network Configuration	Description:	for 65-partner MAB	×		Name
Administration		Add New Attribute		?	name Type the name you want to assign to the RADIUS Authorization Component. [Early to Top]
Databases	Cisco IOS/PIX IETF Ascend	Service-Type (x note-Addr (154)	Add Add Add	Description Type an explanation of the RADIUS Authorization Component. [deck.to.Top]
Network Access Profiles					Add New Attribute To add a new attribute, select the desired vendor attribute using the drop down list
Activity		Assigned Attributes		?	and click the adjacent Add button.
201104 Decumentation	Vendor IETF IETF	Attribute Tunnel-Type (64) Tunnel-Medium-Type (65) Tunnel-Private-Group-ID (81)	Value (T11 VLAN (13) (T11 802 (6) (T11 221		Note: Vendors available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at either group or user (even) under Interface Configuration.
	(iere	(Towner-private-oroup-to (st)	111221		[Back to Top]
		💡 Back to Help			Assigned Attributes The list of RADIUS attributes assigned to the Authoritation Component. To edit or delete an already assigned attribute, click on the attribute value. On the page that displays you can add or add the attribute value. This section is only displayed when attributes have been assigned.
					For attribute descriptions, see your specific vendor documentation. For a description of Citors-responde attributes, see the Online Documentation or other device documentation at Cisco.com.
					[Back to Too] RAC Attribute Add/Edit
		Submit Clone Delete	Cancel		Vice horizonta again additional factors attributes within a RADIUS Authorization Component (RAC). To add or addit what value of an attribute, either enter the appropriate value into the To add the value of an attribute, either enter the appropriate value into the

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

Γ

🖉 CiscoSecure ACS - Win	dows Internet Explore	er and the second s		
G + ttp://12	27.0.0.1:1515/		💌 🐓 🗙 Live Search	₽ •
Eile Edit View Favorit	es <u>T</u> ools <u>H</u> elp			
😪 🍄 🔡 🖌 🏉 Inte	ernet Explorer cannot dis.	O CiscoSecure ACS X	🟠 • 🗟 • i	🖶 🔹 🔂 Page 🔹 🍥 Tools 🔹 🎽
de de	Network Acce	ess Profiles		×
cisco 🛓			- Help	
AlUser				
User Setup		Profile Setup	<u>?</u>	Profile Setup
Group Setup				Use to this page to add, edit, clone, or
Shared Profile Components	Name:	МАВ		delete a Network Access Profile.
Network		A.		Set Profile Name and
Configuration	Description:			Status
System Configuration		x		Set Up the Profile Clone a Profile
Configuration	Active:			Set Profile Name
Administration		<u>, 1</u>		and Status
External User Databases				Type the Name you want to assign to the profile.
	Network Access	Filter: (Any)	3. (Enter a Description. Use the Active checkbox to activate or deactivate the
Posture Validation				profile. An inactive profile is gnored, and can be
Network Access Profiles	Protocol types			activated later.
Reports and	C Allow any Pre			[Back to Top]
Activity	Allow Select	ed Protocol types		Set Up the Profile
Documentation		Protocol type Selected RADIUS (iPass) RADIUS (Cisco IOS/PIX.6		Three conditions are used to determine
		RADIUS (Nortel) RADIUS (Juniper)		how an access- request is classified
		RADIUS (Ascend)		and mapped to a profile. The profile is
		RADIUS (Cisco VPN 500)		selected when all
		RADIUS (Cisco VPN 3000 RADIUS (3COMUSR)		three conditions match. For each
		RADIUS (Cisco BBSM)		condition, you can substitute the value
		RADIUS (Cisco Aironet) RADIUS (Cisco Airespace		"Any" to always match the condition.
		Culturity Classe Delates Connect		
		Submit Clone Delete Cancel		The profile
Done			🛛 🕞 😽 Internet	€ 100% • //



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.)

Γ

CiscoSecure ACS - Wind	ows Internet Explorer		
😋 🕤 🗸 🚺 http://127	.0.0.1:1515/	• 🗙 🗔	ve Search 🖉 🔹
Eile Edit View Favorite	s Iools Help		
😭 🍄 🔡 🔹 🏀 Inter	net Explorer cannot dis 6 CiscoSecure ACS 🗙	<u> </u>	• 🗟 - 🖶 • 🔂 Page • 🎯 Tools • 🎽
	Network Access Profiles		X
cisco 🗕			
Ed	it		- Help
User Setup		-	Configuring Profiles - Setting Protocols
Group Setup	Protocols Settings for MAB	?	
Shared Profile Components	Populate from Global		Specify a profile's authentication rules, by setting allowed
Network	Authentication Protocols	-1	protocols.
Configuration		-	Populate from Global
System Configuration			Authentication Protocols EAP Configuration
Interface Configuration	Allow MS-CHAPv1		Allow RADIUS Key Wrap
-94 L Administration	Allow MS-CHAPv2	-	• <u>PEAP</u>
Control	Allow Agentless Request Processing		EAP-FAST EAP-TLS
Databases			• EAP-MD5
Posture Validation	EAP Configuration	-1	
Network Access Profiles	Allow RADIUS Key Wrap		Populate from
Profiles		-	Global - Click to apply authentication
Reports and Activity	PEAP		settings that were set in the System Configuration-
Online Documentation			>Global Authentication
Canal Cool in the state	Allow Posture Validation		Setup window. The form is populated
	Allow EAP-TLS		with the global settings, and can then be customized.
	EAP-FAST	-	Authentication
			Protocols
	Submit Cancel A change in authentication settings involves deletion of dynamic users linke	а	Allow PAP — To enable PAP, select
	to the profile. The change is applied after pressing "Apply and Restart" butto	in.	this checkbox. PAP uses clear-text
Done		- 🔽 🕰	uses clear-text
1		J 👽 J 🐨	

🖉 CiscoSecure ACS - Wi	ndows Internet Explorer		
😋 💽 👻 🔟 http://:	127.0.0.1:1515/	• + × u	ive Search 🔎
Eile Edit View Favor	rites Iools Help		
😪 🍄 🙁 🕶 🏉 In	ternet Explorer cannot dis O CiscoSecure ACS 🗙		• 🗟 -> 🖶 • 🔂 Page • 🎯 Tools •
	Network Access Profiles		[
cisco			
	Edit		≜ Help
User Setup	Protocols Settings for MAB	?	Configuring Profiles - Setting Protocols
Group Setup	Populate from Global		Specify a profile's
Shared Profile Components			authentication rules, by setting allowed
Network	Authentication Protocols		protocols.
Configuration	Allow PAP		Populate from Global
System Configuration	Allow CHAP		Authentication Protocols EAP Configuration
Configuration	□ Allow MS-CHAPv1		Allow RADIUS Key Wrap
Administration Control	Allow MS-CHAPv2		• <u>PEAP</u> • <u>EAP-FAST</u>
	Allow Agentless Request Processing		• EAP-TLS
Databases			EAP-MD5
Posture Validation	EAP Configuration		
Network Access Profiles	Allow RADIUS Key Wrap		Populate from Global - Click to
Reports and Activity	PEAP		apply authentication settings that were
	□ Allow EAP-MSCHAPv2		set in the System Configuration- >Global
Documentation	Allow EAP-GTC		Authentication Setup window. The
	Allow Posture Validation		form is populated with the global
	Allow EAP-TLS		settings, and can then be customized.
	EAP-FAST		Authentication Protocols
	Submit Cancel		Allow PAP - To
	A change in authentication settings involves deletion of dynamic users l		enable PAP, select this checkbox, PAP
	to the profile. The change is applied after pressing "Apply and Restart" b	outton.	uses clear-text
Done		🎑	Internet 🔍 100% 👻

11. Define the MAC address for authentication for each partner user and map it to the partner user group.

dialia	nternet Explorer cannot dis 0 CiscoSecure ACS				
haha		×		🐴 • 🔊 - 🕯	🛊 🔹 🔂 <u>P</u> age 🔹 🌀
cisco	Network Access Profiles				
User Setup Group Setup					
		Authorizatio	on Rules	for MAB	
Shared Profile Components Network	Condition			Action	
System Configuration	User Group	System Posture Token	Deny Access	Shared RAC	Downloadable ACL
Interface Configuration	C 11: 6500-Employee (7 users) 💌	Any 💌		MAB-65-emp	-
	0 12: 3750-Employee (5 users)	Any 💌		MAB-37-emp	-
Administration Control	0 10: 4500-Employee (18 users) 💌	Any 💌		MAB-45-emp	-
External User Databases	C 6: 37-partner (1 user)	Any 💌		MAB-37-partner	-
Posture Validation	C 4: 65-partner (1 user)	Any 💌		MAB-65-partner	dacl1x 💌
etwork Access rofiles	If a condition is not defined or there is no matched condition:			v	7
Reports and Activity	☑ Include RADIUS attributes from user's				
0nline Documentation	□ Include RADIUS attributes from user I	record			
	The Up/Down b	Add Rule	Delete	Up Down the database.	
		Subr		ancel	

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

I

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





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

I

• • Services Edge: Internet access



Figure 5-1 Guest Access Deployment Topology

I

Figure 5-2 802.1x Flow Guest Access Deployment

802.1x Flow for Guest Access Deployment



5-3

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.

<u>Note</u>

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-model

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

ſ

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:*

1

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

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%

The following table shows the details of QoS Traffic:

Table	B-1	Qos	Traffic
IUDIC		203	nume

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

I

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.

	Hardware	lardware		
Role	Platform	Line Card	Software	
Access L2	C3750E-24TD	StackWise (Four 3750E)	12.2(44)SE	
	C4507R	WS-X4516-10GE WS-X4548-GB-RJ45V	12.2(46)SG	
	C6506	WS-SUP32 WS-F6700-CFC WS-F6K-PFC3BXL WS-SUP720 (MSFC3) WS-X6704-10GE WS-X6148A-GE-45AF WS-X6548-GE-TX	8.7(1)	
Distribution (PE) L2 / L3	C6506	WS-SUP720-3BXL (Dual) WS-F6700-DFC3BXL WS-F6K-PFC3BXL WS-SUP720 (MSFC3) WS-X6704-10GE WS-X6748-GE-TX	12.2(33)SXH2a	
Core (P) L3	C6509	WS-SUP720-3BXL (Dual) WS-F6700-DFC3BXL WS-F6K-PFC3BXL WS-SUP720 (MSFC3) WS-X6704-10GE 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	
ССМ	Cisco Call Manager	N/A	6.1	

Table B-2 Hardware and Software and Device Information

B.3 Test Types

Validation tests are divided into the following categories:

- System Integration
- Scalability
- Reliability

B-5

B.4 System Integration

I

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.

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

Table B-3 Device Role and Feature Information

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

Table B-3Device Role and Feature Information	Table B-3	Device Role and Feature Information
--	-----------	-------------------------------------

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.

Та

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

able B-4	Device Role and Netwo	rk Scalability I	nformation

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.

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	

Table B-5 802.1x Supplicant Scalability Information

Downloadable ACL Scalability (CATOS):

ſ

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





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:					

- Client with Dot1x supplicant – no IP Phone.

I

- Client with Dot1x Supplicant with supplicant IP Phone.
- Client with Dot1x supplicant with supplicantless IP Phone.
- Client with Dot1x supplicant Fallback to MAC auth Bypass (MAB) no IP Phone.
- Client with Dot1x supplicant Fallback to MAC auth Bypass (MAB) with supplicant IP Phone.
- 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: Client with Dot1x supplicant – no IP Phone. 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:						

- Client without Dot1x supplicant – no IP Phone.

With no Dot1x	 	Passed	
supplicant			



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 CSCsI90751

Description: Dot1x critical: Re-auth of MAB kicks security violation. Severity: Moderate. Status: Resolved in IOS version 12.2(44)SG.

D.8 CSCs183010

Description: dot1x critical: phones cannot be recovered. Severity: Moderate. Status: Resolved in IOS version 12.2(44)SE2.

D.9 CSCs182998

Description: dot1x critical: Traffic allowed blindly on the Voice-VLAN. Severity: Moderate. Status: Resolved in IOS version 12.2(44)SE2.

D.10 CSCsI77063

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 CSCsI48111

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

ſ

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

I

Description: To Handle code review comments regarding Base code issues. Severity: Moderate. Status: Resolved in IOS versioin 12.2(33)SXH.