Identity-Based Networking Services: IP Telephony In IEEE 802.1X-Enabled Networks Deployment and Configuration Guide

Contents

1. Introduction 3
1.1 Solution Scope 3

2. About IP Telephony in Identity-Enabled Networks 4
2.1 Functional Overview 4
2.1.2 Device behind phone authenticates 8
2.1.3 Phone disconnects 10
2.1.4 Device behind phone disconnects: the link state issue 10
2.2 Benefits and Limitations 14
2.3 Feature Interaction 15
2.3.1 IEEE 802.1X 15
2.3.2 MAC Authentication Bypass (MAB) 23
2.3.3 WebAuth 24
2.3.4 Guest VLAN 24
2.3.5 Auth-Fail VLAN 25
2.3.6 Inaccessible-Auth Bypass 25
2.3.7 Dynamic ACL Assignment 25
2.3.8 Dynamic VLAN Assignment 26
2.3.9 Re-authentication 26
2.3.10 Wake on Lan 27
2.3.11 Open Access 27
2.3.12 Host Modes 28
2.3.13 RADIUS Accounting 29
2.3.14 AutoQoS 29
2.3.15 Auto Smart Ports 29
2.3.16 Port Security 29
2.3.17 DHCP Snooping 29
2.3.18 Dynamic ARP Inspection 29
2.3.19 IP Source Guard 29
2.3.20 Deployment Scenarios 29
2.4 Deployment Summary for IP Telephony 31

3. Configuring IP Telephony 32
3.1 Configure ACS (All Phone Authentication Types) 32
3.1.1 Configure the Switch as a RADIUS Client in ACS 33
3.1.2 Create a Phone Authorization Profile in Cisco Secure ACS 33
3.2 IEEE-802.1X Capable Phones 34
3.2.1 Enable Phones for IEEE 802.1X 34
3.2.2 Deploying LSCs 35
3.2.3 Export CA Certs from CUCM 36
3.2.4 Import CA Certificates into ACS 37
3.2.5 Configure an IEEE 802.1X Access Service 37
3.2.6 Create an IEEE 802.1X Service Selection Rule 42
3.3 Non-IEEE-802.1X Capable Phones 44
3.3.1 Enter Phone MAC Address in Cisco Secure ACS Internal Host Database 44
3.3.2 Configure an MAB Access Service 44
3.3.3 Create an MAB Service Selection Rule 48
3.4 Configure Switch (All Phone Authentication Types) 50
3.4.1 Verify Existing Configuration 50
3.4.2 IEEE 802.1X and MAB Configuration for IP Telephony 50
3.5 Monitor IP Telephony in an IEEE 802.1X Environment 52
3.5.1 Monitoring Sessions from The CLI 52
3.5.2 Monitoring Sessions from ACS 54
3.6 Troubleshoot IP Telephony In an IEEE 802.1X-enabled environment 55

4. Conclusion 55

5. Appendix A: References 55
5.1 Cisco Product Documentation 55

1. Introduction

As IEEE 802.1X becomes more widely deployed in wired networks, organizations must reconcile the Layer 2 access controls provided by IEEE 802.1X with the unique requirements of other technologies that also operate at the access layer of the network. One of the most widely deployed technologies that has specific requirements and expectations of the access layer is IP telephony. This whitepaper addresses deployment considerations and best practices when integrating IP telephony with an IEEE 802.1X-enabled network.

1.1 Solution Scope

The following hardware platforms and software releases are the recommended versions required to configure the features described in this guide:

- Cisco Catalyst® 2960 Series Switches with Cisco IOS® Software Release 12.2(52)SE
- Cisco Catalyst 3560 Series Switches with Cisco IOS Software Release 12.2(52)SE
- Cisco Catalyst 3750 Series Switches with Cisco IOS Software Release 12.2(52)SE
- Cisco Catalyst 4500 Series Switches with Cisco IOS Software Release 12.2(53)SG
- Cisco Catalyst 6500 Series Switches with Cisco IOS Software Release 12.2(33)SXI
- Cisco® Secure Access Control System (ACS) Version 5.1
- Cisco IP Phone Firmware 9.0.2
- Cisco Unified Communication Manager 7.1.2

Other switch platforms are expected to perform similarly with equivalent software releases. Earlier versions of software may also support the required functions with some caveats.

2. About IP Telephony in Identity-Enabled Networks

Cisco IOS software enables standards-based network access control at the access layer by using the IEEE 802.1X protocol to secure the physical ports where end users connect. 802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device. The IEEE standard was not, however, designed to accommodate the unique requirements of IP telephony. In particular, IP phones conflict with or complicate the requirements of IEEE 802.1X in the following ways:

- **Assumption of Network Access:** By default, IEEE 802.1X-enabled ports deny all access until and unless the attached device has successfully authenticated. IP phones, on the other hand, expect immediate access to the network.
- **Support for Two Devices Per Port:** Cisco IOS software enables IP telephony by allowing the same access switch port to provide network access to an IP phone and a data device connected on the Ethernet port behind the phone—with the phone only capable of sending tagged traffic on the voice VLAN and the PC capable of sending untagged traffic on the data VLAN. This is done to cut down on cabling, capital equipment, and administrative costs. IEEE 802.1X, however, does not address this issue directly.
- **Lack of Link State Awareness:** When an IP Phone is present, the switch has no knowledge of the link state of the port on the back of the IP Phone. IEEE 802.1X-enabled ports, however, rely heavily on link state to determine when to start and stop the authentication state machine. This functionality is essential to ensuring the validity of the authenticated session, thus preventing both security holes and security violations.

Successfully integrating IP telephony in an IEEE 802.1X-enabled network requires an end-to-end solution that can achieve the following:

- Phones that are capable of performing IEEE 802.1X must be configured to do so
- Phones that are not capable of IEEE 802.1X must be provided with some other means to access the voice network.
- IEEE 802.1X-enabled ports must address IP Telephony deployments with a phone and a data device on the same port.
- The lack of link-state awareness must be addressed.

This whitepaper describes how each of these requirements can be addressed in a Cisco-powered network.

2.1 Functional Overview

This section describes the recommended operation of IP telephony in an IEEE 802.1X-enabled network.

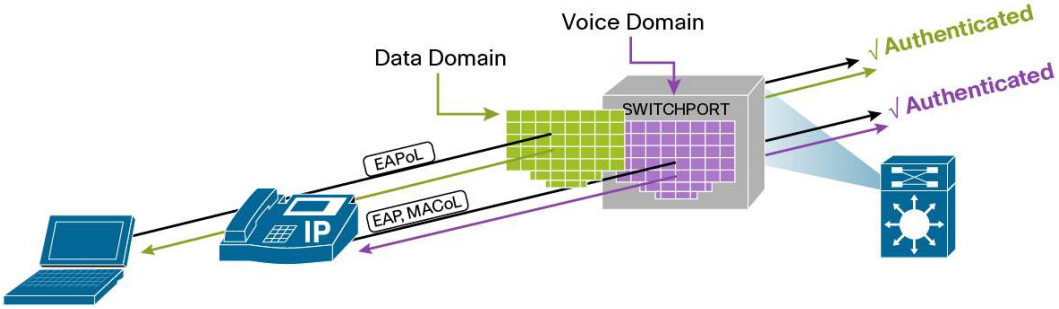
The most secure and flexible deployments of IP telephony start with Multi-Domain Authentication (MDA) host mode. MDA is a feature that allows a Cisco Catalyst switch to modify the default IEEE 802.1X requirement that only a single device connect to a switchport while retaining the security and visibility that IEEE 802.1X provides.

When properly enabled for MDA, the switch divides the switchport into two virtual “domains” (a domain is equivalent to a VLAN on a wired network). The switch independently and

asynchronously authenticates the phone and the device behind the phone. When the phone authenticates successfully, it is given access to the voice domain. When the device behind the phone is authorized, it is given access to the data domain. (See Figure 1.)

Note: The order of authentication is not relevant. In some scenarios, a data device may be able to authenticate in the Data domain before the IP Phone is authenticated in the Voice domain and vice versa. In addition, although MDA allows you to connect a phone and a data device to the same port, it does not require two devices to connect all the time. If only one device (a phone or a data device) is connected to a given switchport, the switch will authenticate that device into the correct domain.

Figure 1. Multi-Domain Authentication



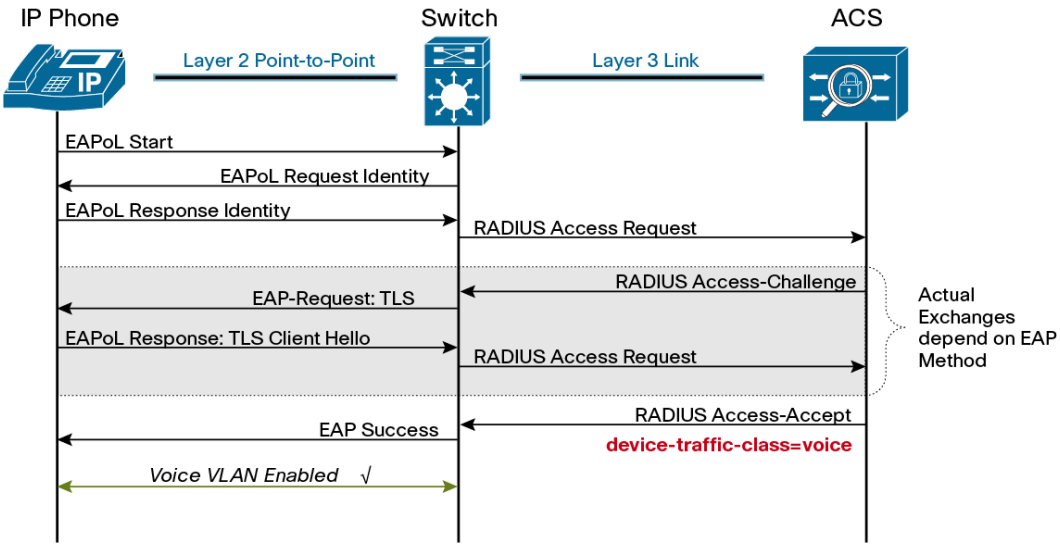
The following sections discuss the important stages of MDA.

2.1.1 Phone Authenticates

When a phone first plugs into a switchport, the LINK-UP event will trigger the start of the IEEE 802.1X state machine on the port. To get network access, the phone must now authenticate. Phones can authenticate in one of two ways: IEEE 802.1X or MAC Authentication Bypass (MAB). As part of a successful authentication, the AAA server must inform the switch that the authenticated device is a phone.

A typical IEEE 802.1X authentication for a phone is shown in Figure 2 below.

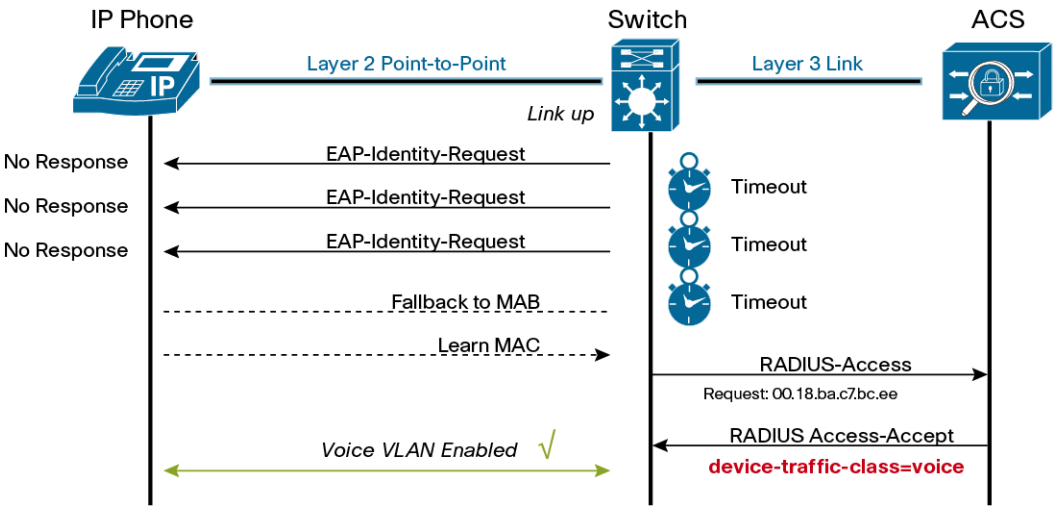
Figure 2. MDA with IEEE 802.1X Phone



For more details on operationalizing IEEE 802.1X for IP Phones, see Section 2.3.1.

A typical MAB authentication for a phone is shown in Figure 3 below. The switch initially tries to authenticate the phone using IEEE 802.1X. When there is no response to the Identity-Request messages, the switch times out and falls back to MAB.

Figure 3. MDA with MAB Phone



For more operational details on MAB for IP Phones, see Section 2.3.2.

Regardless of whether the phone is authenticated via IEEE 802.1X or MAB, the most important message (from the MDA perspective) is the final RADIUS Access-Accept from the ACS. The Access-Accept message contains a special Cisco Vendor Specific Attribute (VSA) that includes the string “device-traffic-class = voice.” This VSA is what tells the switch that the device that just authenticated is a phone and should be allowed access to the voice VLAN.

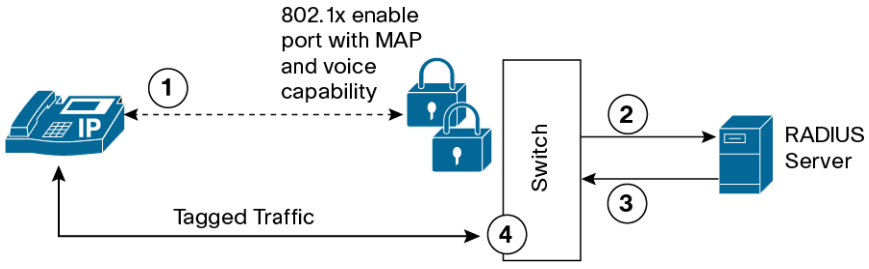
2.1.1.1 Cisco IP Phones vs Third Party Phones

At a high level, MDA behaves the same way no matter what kind of IP Phone is connected to the port. However, there are some functional differences between phones that require special consideration. Of particular importance is how the phone learns the voice VLAN. Cisco IP Phones and some third party phones learn the voice VLAN via CDP or LLDP. Other third party phones rely on a different mechanism such as DHCP or TFTP. MDA is flexible enough to handle both kinds of phones.

Cisco IP Phones (and LLDP-enabled phones)

Once a Cisco IP Phone is plugged into an MDA-enabled switch port, the sequences of steps highlighted in Figure 4 below occurs.

Figure 4. MDA with Cisco IP Phones



1. The Cisco IP Phone and the switch start exchanging CDP messages. The first CDP frame received from the Cisco IP Phone allows the switch to realize that a Cisco IP phone is actually connected to the port so that the right information (power level, VVID, etc) can then be delivered to the phone. CDP messages originated by the Cisco IP Phone are always untagged, even when the Cisco IP Phone learns the configured VVID. For non-Cisco phones that support LLDP for voice VLAN learning, the process is the same.

Note: Traffic Allowed Prior To Authentication

By default, IEEE 802.1X ensures that all traffic is dropped except for traffic needed for authentication. When MDA is enabled, however, the switch makes a few exceptions to this rule. Most notably, both CDP and LLDP are allowed prior to authentication. This allows phones to send and receive information regarding power requirements and the voice VLAN. Note that the processing of CDP does not mean that the phone is able to use CDP or LLDP to bypass authentication for general network access. Although phones may learn the voice VLAN via CDP or LLDP prior to authentication, the switch will drop all other traffic (tagged with the voice VLAN or not) if the phone has not authenticated.

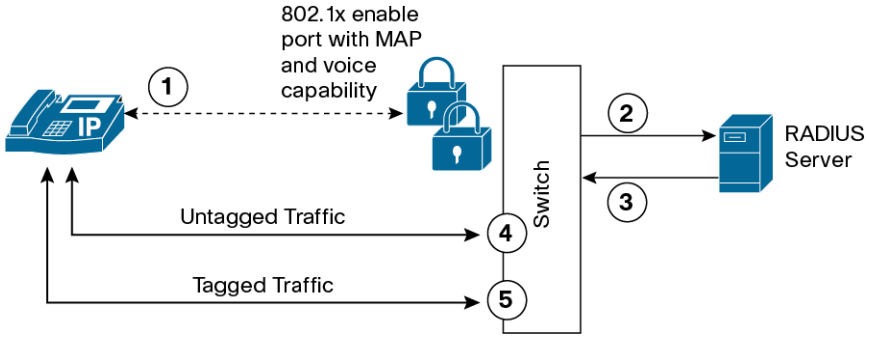
Since LLDP and CDP are allowed prior to authentication, Control Plane Policing (CoPP) can be used to prevent them from being used as a DoS attack vector. Consider enabling CoPP if your platform supports it.

2. Asynchronously from the CDP exchange, the process of authentication begins and the switch generates a RADIUS-Request sent to the backend Authentication Server.
3. Once the Cisco IP Phone is successfully authenticated via IEEE 802.1X or MAB, the AAA server sends a RADIUS-Accept message to the switch with the device-traffic-class=voice VSA. Once this attribute is received, the switch authorizes the phone's MAC and allows it access to the voice VLAN. The switch also temporarily allows the phone's MAC on the data VLAN (in case the phone has not yet learned the VVID).
4. Cisco IP Phone tags all its traffic leveraging the VVID information learned via the CDP exchange discussed in step 1) above. This traffic is allowed through the switch port as a result of authenticating the Cisco IP Phone MAC address in the Voice domain. Once the switch receives tagged traffic from the phone (indicating that the phone has learned the VVID), the switch no longer allows the phone's MAC on the data VLAN.

Third-Party IP phones Without LLDP

When a third-party IP phone is plugged into an MDA-enabled switch port, the procedure required to allow it to achieve network connectivity is slightly different a Cisco IP Phone. (See Figure 5.) This is because third-party phones may not be capable of sending LLDP frames to learn the voice VLAN.

Figure 5. MDA with Third-Party IP phones



1. After link up, the IP phone sends untagged traffic (assuming that the Voice VLAN has not been statically configured on the phone). All this traffic is initially dropped because the switch port is unauthorized.
2. Asynchronously from the sending of untagged traffic discussed above, the process of authentication is started and the switch sends a RADIUS-Access-Request to the AAA server.
3. Once the connecting IP phone is successfully authenticated via IEEE 802.1X or MAB, the AAA server responds with a RADIUS-Access-Accept with the device-traffic-class=voice VSA and the switch port will be authorized in the Voice domain.
4. Port forwarding is still authorized on both the Voice and Data VLANs at this point. While the switch generally limits authenticated phones to the voice VLAN, MDA makes a temporary exception to accommodate third-party phones that do not learn the voice VLAN via CDP or LLDP. Immediately after authentication, phones are allowed to send untagged traffic in the data VLAN. This allows a third party phone to learn the voice VLAN (typically via DHCP or TFTP) on the data VLAN.
5. After learning the VVID, the IP phone starts tagging traffic. The switch immediately removes the temporary access to the data VLAN and the phone is strictly limited to the voice VLAN. Access to the Data VLAN is now prohibited for the IP phone.

2.1.2 Device behind phone authenticates

MDA requires that the device behind the phone successfully authenticate to gain access to the network. Because the data device is not directly connected to the switch, the switch cannot rely on link state to know when to start authenticating the data device. Therefore, the switch waits until it detects traffic from the second device (such as an EAPoL-Start from an IEEE 802.1X supplicant or DHCP or ARP traffic from a non-IEEE-802.1X-capable device), at which point it sends a unicast EAPoL Request packet to the device to initiate the authentication.

Note: Multicast vs. Unicast EAPoL

An IP Phone usually sends multicast EAPoL frames to the switch with the destination MAC address 01-80-C2-00-00-03. The switch, however, responds with unicast EAPoL frames to the IP Phone's MAC address. The sending of unicast EAPoL frames from the switch is an important characteristic of MDA. When the IP Phone first connects to the switch port, the switch may initiate a transmission of multicast EAPoL messages and revert to unicast as soon as the MAC address of the device is learned. When a device connects behind the phone, however, the switch sends no EAPoL frames until the MAC address of the device is learned. This way, the switch will not risk disturbing the phone's authenticated session. By using unicast EAPoL messages, the switch can independently authenticate both devices.

If the data device is not ready to or not capable of performing IEEE 802.lX, the switch will time out and continue to the next authentication method (e.g. MAB) and/or authorization type (e.g. Guest VLAN). If the device later becomes capable of performing IEEE 802.1X (e.g. because the operating system finished booting or a supplicant was manually enabled), then the data device should send an EAPoL-Start message to explicitly tell the switch to begin authentication.

Best Practice Recommendation: Configure Supplicants to send EAPoL-Starts

Although EAPoL-Starts are optional according to the IEEE specification, they perform an important function by ensuring that a supplicant can authenticate, even if the switch has already timed out IEEE 802.1X. If your supplicant does not send EAPoL-starts by default, Cisco recommends enabling them.

If the data device passes authentication (either via 802.1X or MAB), it will be allowed access to the data domain only. If the device fails authentication, it will not be allowed access to either domain (unless the Auth-Fail VLAN has been configured), but the phone will continue to operate normally.

Note: MDA, Failed Authentications and Security Violations

MDA extends the default single-device-per-port requirement to allow two devices, one in the voice domain and one in the data domain. If more than one device is detected in either domain, a security violation will be triggered. This can be a problem when a phone fails to authenticate properly. If a phone fails authentication, then the switch does not receive the "device-traffic-class=voice" VSA from the AAA server and the switch will assume that the failed device was in the data domain. But if there is already a data device behind the phone, there will now be two devices in the data domain, and a security violation is triggered. So while a failed authentication in the data domain does not affect a passed authentication in the voice domain, the inverse is not true. A failed authentication in the voice domain can adversely affect a passed authentication in the data domain.

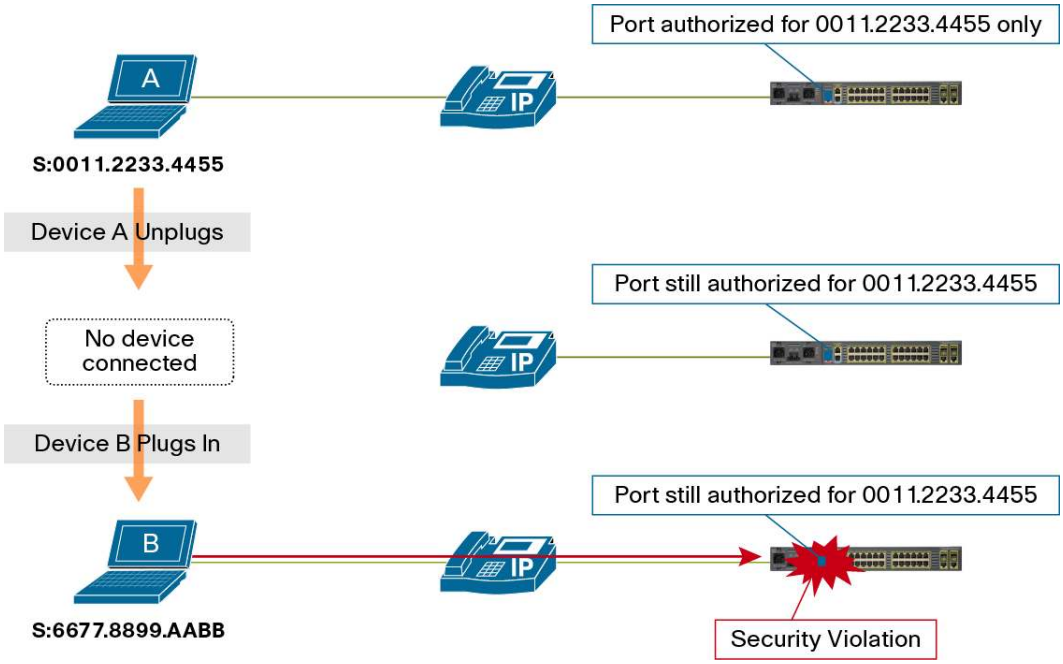
2.1.3 Phone disconnects

If the phone unplugs from the switch, link state will go down and the switch will clear all sessions on the port. Any phone or device that later connects to that same port will be forced to authenticate to gain access.

2.1.4 Device behind phone disconnects: the link state issue

If the device unplugs from behind the phone, the switch cannot rely on link state to know when to clear the session. Dangling sessions can lead to security violations and security holes. Take the situation illustrated in Figure 6 below.

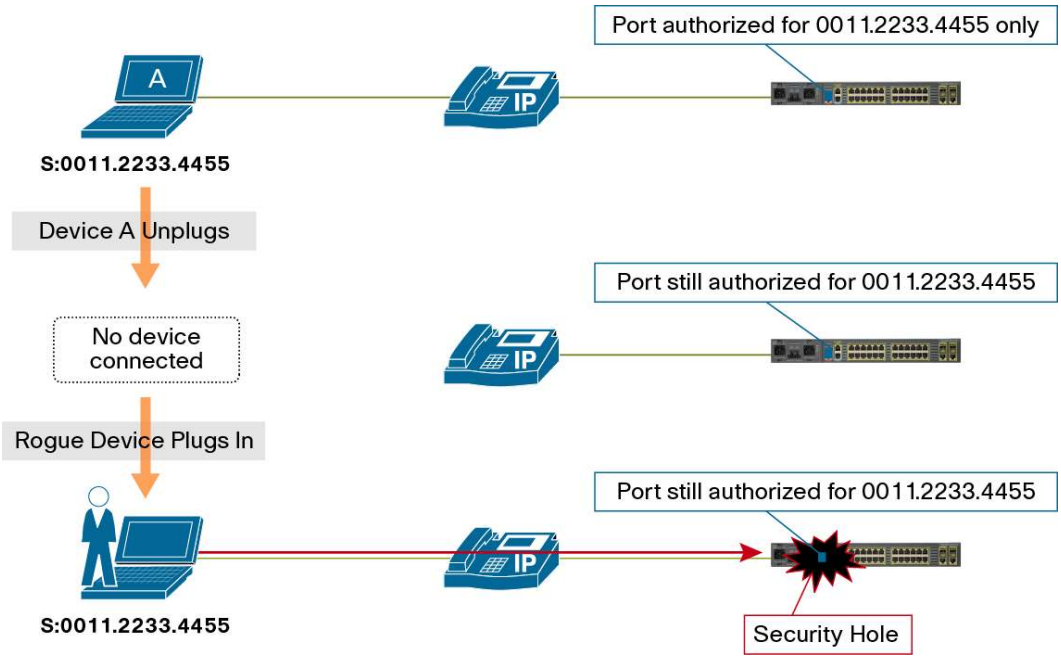
Figure 6. Link State Problem 1: Authorized User B Triggers Security Violation



In the figure above, Device A has previously authenticated behind the IP Phone. Device A unplugs, but the switch, not knowing A has left, keeps the port authorized for Device A's MAC address only. Sometime later, Device B plugs in and sends traffic. Because there is still an existing session for Device A, the switch does not attempt to authenticate Device B. From the switch's perspective, Device B is an unauthorized device that may be trying to piggyback on Device A's authenticated session. Therefore, the switch immediately triggers a security violation.

Another consequence of not removing authenticated session when the data device disconnects from behind the phone is a security hole that could be exploited by a rogue user. This security hole is illustrated in Figure 7 below.

Figure 7. Link State Problem 2: Rogue User Spoofs Authenticated User's Session



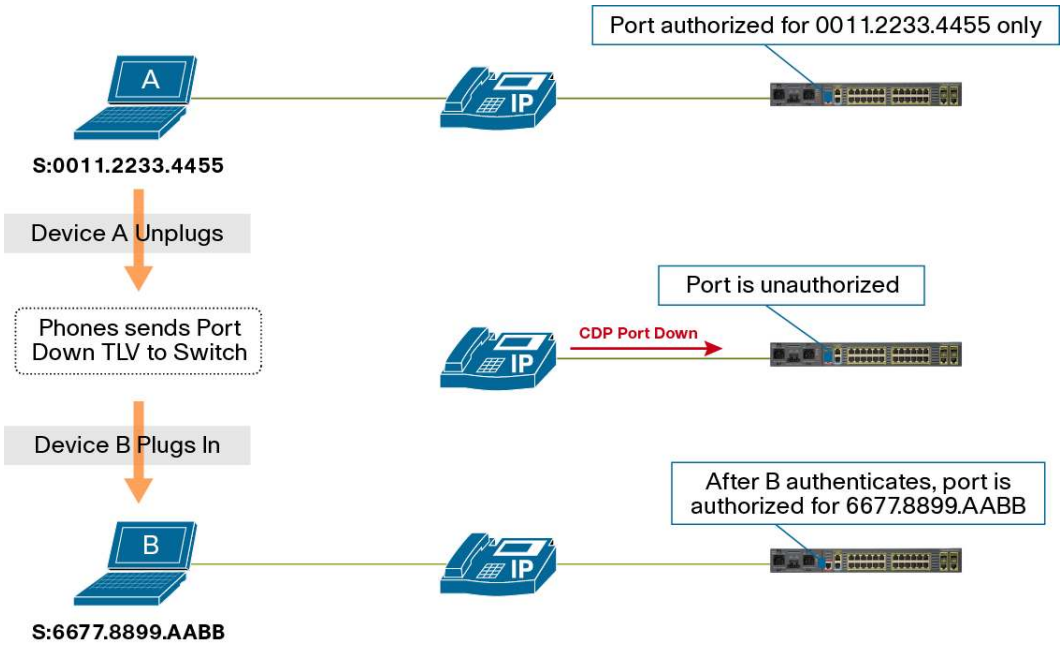
In the figure above, Device A has previously authenticated behind the IP Phone. Device A unplugs, but the switch, not knowing A has left, keeps the port authorized for Device A's MAC address. Sometime later, a rogue user plugs in and spoofs Device A's MAC address. Because there is still an existing session for Device A, the switch allows all traffic from the rogue device without forcing the rogue device to authenticate.

To avoid security violations and security holes, some method must be used to clear the session for the data domain. This section discusses three possible solutions, in order of preference. One or more of these methods must be operational to ensure smooth integration of IP Telephony and IEEE 802.1X.

Cisco Discovery Protocol (CDP) Enhancement for Second Port Disconnect

The best solution for the lack of direct link state awareness is to address the root cause. The switch does not know the link state of the phone's data port ("the second port"), but the phone does. Therefore, if the phone could communicate link state to the switch, then the switch could immediately clear the session. This is exactly what the CDP Enhancement for Second Port Disconnect (aka "Host Movement Detection") does. Cisco IP Phones can send a CDP message to the switch indicating that the link state for the data device's port is down, allowing the switch to immediately clear the data device's session. (See Figure 8 below.)

Figure 8. Recommended Link State Solution: CDP Enhancement For 2nd Port Disconnect



Cisco IP Phones and Catalyst switches with the appropriate releases of code automatically perform CDP Enhancement for Second Port Disconnect. It works for all authentication methods (IEEE 802.1X, MAB, Web-Auth) and no configuration is required.

Best Practice Recommendation: Use CDP Enhancement for Second Port Disconnect

This feature works for all authentication method, takes effect as soon as the device disconnects, and requires no configuration. If you are using Cisco IP Phones and Catalyst switches with the appropriate release of code, this is the simplest and most effective solution. No other method works as well to address the switch's inability to detect link state for devices connected behind IP Phones.

Table 1. CDP Enhancement for Second Port Disconnect Support

Cisco IP Phone Model	Minimum firmware for CDP Enhancement for Second Port Disconnect ("Host Movement Detection")
7902, 7905, 7910, 7912, 7920, 7935, 7936	Not Supported
7940, 7960	8.1(1)
7906, 7911	8.4(1)
7931, 7937	8.4(1)
7941, 7942-G, 7945-G	8.4(1)
7961, 7962-G, 7965-G	8.4(1)
7970, 7971, 7975-G	8.4(1)

Proxy EAPoL-Logoff

If your switch or phone does not support CDP Enhancement for Second Port Disconnect, Proxy EAPoL-Logoff can provide a partial solution for IEEE 802.1X-authenticated data devices. Proxy EAPoL Logoff enables the phone to transmit an EAPoL-Logoff message on behalf of the data device when the phone detects that an IEEE 802.1X device has unplugged from behind the phone.

The phone substitutes the data device's MAC address, so the proxy EAPoL-Logoff message is indistinguishable from an actual EAPoL-Logoff from the data device itself. The switch will immediately clear the session as soon as it receives the Logoff message.

To support this feature, your phone must be capable of sending proxy EAPoL-Logoff messages. All Cisco IP Phones and some third party phones provide this functionality. No special functionality is required from the switch since the EAPoL-Logoff message is fully support as per the IEEE standard.

While effective for IEEE 802.1X-authenticated endpoints, Proxy EAPoL-Logoff will not work for MAB or WebAuth, since these authentication methods do not use EAP to authenticate. Another method, such as Inactivity Timer, must be used to ensure that MAB sessions are appropriately cleared.

Inactivity Timer

If your switch or phone does not support CDP Enhancement for Second Port Disconnect, the inactivity timer can provide a partial solution for disconnected data devices. When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When a device disconnects, the inactivity timer will countdown. When the timer expires, the switch removes the authenticated session. The inactivity timer applies to IEEE 802.1X and MAB sessions.

Note: Inactivity Timer Does Not Clear WebAuth Sessions

The current implementation of WebAuth uses a different (IP Device Tracking-based) inactivity timer than IEEE 802.1X and MAB. This timer clears the WebAuth authorization state, but it does not clear the entire session state. The only way to clear a WebAuth session behind a phone is to use the CDP Enhancement for Second Port Disconnect.

The inactivity timer for IEEE 802.1X and MAB can be statically configured on the switch port or it can be dynamically assigned using RADIUS attribute 28. Cisco recommends setting the timer via the RADIUS attribute as this gives you control over what devices are subject to this timer and how long the timer is for each class of devices. For example, if your phones are capable of Proxy-EAPoL-Logoff, then there would be no need to assign an inactivity timer for IEEE 802.1X-authenticated session. In this scenario, you could prevent the inactivity timer from being needlessly assigned to IEEE 802.1X-authenticated devices by only sending RADIUS Attribute 28 to MAB-authenticated devices.

There are two important caveats when using the inactivity timer to clear sessions from behind IP Phones. First, while the inactivity timer is counting down, the port is still subject to the potential security violation and security hole described above. Second, the inactivity timer is an indirect mechanism the switch uses to infer that a device has disconnected. An expired inactivity timer cannot guarantee that a device has disconnected. So a "quiet" device that does not send traffic for long periods of time (e.g. a network printer that services occasional requests but is otherwise silent) may have its session cleared even though it is still connected. That device will then have to send traffic before it can be authenticated again and have access to the network.

In general, testing will be required to find an optimal value for the inactivity timer in your network -- short enough to minimize the impact of security violations and holes, long enough to prevent “quiet” devices from being inadvertently disconnected from the network.

In summary, the best practices for using the inactivity timer to clear sessions behind IP Phones are as follows:

- Only use the inactivity timer if there is no other way to address the link-state issue.
- Use RADIUS to dynamically assign the best inactivity timeout value for each class of device authenticating via IEEE 802.1X or MAB.
- If your phones support proxy EAPoL-Logoff, rely on that feature to clear sessions for IEEE 802.1X-authenticated devices and use the RADIUS-assigned inactivity timer for MAB devices.
- Test your network to find the optimal value for this timer. Use the smallest possible value that doesn’t impact your quiet devices.

2.2 Benefits and Limitations

An IEEE 802.1X-aware IP telephony system and a flexible policy server must be part of an intelligent infrastructure. Cisco can deliver an end-to-end solution for an IEEE 802.1X-enabled network that fully integrates IP telephony. Key features in this solution include:

- **Multi-Domain Authentication (MDA):** MDA is a feature on Cisco Catalyst switches that divides a single port into two “domains”: the voice domain and the data domain. MDA enables the switch to independently authenticate a voice device and a data device on the same switch port.
- **Cisco Discovery Protocol (CDP) Enhancement for Second Port Disconnect:.** This feature allows a Cisco IP phone to send a CDP message to the switch when a host unplugs from behind the phone. The switch is then able to clear any authenticated session for the indirectly connected host, exactly the same as if the host had been directly connected and the switch had detected a link down event.

In addition to solving system integration issues, a Cisco solution also provides many enhancements and optimizations that lower barriers to deployment. These feature include:

- **IEEE 802.1X Capable IP Phones:** Many versions of Cisco’s IP Phones support IEEE 802.1X. They can use either pre-provisioned Manufacturing Installed Certificates (MIC) or customer-controlled Locally Significant Certificates (LSC)for IEEE 802.1X authentication.
- **Touchless Phone Configuration and Certificate Enrollment:** Starting in version 7.1.2, the Cisco Unified Communication Manager (CUCM) can centrally enable phones for IEEE 802.1X via a downloaded configuration file. In addition, CUCM provides a Certificate Authority Proxy Function (CAPF) that enables phones to enroll locally-signed LSCs to use for authentication. Since these functions are performed over the network, there is no need to physically touch the phones.
- **Touchless Phone Authentication:** Cisco Access Control Server (ACS) can be configured to authenticate IP Phones and authorize them into the voice domain purely on the basis of a valid certificate. Since the certificate attributes alone can be used to determine whether or not this is a valid phone, there is no need to enter the names of the phones in any database

(internal or external). This significantly reduces the amount of configuration required to support IP phones.

While this solution has been optimized for an end-to-end Cisco solution with the latest code and firmware revisions, many additional features are available to support legacy and/or 3rd party devices. These features include:

- **MAC Authentication Bypass (MAB):** MAB is a secondary authentication method that enables a Cisco Catalyst switch to check the connecting device's MAC address in lieu of a successful IEEE 802.1X authentication. Phones that cannot perform IEEE 802.1X can be authenticated based on a MAC address.
- **Flexible Authentication (FlexAuth):** FlexAuth is a combination of features that enables you to deploy a single configuration for every port in the network and know that the Catalyst Cisco switch will intelligently apply the correct authentication and authorization policy, regardless of whether the device is a phone or a PC or whether the device is capable of IEEE 802.1X or not. FlexAuth also enables you to configure the order and priority of authentication methods so that you can choose the combination that works best for your network.
- **Proxy EAPoL-Logoff:** If the phone and/or switch cannot support CDP Enhancement for Second Port Disconnect, a Cisco IP Phone can send a proxy EAPoL-Logoff message to the switch when an IEEE 802.1X-authenticated device unplugs from behind the phone. This allows the switch to cleanly terminate the authenticated session in the absence of direct knowledge of the link state of the port to which the device was connected. Unlike CDP Enhancement for Second Port Disconnect, however, this feature only works for IEEE 802.1X authenticated devices.
- **Inactivity Timer:** If there is no activity from a client, the switch can be configured to terminate the authorized session after a period of time. This feature can be used to terminate sessions of devices that disconnect from behind phones. The inactivity timer provides a way to terminate MAB sessions when CDP Enhancement for Second Port Disconnect is not available. The inactivity timer can also be used to terminate IEEE 802.1X-authenticated sessions if the phone does not support proxy EAPoL-Logoff.
- **Configurable Security Violation Handling:** This feature can be used in conjunction with the inactivity timer. If another device attempts to authenticate behind a phone before the inactivity timer has expired, a security violation will be triggered. By default, some Catalyst switches will err-disable (shutdown) the port in response to a violation. Shutting down the port will immediately cause the phone to go offline as well. Configurable security violation handling allows Cisco Catalyst switches to take alternative actions (such as dropping traffic from the new device) that have a less drastic effect on the phone.

2.3 Feature Interaction

2.3.1 IEEE 802.1X

When MDA is enabled, both the phone and the device behind the phone can authenticate using IEEE 802.1X.

There is nothing special about IEEE 802.1X on phones: phones use the same protocols and submit the same types of credentials as other users and devices that perform IEEE 802.1X. However, there are some unique requirements for preparing the voice and authentication

infrastructure for IP Phones. The following sections discuss deployment considerations and best practices for enabling IEEE 802.1X on IP Phones. While the focus here is on Cisco IP Phones, many of these same principles will apply to other kinds of IP Phones as well.

2.3.1.1 Credentials for IP Phones

To successfully authenticate using IEEE 802.1X, the phone must present some form of credential to identify itself, typically either an X.509 digital certificate or a password.

Best Practice Recommendation: Use X.509 Certificates For Phone Authentication

In addition to providing the strongest form of authentication, X.509 certificates on Cisco IP Phones are simple to deploy. They can be validated by the ACS in a single authorization rule without the need to configure and maintain a database of phone usernames and/or

2.3.1.1.1 Certificates

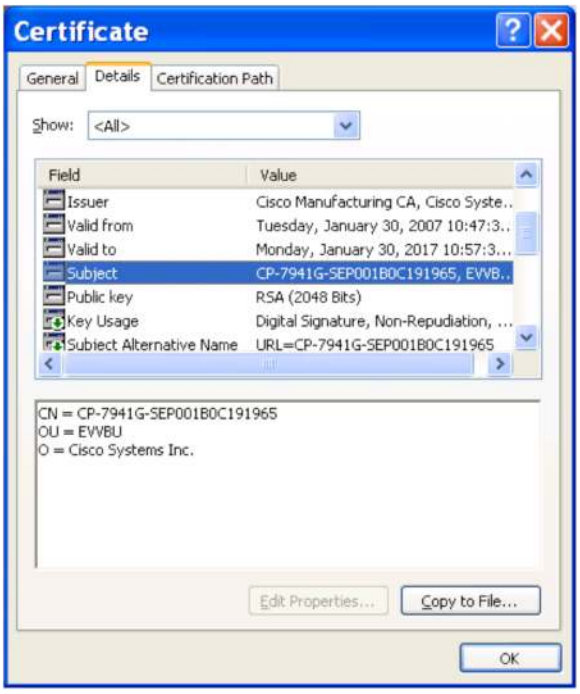
The following Cisco IP Phones support authentication via X.509 Certificates using the EAP-TLS or EAP-FAST methods of authentication:

Table 2. Certificate-based IEEE 802.1X support

Cisco IP Phone Model	Minimum firmware for X.509 Certificate-based IEEE 802.1X using EAP-TLS or EAP-FAST	Recommended firmware for IEEE 802.1X
7906, 7911	8.5(2)	9.0(2)
7931, 7937	8.5(2)	9.0(2)
7941, 7942-G, 7945-G	8.5(2)	9.0(2)
7961, 7962-G, 7965-G	8.5(2)	9.0(2)
7970, 7971, 7975-G	8.5(2)	9.0(2)

Cisco IP Phones support two types of X.509 certificates: the Manufacturing Installed Certificate (MIC) and the Locally Significant Certificate (LSC). Customers typically leverage MICs and LSCs in order to secure the signaling and voice path used for IP telephony, but these same certificates can be used for IEEE 802.1X.

As the name suggests, the MIC is pre-loaded on the phone at the time of manufacture. It is signed by the Cisco Manufacturing Certificate Authority. A sample MIC is shown below:



The detailed fields for this example MIC are shown in the table below:

Key	Field
Version	V3
Serial Number	110021dd0000000dce3f
Signature Algorithm	sha1RSA
Valid From	January 30, 2007
Valid To	January 30, 2017
Subject	Common Name=CP-7941G-SEP001B0C191965 Organization = Cisco Systems Inc. Organization Unit = EVVBU
Public Key	RSA (2048 Bits)
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Subject Alternative Names	URI:CP-7941G-SEP001B0C191965
Subject Key Identifier	a1 9e f4 fc c3 ba 7b 3b 7f ce 9d 1f 1f cc 02 12 9a e2 37 03
Authority Key Identifier	KeyID=d0 c5 22 26 ab 4f 46 60 ec ae 05 91 c7 dc 5a d1 b0 47 f6 6c
CRL Distribution Points	Distribution Point Name:Full Name:URL=http://www.cisco.com/security/pki/crl/cmca.crl
Authority Information Access	Access method=Certificate Authority Issuer Alternative Name: URL=http:// www.cisco.com/security/pki/crl/cmca.crl
Certificate Template Name	IPSECIntermediateOffline
Enhanced Key Usage	Server Authentication Client Authentication IP security end system
Thumbprint algorithm	sha1
Thumbprint	F2 4b 0a 91 60 77 2a 20 62 46 39 2d 44 5d c5 ed 73 71 81 93

Tip: Viewing Phone Certificates

One way to view the actual certificate on the phone is to use the Troubleshoot operation in the CAPF Settings of the Phone Configuration window in CUCM. This option retrieves the LSC or the MIC, so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified Communications Manager creates two trace files, one for each certificate type. The Troubleshoot option does not display if a certificate does not exist in the phone. After scheduling the Troubleshoot option within CUCM, LSC and MIC certificates will be stored in following locations on CUCM: /var/log/active/cm/trace/capf/sdi.

Another way to view the phone's certificate is to get a sniffer trace of the EAP-TLS authentication and examine the contents of the certificate as it is being sent.

A phone that presents a valid MIC can be assumed to be a valid Cisco phone. However, the MIC by itself cannot be used to determine if this phone is a corporate asset or a rogue Cisco phone. For that, you need an LSC. Unlike the MIC, the LSC is signed by the Certificate Authority Proxy Function (CAPF) of the Cisco Unified Communication Manager (CUCM), the central call control and configuration engine for Cisco IP Telephony.

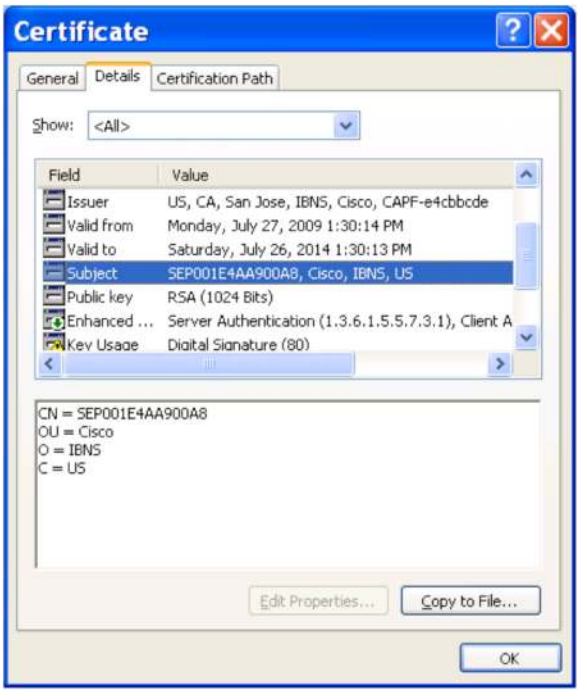
Note: Self-signed CAPF vs. CA-signed CAPF

CUCM can sign LSCs using two different types of CAPF: self-signed CAPF or CA-signed CAPF. A self-signed CAPF acts as a standalone CA, signing the LSCs with its own self-signed certificate. A CA-signed CAPF, on the other hand, is signed by an external CA. A CA-signed CAPF signs the LSCs with the externally signed certificate.

Self-signed CAPF CAs have a lifetime of 5 years. Therefore, if you use a self-signed CAPF, the CAPF certificate must be renewed after 5 years and all the LSCs will have to be reissued. The ACS will not allow the phones network access if the LSCs have expired.

The lifetime of the CA-signed CAPF is determined by the CA when it issues the certificate to CUCM. Whatever lifetime you choose, be sure to renew the CAPF certificate and reissue the LSCs prior to expiration.

Because the LSC has been issued by your own CUCM Certificate Authority, you can be certain that a phone presenting a valid LSC is in fact a corporate owned and managed asset. A sample LSC is shown below:



The detailed fields for this example LSC are shown in the table below:

Key	Field
Version	V3
Serial Number	01
Signature Algorithm	sha1RSA
Valid From	July 27, 2009
Valid To	July 26, 2014
Subject	Common Name=SEP001E4AA900A8 Organization = IBNS Organization Unit = Cisco Country = US
Public Key	RSA (1024 Bits)
Key Usage	Digital Signature
Enhanced Key Usage	Server Authentication Client Authentication IP security end system
Thumbprint algorithm	sha1
Thumbprint	13 22 29 02 39 42 50 20 9a 3c 52 8e f0 cb dc f1 dd cf 83 f6

Because you control the enrollment of LSCs on phones, LSCs represent a more tightly controlled and trusted credential than MICs.

The following table highlights some key difference between LSCs and MICs.

	MIC	LSC
Issued By	Varies. Typically one of the following: • Cisco Manufacturing CA • Cisco Root CA • CAP-RTP-001 • CAP-RTP-002	CAPF CA
Subject Attributes	Common Name Organization Organizational Unit	Country Common Name Organization Organizational Unit
Common Name Format	CP-XXXXX-SEPYYYYYYYYYYYY where XXXXX is the phone model and YYYYYYYYYYYY is the MAC address of the phone	SEPYYYYYYYYYYYY where YYYYYYYYYYYY is the MAC address of the phone
Organization	Cisco Systems Inc	Determined by CAPF configuration
Organizational Unit	evvbu	Determined by CAPF configuration
Validity	10 years	Configurable, default 5 years
Key Size	2048	Configurable, default 1024
Renewal	N/A	Manually re-issue LSC from CUCM at end of lifetime
Revocation	Not supported.	Not supported
Best Use Cases	Lab testing, bootstrapping a phone onto the network	General Use

In an IEEE 802.1X authentication, the AAA server is responsible for validating the certificate provided by the phone. To do this, the AAA server must have a copy of the root CA certificate that signed the phone's certificate. The root certificates for both LSCs and MICs can be exported from the CUCM Operating System Administration interface and imported into your AAA server.

Once the certificate has been validated, the AAA server may be able to authorize the phone simply based on attributes in the certificate. This is the recommended way to authorize phones with certificates, since it enables you to authenticate and authorize phones with a single global policy and avoids the need to enter individual phones in a database. Cisco ACS supports this type of authorization, but not all AAA servers do.

Best Practice Recommendation: Use Certificate Attributes for Phone Authorization

Using certificate attributes to authorize phones avoids the need to enter individual phones in a database, thus significantly reducing the effort needed to deploy IEEE 802.1X for phones.

ACS 5.x supports certificate attribute-based authorization for EAP-TLS. Note that as of release 5.1, only the certificate subject's attributes (listed above in the table above) can be used in an ACS 5.x authorization policy. The issuer's attributes cannot be used.*

*ACS 4.2 supports certificate-only authorization for EAP-FAST with the PAC-Free and PKI Authorization Bypass features.

If your AAA server does not support authorization based on certificate attributes alone, it will require an additional lookup, using the Common Name (CN) or other attribute in the certificate to query another database (internal or external) to gather sufficient information to authorize the

phone. Thus, the name of every phone will need to be entered into an internal or external database for validation.

Note: Certificate Revocation

There is currently no mechanism for certificate revocation for MICs and LSCs for Cisco IP Phones. If a phone's certificate becomes invalid or a phone is stolen, that phone can be removed from (or renamed in) CUCM to prevent it from gaining access to the call control resources in CUCM. Although the phone will not be able to register or make calls, the lack of a certificate revocation mechanism means that the phone will still be able to authenticate using IEEE 802.1X (since its certificate is still valid as far as the AAA server can determine). To keep the phone with an invalid certificate from gaining network access via IEEE 802.1X, use an exception policy in ACS 5 to specifically disallow that phone when it attempts to authenticate. See the ACS product documentation for more information on exception policies.

2.3.1.1.2 Passwords

The following Cisco IP Phones support authentication via username and password using the EAP-MD5 method of authentication:

Cisco IP Phone Model	Minimum firmware for password-based IEEE 802.1X using EAP-MD5
7906, 7911	7.2(3)
7931, 7937	7.2(3)
7941, 7942-G, 7945-G,	7.2(3)
7961, 7962-G, 7965-G,	7.2(3)
7970, 7971, 7975-G	7.2(3)

The username for a Cisco IP Phone follows the format CP-XXXXX-SEPYYYYYYYYYYYY, where XXXXX is the phone model (e.g. 7965G) and YYYYYYYYYYYY is the MAC address of the phone. This name is hardcoded and cannot be changed. The password is manually configured on the phone itself. There is no centralized mechanism to provision passwords on phones.

Note: Phones Have Long User Names

IP phones have 24 character usernames. Some AAA servers and backend directory servers (including Active Directory) have trouble with usernames that exceed 20 characters. Be sure that your AAA server can support the length of the hardcoded IP Phone name. ACS5 can support usernames up to 64 characters.

2.3.1.1.3 Enabling IEEE 802.1X On Phones

Out of the box, Cisco IP Phones are capable of IEEE 802.1X but they are not enabled for IEEE 802.1X. This was done to preserve backwards compatibility with older releases of code. While Cisco IP Phones can be enabled for IEEE 802.1X manually using the phone's keypad, the is not a scalable process when deploying large numbers of phones.

For scalability and ease of deployment, phones should be enabled for IEEE 802.1X via the network. Starting with CUCM 7.1.2, it is possible to enable IEEE 802.1X on phones by enabling IEEE 802.1X in the phone configuration file or via the Bulk Administration Tool on the CUCM. The next time the phone resets and downloads its configuration file, IEEE 802.1X will be enabled for all supported EAP methods.

Deployment Tip: Configure ACS to Request the Preferred EAP Method

There is no way to disable individual EAP methods on a Cisco IP Phone. Therefore, the phone will accept any EAP method that the ACS requests. So, for example, if ACS request EAP-MD5, the phone will accept that method, even if a password has not been configured. If a password was not configured, the phone will fail EAP-MD5 authentication, even if the phone has a valid certificate and is capable of EAP-FAST or EAP-TLS. To avoid this situation, configure the ACS to request only the preferred EAP method when authenticating a phone.

Obviously, enabling IEEE 802.1X on phones via the network requires that the phones have network access in the first place. This means that you should enable the phones for IEEE 802.1X before you enable identity-based access control on the switches.

Best Practice Recommendation: Enable IEEE 802.1X on Phones First

IP Phones that have IEEE 802.1X disabled are subject to a classic chicken-and-egg dilemma when connecting to network that is enabled for IEEE 802.1X-based access control. The phones need access to the network to enable IEEE 802.1X, but they can’t get access without first doing IEEE 802.1X.

While enabling IEEE 802.1X on phones first is a best practice, it may not always be possible, particularly when adding new phones to a network that has previously been enabled for IEEE 802.1X. In those situations, you have several options:

1. Bring up new phones in a physically secure staging area where the access ports are not enabled for IEEE 802.1X. This will allow the phones to access the network and download the needed configuration files.
2. Manually enable IEEE 802.1X on each phone using the keypad. While not practical for initial deployments of large numbers of phones, it may work for small numbers of phones.
3. Authenticate the phone using MAB to give the phone enough access to the network to download its configuration file.
4. Use a Low Impact deployment scenario to allow the phone enough access to the network prior to IEEE 802.1X authentication. Low Impact mode allows you to deploy IEEE 802.1X on access ports with selectively open access (as specified by a port ACL) prior to authentication. For more information on Low Impact Mode, see Section 2.3.20.2.

2.3.2 MAC Authentication Bypass (MAB)

MAB enables a Cisco Catalyst switch to check the connecting device's MAC address in lieu of a successful IEEE 802.1X authentication. MAB is attempted when IEEE 802.1X times out (by default) or fails (if configured). When MDA is enabled, both the phone and the device behind the phone can authenticate using MAB.

The following table lists Cisco IP Phones that do not support IEEE 802.1X and thus should be authenticated using MAB:

Cisco IP Phone Model	Support For IEEE 802.1X
7902, 7905	No
7910, 7912, 7920	No
7935, 7936	No
7940	No
7960	No

When deploying MAB for phones that cannot perform IEEE 802.1X, there are two main issues to consider: network access timing and MAC databases.

Network Access Timing

Like any device that uses MAB to get access to the network, phones will be subject to delays in network access. The switch will first attempt IEEE 802.1X as soon as link goes up. By default, the switch sends three EAP messages (30 seconds apart) before MAB is attempted. This adds a 90 second delay before network access is allowed. To give non-IEEE-802.1X phones faster access, you will have three options: adjust the default timers, use FlexAuth to configure the port to attempt MAB before IEEE 802.1X or use a deployment scenario (such as Low Impact Mode) that allows some network access prior to authentication.

MAC Databases

The other major consideration for deploying MAB for IP Phones is how to create and maintain a MAC database that the AAA server can reference when validating the MAC address of the phone.

The quickest way to create a MAB database for an existing Cisco IP Phone deployment is to export the MAC addresses of all registered non-IEEE-802.1X-capable phones from CUCM and import them into your AAA server or an identity store (such as an LDAP directory) that your AAA server can query. Both CUCM and ACS provide GUI support for exporting and importing MAC addresses.

A second option for creating a MAC database is to use a tool such as the NAC Profiler to discover and classify devices on your network. Before deploying IEEE 802.1X on your network, you could run NAC Profiler for a period of time. Using DHCP fingerprinting and other sources of information, NAC Profiler can determine which MAC addresses on your network are likely to be phones. After IEEE 802.1X has been deployed, NAC Profiler can act as an LDAP directory which can be queried from the AAA server to validate phone MAC addresses. Note, however, that NAC Profiler can only tell you what MACs are likely to belong to phones. It cannot tell you which phones are valid corporate assets. If this is a necessary distinction for your security policy, some sort of manual process (such as exporting phone MACs from CUCM) is required.

Another possible option for 3rd party phones is to use MAC wildcarding. When assigning MAC addresses to devices, vendors set the first three octets to a specific value called the

Organizationally Unique Identifier (OUI). OUIs are assigned by the IEEE, and uniquely identify the manufacturer of a given device. If a phone vendor has an OUI (or set of OUIs) that is exclusively assigned to IP Phones, then it is possible to create a wildcard rule in your AAA server policy that allows any device presenting a MAC address beginning with that OUI to be authenticated and authorized into the voice domain. ACS v5 supports OUI wildcarding through the use of authorization rules, but not all AAA servers do. Also be aware that Cisco IP Phones cannot support OUI wildcarding since Cisco uses many OUIs for its products, none of which are used exclusively for IP Phones.

Once a database has been created, it will need to be maintained as phones are added to or removed from the network. The simplest and most direct way to accomplish this is by manually adding or removing the MAC address from the AAA server or external MAC database. The effort involved in creating and maintaining a MAC database is one reason you should enable IEEE 802.1X on every device in your network that supports it.

2.3.3 WebAuth

WebAuth enables a Cisco Catalyst switch to check the a user's credentials submitted through a web login portal on the switch. WebAuth is supported with IP Telephony deployments with a few important design considerations discussed below.

First, when MDA is enabled, only the device behind the phone can authenticate using WebAuth. Cisco IP Phones cannot be authenticated using WebAuth.

Second, Cisco's implementation of WebAuth on Catalyst switches utilizes access-lists (ACLs) to control access. Before WebAuth succeeds, access is controlled by a port ACL. The port ACL can be applied dynamically (as part of a WebAuth fallback profile configured on the switch) when 802.1X or MAB times out or fails or it can simply be configured statically on the port. However, if IP Telephony is enabled, only the latter method (statically configured port ACL) is supported. After WebAuth succeeds, access is controlled by a dynamic ACL that is downloaded from the ACS. Through the use of source substitution, a Cisco Catalyst switch can ensure that this ACL only allows traffic from the authenticated device in the data domain. However, like the port ACL, the dynamic ACL applies to the entire port (both domains). Therefore, to ensure that voice traffic is permitted, it is essential that the phone downloads its own ACL as part of its authorization process in the voice domain.

Third, the only way to clear a WebAuth session behind a phone is using CDP Enhancement for Second Port Disconnect. As discussed in section 2.2.4, inactivity timers cannot be currently be used to clear WebAuth session behind phones. Since the CDP Enhancement feature is currently supported on Cisco phones and switches only, third party phones cannot be used with WebAuth.

Note: WebAuth Is Not Supported Behind Third Party Phones

Because third party phones have no way to communicate second port status to the switch, WebAuth sessions behind third party phones will not be cleared correctly. Since dangling sessions behind phones can lead to security violations and security holes, this is not a viable deployment option.

2.3.4 Guest VLAN

If an IEEE 802.1x authentication times out while waiting for an EAPOL message exchange and MAB (if configured) fails, the switch can be configured to assign the client to a guest VLAN that provides limited services. However, when MDA is deployed, the Guest VLAN is only supported for devices in the data domain. Phones that inadvertently get assigned to the guest VLAN because of a failed MAB authentication will not function properly (since they will not have access to the voice VLAN) and may cause security violation if there is already an authenticated device in the data domain.

2.3.5 Auth-Fail VLAN

If an IEEE 802.1x authentication fails, the switch can be configured to assign the client to an Auth-Fail VLAN that provides limited services. However, when MDA is deployed, the Auth-Fail VLAN is only supported for devices in the data domain. Phones that inadvertently get assigned to the Auth-Fail VLAN because of a failed IEEE 802.1X authentication will not function properly (since they will not have access to the voice VLAN) and may cause security violation if there is already an authenticated device in the data domain.

2.3.6 Inaccessible-Auth Bypass

If an IEEE 802.1x authentication fails because the AAA server is unavailable, the switch can be configured to allow clients access to a special VLAN (sometimes called the “Critical VLAN”) that provides configurable access to the network. The Critical VLAN can be any VLAN except for the voice VLAN.

When MDA is deployed, Inaccessible-Auth Bypass is fully supported for the data domain. The operational impact of this feature on IP Phones depends on the authorization state of the voice domain when the failure occurs.

- If a phone has previously authenticated and re-authentication occurs after the AAA server has become unreachable, the switch puts the critical port in the critical-authentication state in the current VLAN (either the statically configured voice VLAN or a dynamically assigned voice VLAN from the AAA server). IP connectivity will not be disrupted for previously authenticated phones.
- If a phone plugs into the port when the AAA server is down, the switch will put the port in the critical VLAN. Phones that get assigned to the critical VLAN will not function properly (since they will not have access to the voice VLAN). Because the switch relies on the device-traffic-class=voice VSA that only the AAA server can provide, the switch has no way to authorize a phone into the voice domain if the AAA server is down.

While there is no concept of Inaccessible Auth Bypass for phones today, it is important to remember that wired phones are typically static devices. Therefore, most wired phones will be properly authenticated when the AAA server is up and stay authenticated when the AAA server is unavailable. Only phones that connect to the network when the AAA server is down will be affected. Since this would be a rare occurrence, the current behavior of Inaccessible-Auth Bypass is usually not a significant operational issue for IP telephony deployments

2.3.7 Dynamic ACL Assignment

IP Telephony is compatible with ACLs that are dynamically assigned by the AAA server as the result of a successful authentication. Dynamic ACLs are applied to the entire port (voice and data domains) but the switch dynamically substitutes the source address of the authenticated client to be sure that the ACL only permits and denies traffic from the authenticated device. To prevent

ACLs in one domain from adversely impacting the other domain, if an ACL is assigned for a device in the data domain, then an ACL must also be assigned to IP phones in the voice domain (and vice versa).

2.3.8 Dynamic VLAN Assignment

IP telephony is fully compatible with VLANs that are dynamically assigned by the AAA server as the result of a successful authentication. Both the data and the voice VLAN can be dynamically assigned. In the current release of code, a static voice VLAN must be configured on the port (via the switchport access voice vlan) command before a new VLAN can be assigned via RADIUS.

Note: Third Party Phones And Dynamic VLAN Assignment

Before dynamically assigning VLANs to phones, ensure that your phone has a mechanism whereby it can learn the new voice VLAN. Cisco IP Phones learn the dynamic VLAN from CDP (which the switch sends as soon as the new voice VLAN is assigned) and immediately begin tagging voice traffic with the new VLAN. Some third party phones can use LLDP to learn the voice VLAN in the same way. For phones that use some mechanism other than CDP or LLDP, it will be necessary to have some other process to synchronize the VLAN assigned by RADIUS with the VLAN that the phone is configured to use.

2.3.9 Re-authentication

IP Telephony is compatible with re-authentication. The phone and/or the device behind the phone can be independently re-authenticated at statically configured intervals on the switch or at dynamically RADIUS-assigned intervals. However, re-authentication is not typically recommended for IP Phones for the following reasons:

1. **Re-authentication Is Not Always Necessary:** Since IEEE 802.1X is a port-based authentication technique, the physical status of the port directly impacts how long the authenticated session remains active. After a successful IEEE 802.1X (or MAB) authentication, the port remains open until the switch detects a physical link-down event or receives an explicit logoff notification. Any device attempting to connect to the port after a link-down or a logoff will be required to authenticate again. In the absence of link-down/logoff events, there is usually no need to re-authenticate a previously authenticated phone that remains connected to the network. Since phones are directly connected to the network and physical connectivity is continuously maintained, there is no question that an authenticated phone remains connected to the port. Under these circumstances, periodically re-interrogating the phone's credentials would serve no purpose.
2. **Re-Authentication Adds Load to the AAA server:** Each re-authentication adds to the load on the AAA server.
3. **Limitations of Switch-based Re-Authentication:** If re-authentication is locally configured on the switch, the switch will not re-learn the MAC address of a MAB-authenticated device when the re-authentication timer expires. Instead, the switch will simply send the previously-learned MAC address to the AAA server again. This is essentially a no-op. In addition, switch-based re-authentication applies to all IEEE 802.1X and MAB sessions, so it cannot be selectively enabled for certain devices.
4. **Limitations of Server-based Re-Authentication:** The AAA server can force the switch to re-learn the MAC address of the connected MAB device during re-authentication by sending the Termination-Action RADIUS Attribute (Attribute [29]) set to "Default." However, this setting causes the switch to terminate the existing session and restart IEEE 802.1X, so the phone will lose network connectivity until IEEE 802.1X times out and MAB is re-attempted. Setting the Termination-Action Attribute to "RADIUS-Request" will cause the switch to send the

previously-learned MAC address to the AAA server without impacting the network connectivity of the phone (again, a no-op).

Re-authentication may have some value for devices in the data domain. Since the data device is connected to the port via the IP phone, the switch might not have direct knowledge of link-down events. During re-authentication, the switch sends an EAP-Request to the host to initiate a new IEEE 802.1X authentication session, thus providing a mechanism by which the switch can confirm that the authenticated host is still connected. However, as discussed in Section 2.2.4, the CDP Enhancement for Second Port Disconnect provides a more direct way to solve this problem.

Best Practice Recommendation: Use Re-Authentication Selectively, If At All

Because low impact mode allows limited access to the voice VLAN prior to authentication, it can be used to bootstrap phones onto the network.

If re-authentication is desired for data devices, use server-based re-authentication. One benefit of server-based re-authentication is that it can be used selectively. The server can send down different values for the session timeout for different classes of devices or send no values at all (effectively disabling re-authentication for that session). Server-based re-authentication allows you to enable re-authentication for some devices (e.g. laptops) while not enabling it for others. If continuous network connectivity is important, set the Termination-Action Attribute to "RADIUS-Request" and set the Session-Timeout RADIUS Attribute (Attribute [27]) to the desired length of the re-authentication. To disable re-authentication for a device (e.g. a phone), configure the AAA server to not send either Attribute 27 or Attribute 29 for that session.

2.3.10 Wake on Lan

IP Telephony is compatible with the Wake on Lan (WoL) feature for IEEE 802.1X. The WoL feature allows dormant PCs to be powered when the switch receives a specific Ethernet frame, known as the magic packet. You can use this feature in environments where administrators need to connect to systems that have been powered down.

2.3.11 Open Access

IP Telephony is compatible with the open-access feature.

By default, IEEE 802.1X drops all traffic prior to a successful IEEE 802.1X (or MAB) authentication or WebAuth initialization. This is sometimes referred to as closed mode. Cisco switches can be configured for open-access mode, which allows all traffic (in both the data and voice VLANs) prior to successful authentication (subject to any ACL configured on the port). Open-access mode is a key component of the Monitor Mode and Low Impact Mode Deployment Scenarios. For more information on these deployment scenarios, see Section 2.3.20."

2.3.12 Host Modes

The host mode on a port determines the number and type of devices allowed on a port. As discussed earlier, the current best practice for IP Telephony is to use Multi-domain Authentication host mode. For completeness' sake, the other host modes are discussed below. Note that, with the exception of multi-auth mode, all other host modes are not recommended for IP Telephony.

2.3.12.1 Single-Host Mode

In single-host mode, only a single MAC or IP address can be authenticated on a port. If a different MAC address is detected on the port after a host has authenticated, then a security violation will be triggered on the port. Cisco IP phones are the sole exception to this rule.

When a Cisco IP Phone is plugged into a port that is configured with a Voice VLAN and single-host mode, the phone will be silently allowed onto the network by way of a feature known as CDP Bypass. The phone (or any device) that sends the appropriate TLVs in a CDP message will be allowed access to the voice VLAN. CDP Bypass is a legacy feature that has been deprecated in favor of MDA for the following reasons:

- Lack of Visibility: Phones are effectively invisible since they access the network without generating any kind of accounting record or syslog
- Lack of Access Control: Since the phones are not authenticated, their identity is not validated prior to allowing access. Anyone who can spoof CDP can access the voice network.
- Lack of Authorization: Without an authentication event, the phone cannot be authorized with a dynamic ACL or dynamic VLAN.
- Incompatibility: CDP Bypass cannot be used with WebAuth or dynamic ACL assignment for data devices.
- No support for 3rd party phones: CDP Bypass only works with Cisco phones.
- Not supported across all switch platforms: The 3560e and 3750e platforms do not support CDP Bypass.

2.3.12.2 Multi-Domain Authentication (MDA) Host Mode

MDA is the recommended host mode for IP Telephony deployments.

2.3.12.3 Multi-Auth Host Mode

Multi-auth host mode is essentially a superset of MDA. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain (MDA only allowed a single device in the data domain).

Multi-auth is supported for IP Telephony deployments when more than one data device needs to authenticate behind a phone. A common use case for multi-auth behind a phone would be a virtualized device with multiple host OS's. Note, however, that multiple data devices (whether virtualized devices or physical devices connected to a hub) behind a phone can exacerbate the link-state awareness issue discussed in Section 2.2.4.

2.3.12.4 Multihost Mode

Multi-host mode is not recommended for IP telephony.

2.3.13 RADIUS Accounting

RADIUS Accounting is supported for IP Telephony deployments. Cisco recommends enabling accounting to ensure maximum visibility for all endpoints, voice and data, in the network.

2.3.14 AutoQoS

AutoQoS for VoIP is compatible with an IEEE 802.1X-enabled network.

2.3.15 Auto Smart Ports

AutoSmart Ports is not recommended when deploying VoIP in an IEEE 802.1X-enabled network.

2.3.16 Port Security

In general, Cisco does not recommend enabling port security when IEEE 802.1X is also enabled. Therefore, port security is not a recommended best practice when deploying IP Telephony in an IEEE 802.1X-enabled network.

2.3.17 DHCP Snooping

DHCP snooping is fully compatible with IP Telephony and should be enabled as a best practice.

2.3.18 Dynamic ARP Inspection

Dynamic ARP Inspection is fully compatible with IP Telephony and should be enabled as a best practice.

2.3.19 IP Source Guard

IP Source Guard is fully compatible with IP Telephony.

2.3.20 Deployment Scenarios

When deploying IEEE 802.1X, Cisco recommends a phased deployment model that gradually deploys identity-based access control to the network. The three scenarios for phased deployment are monitor mode, low-impact mode, and high-security mode. The interaction of IP Telephony with each scenario is described in the following sections.

For more information about scenario-based deployments, see http://www.cisco.com/go/ibns.

2.3.20.1 Monitor Mode

IP Telephony is fully supported in monitor mode.

The primary goal of monitor mode is to enable authentication without imposing any form of access control. This approach allows network administrators to see who is on the network and prepare for access control in a later phase without affecting end users in any way.

To get the most value out of monitor mode, fully configure your phones and backend databases to the fullest extent possible. Enable IEEE 802.1X on the phones that support it, and create the most up-to-date MAC database possible. Although authorization (such as VLAN assignment and ACL assignment) is typically not done in Monitor Mode, go ahead and enable authorization on the switch and create an authorization policy on the AAA server that sends the device-traffic-class=voice VSA for phones. This way, known phones will be correctly identified and assigned to the voice domain, allowing you to discover phones that can’t authenticate and phones that can authenticate but are not properly authorized into the voice domain. Since you are in monitor mode, you can identify and fix authentication and authorization problems without impacting the operation of the phone.

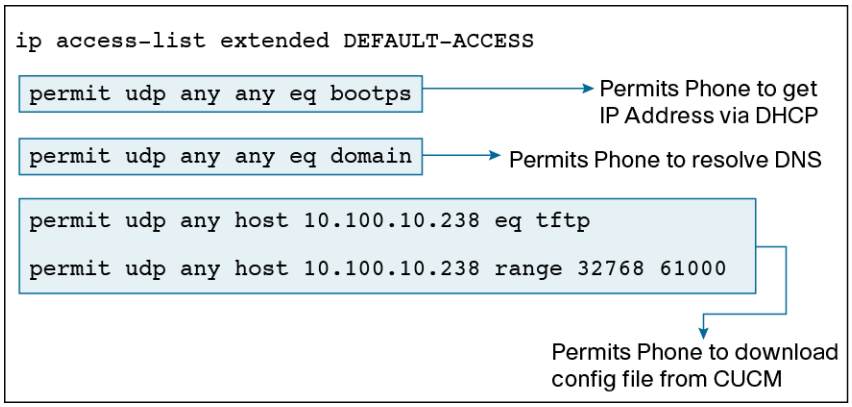
When enabling monitor mode in an IP Telephony environment, the host mode should be set to Multi-Auth Host Mode. This prevents security violations even if the ACS server does not return the device-traffic-class=voice VSA for the phone.

2.3.20.2 Low-Impact Mode

IP Telephony is fully supported in low impact mode. Low impact mode can also solve specific deployment challenges for IP Telephony.

Low impact mode builds on the idea of monitor mode, gradually introducing access control in a completely configurable manner. Instead of deny all access before authentication (as a traditional IEEE 802.1X deployment would require), low impact mode allows you to use ACLs to selectively allow traffic before authentication. This is particularly useful to devices that can't perform IEEE 802.1X and rely on MAB to get access to the network (such as older generation IP Phones). Waiting until IEEE 802.1X times out and falls back to MAB can have a negative impact on the boot process of these devices. Low impact mode enables you to permit time-sensitive traffic prior to authentication, enabling these devices to function effectively in an IEEE 802.1X-enabled environment.

As an example of low impact mode's effectiveness, consider the chicken-and-egg dilemma discussed in Section 2.3.1.1.3. Out of the box, new Cisco IP phones need access to the network to enable IEEE 802.1X, but they can't get access without first doing IEEE 802.1X. Using low impact mode, you could selectively allow the traffic that the phone needs to contact the call manager and download a config file that enables IEEE 802.1X. Consider the sample ACL below.



Applied to a port in low impact mode, this ACL would allow the phone to get an IP address, resolve the hostname of its Call Manager, and download a config file and firmware load, all prior to authentication. Note, however, that the phone would not be able to place calls, since the ACL only allows DNS, DHCP and TFTP. After IEEE 802.1X was enabled on the phone via the config file, the phone would automatically authenticate. As part of the phone's authorization policy, the switch could be instructed to apply a dynamic ACL such as "permit ip any any" to the phone's port. The successfully authenticated phone would now be fully operational. Low impact mode has effectively enabled the phone to bootstrap itself onto the IEEE 802.1X-enabled network.

Best Practice Recommendation: Use Low Impact Mode to Bootstrap Phones

Because low impact mode allows some access to authentication, it can be used to bootstrap phones and other devices onto the network.

2.3.20.3 High-Security Mode

IP Telephony is fully supported in High Security Mode.

High security mode is a more traditional deployment model for IEEE 802.1X which denies all access prior to authentication. It also facilitates VLAN assignment for the data and voice domains. The primary design consideration for IP Phones in high security mode is the lack of immediate network access for non-IEEE-802.1X devices. Phones that were not capable of or not enabled for IEEE 802.1X would have to wait for IEEE 802.1X to timeout and fallback to MAB before they get access to the network. It may be necessary to adjust the default timeout (90 seconds) to ensure that phones and other non-IEEE-802.1X devices get network access in a timely fashion. The actual value of the timer will depend on the sensitivity of your phones to delays in network access. You should always test your timer values prior to making large scale changes.

2.4 Deployment Summary for IP Telephony

Table 3 summarizes the major design decisions that need to be addressed prior to deploying IP Telephony in an IEEE 802.1X-environment.

Table 3. IP Telephony Deployment Reference

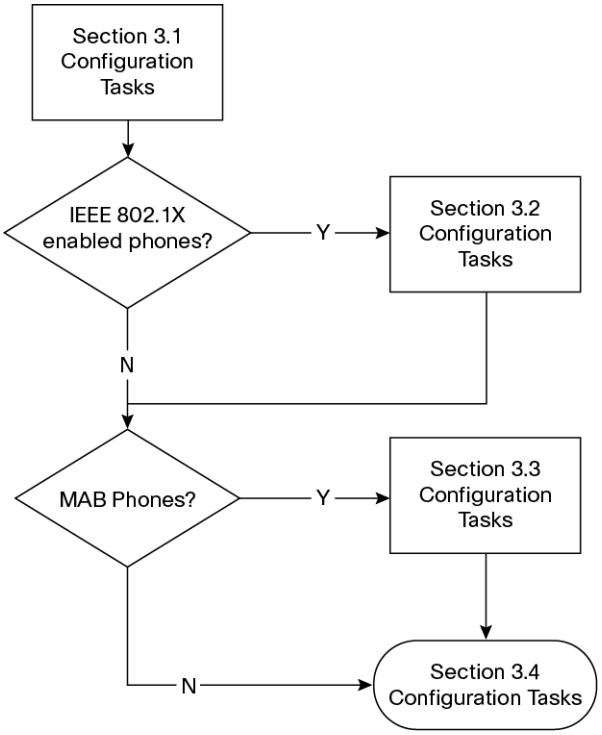
Design Consideration	Relevant Section
Use multi-domain authentication host mode to support IP Telephony in an IEEE 802.1X-enabled network.	2.2
Supplicants on data devices behind IP Phones should be configured to send EAPoL-Starts.	2.2.2
Address the lack of direct link-state knowledge for the device behind the phone using CDP Enhancement for Second Port Disconnect (recommended) or a combination of Proxy-EAPoL-Logoff and (server-based) Inactivity Timers.	2.2.4
Use IEEE 802.1X to authenticate your phones if your phones support it. Otherwise, use MAB.	2.3.1
Use CUCM 7.1.2 or higher to enable phones for IEEE 802.1X over the network.	2.3.1.1.3
For IEEE-802.1X-enabled-Cisco IP Phones, use EAP-FAST for ACS 4.2 or EAP-TLS for ACS 5.0.	2.3.1.1.1
For IEEE-802.1X-enabled-Cisco IP Phones, use LSCs for IEEE 802.1X authentication.	2.3.1.1.1
Use Monitor Mode in the initial phase of your deployment to assess the readiness of your voice and data endpoints.	2.3.15.1
Use Low Impact Mode to enable new IEEE-802.1X-capable-phones to perform IEEE 802.1X out of the box when access control has been enabled.	2.3.15.2
For non-IEEE-802.1X-capable phones, export MAC addresses from CUCM and import them into ACS to rapidly create a phone MAC database.	2.3.2
Only enable switch-based local WebAuth if you are using Cisco IP Phones that support CDP Enhancement for Second Port Disconnect.	2.3.3
Use server-based re-authentication to selectively enable re-authentication for data devices only. Do not enable re-authentication for IP Phones.	2.3.9
Use multi-auth host mode if you want to support multiple data devices plugging in behind a single phone.	2.3.12.3

3. Configuring IP Telephony

This section describes how to configure a system based on Cisco IOS Software for IEEE 802.1X with WebAuth fallback. The sample configurations given in this section highlight the following features:

- Section 3.1: Configuration tasks for ACS 5.1 (required for all phones)
- Section 3.2: Configuration tasks for IEEE 802.1X-capable phones
- Section 3.3: Configuration tasks for MAB phones
- Section 3.4: Configuration tasks for Catalyst switches (required for all phones)

The tasks described in sections 3.1 and Section 3.4 are required for all IP telephony deployments. In addition, you must also perform the tasks in Section 3.2 if you have IEEE 802.1X-capable phones and/or perform the tasks in Section 3.4 if you have phones that need to authenticate using MAB. The following flowchart represents the correct sequence of configuration tasks:



3.1 Configure ACS (All Phone Authentication Types)

The following sections describe two configuration tasks for ACS 5.1 that are required for all phone types: configuring a RADIUS client and configuring a Phone profile. Additional ACS configuration tasks that are specific to a certain authentication type (IEEE 802.1X or MAB) are covered in subsequent sections.

3.1.1 Configure the Switch as a RADIUS Client in ACS

In this section, the switch that will be authenticating phones is added as a AAA client in Cisco Secure ACS.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Network Resources** and select **Network Devices and AAA Clients**.
3. Click **Create**. The following window will appear:

4. Specify the name, IP address, and RADIUS shared secret for this switch. Optionally, add Description, Location, and Device Type information.

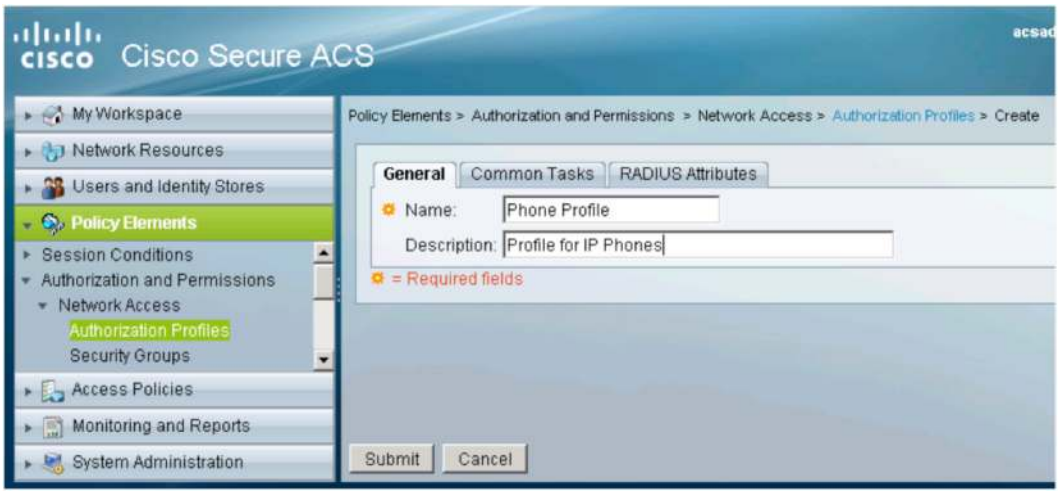
Note: The RADIUS shared secret must match the key configured on the switch. The IP address must match the IP address of the RADIUS source interface that the switch uses to source RADIUS packets for Cisco Secure ACS. See Section 3.4 for information about how to configure the key and the RADIUS source interface on the switch.

5. Click **Submit**.

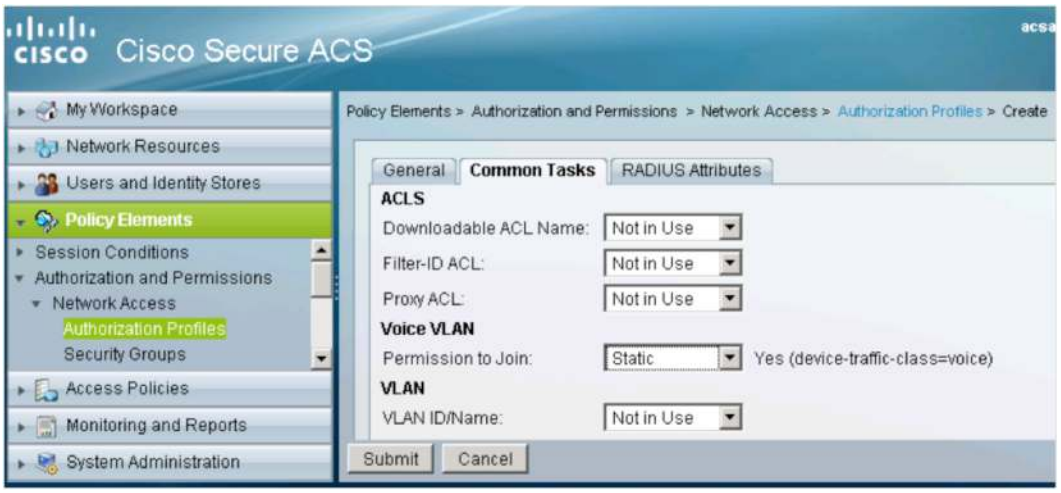
3.1.2 Create a Phone Authorization Profile in Cisco Secure ACS

In this section, an authorization profile is created in Cisco Secure ACS. This profile will be used in the authorization policy in a subsequent step.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, under **Policy Elements**, expand **Authorization and Permissions** and **Network Access**. Select **Authorization Profiles**.
3. Click **Create**. The following window will appear:



4. On the General tab, specify a name for this profile.
5. Click the **Common Tasks** tab. Under **Voice VLAN**, navigate to **Permission to Join**. Choose **Static**. This is the setting that will cause ACS to send the device-traffic-class=voice VSA to the switch when a phone authenticates.



6. Click **Submit**.

3.2 IEEE-802.1X Capable Phones

The following sections described the configuration steps for CUCM and ACS that are required to authenticate phones using IEEE 802.1X.

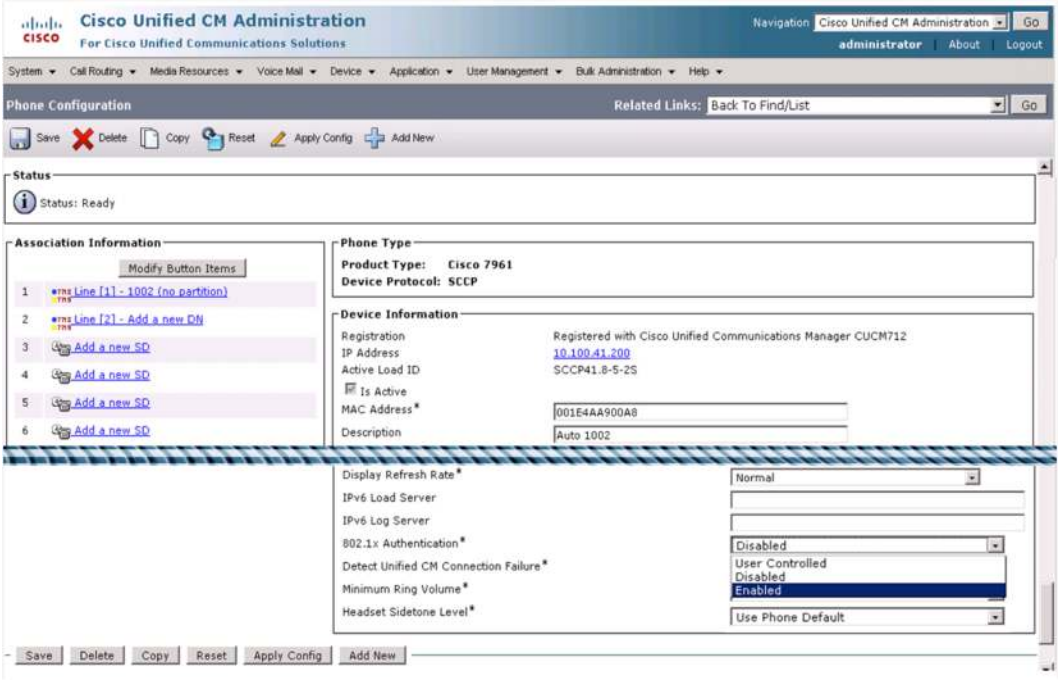
3.2.1 Enable Phones for IEEE 802.1X

In this section, the CUCM administrative interface is used to enabled a Cisco IP phone for IEEE 802.1X. This section is only required when using IEEE 802.1X-capable Cisco IP Phones.

Best Practice Recommendation: For Multiple Phones, Use BAT

For changing the IEEE 802.1X configuration on multiple phones, use the Bulk Administration Tool (BAT) inside CUCM.

1. In the Cisco Unified CM Administration user interface, choose **Device > Phone**.
2. The Find and List Phone window displays. Find and select the phone you wish to enable for IEEE 802.1X.
3. The Phone Configuration window appears.
4. Scroll down to the line titled “802.1x Authentication.” From the drop-down menu, select **Enabled**.



5. Click **Save** and then **Apply Config** to enable IEEE 802.1X on the phone.

3.2.2 Deploying LSCs

In this section, the CUCM administrative interface is used to install an LSC on an IP Phone. section is only required when using IEEE 802.1X-capable Cisco IP Phones.

Note: To deploy LSCs, CUCM first must be enabled for Certificate Authority Proxy Functionality (CAPF). Configuring CAPF is a multi-step process that is not covered in this document. For full details on how to deploy CAPF, see the Cisco Unified Communications Security Guide.

1. In the Cisco Unified CM Administration user interface, choose **Device > Phone**.
2. The Find and List Phone window displays. Find and select the phone to which a certificate should be deployed.
3. The Phone Configuration window appears.
4. Scroll down to the section entitled **Certificate Authority Proxy Function (CAPF) Information**.
5. Under **Certificate Operation**, select **Install/Upgrade**.
6. Under **Authentication Mode**, select **By Existing Certificate (precedence to LSC)**.
7. Under **Operation Completes By**, enter the date and time the certificate should be deployed.

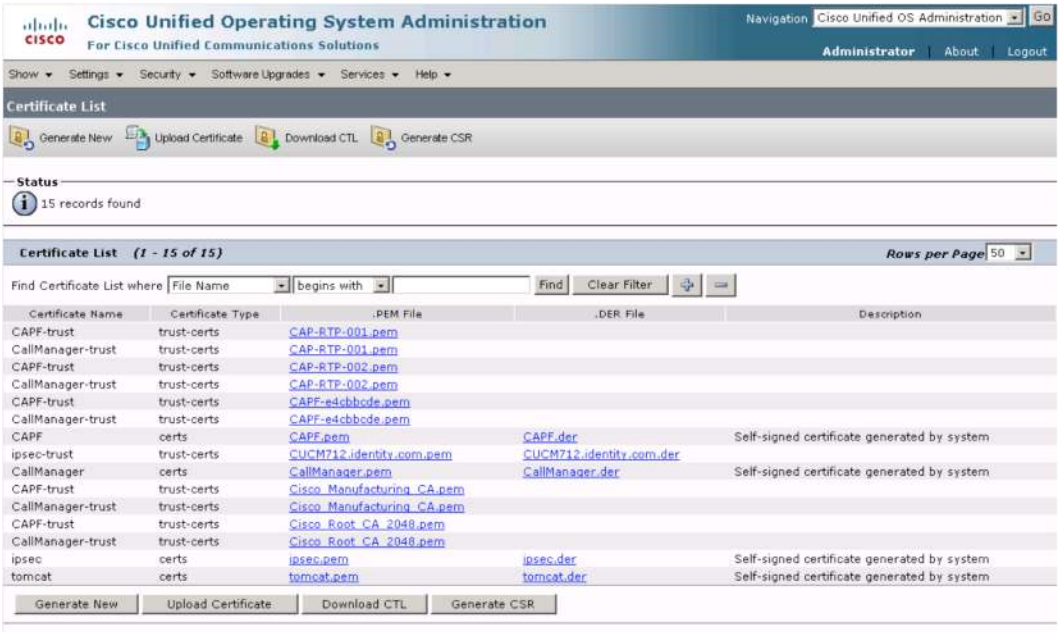
8. Click **Save** and then **Apply Config** to begin the process of enrolling a certificate for the phone.

3.2.3 Export CA Certs from CUCM

In this section, root Certificate Authority Certificates are exported from CUCM (to be imported into ACS in the next section). This section is only required when using IEEE 802.1X-capable Cisco IP Phones.

1. In the Cisco Unified Operating System Administration user interface, choose **Security > Certificate Management**.

2. Select **Find** to display all the certificates



3. For each required certificate, select the name of the certificate in .PEM format and then **Download**. When prompted, save the certificate.
4. Repeated for each required certificate.

> **Note:** If authenticating phones using MICs, the required certificates may include: Cisco_Root_CA_2048, Cisco_Manufacturing_CA, CAP-RTP-001, and CAP-RTP-002.
>
> If authenticating using LSCs, the required certificates will depend on your CAPF deployment. In the example above (using a self-signed CAPF), the required certificate is CAPF-e4cbbcde. The actual name of your CAPF CA will vary.

3.2.4 Import CA Certificates into ACS

In this section, the CA certificates that were exported from CUCM in the previous step are imported into ACS. This section is only required when using IEEE 802.1X-capable Cisco IP Phones.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation panel, select **Users and Identity Stores > Certificate Authorities**. The current list of trusted certificate authorities is displayed.

3. Select **Add**.
4. Enter the name of the certificate file that was exported in the previous step and check the box next to **Trust for client with EAP-TLS**. Optionally, enter a description for this certificate.

5. Click **Submit**.
6. Repeat for each of the certificates exported from the CUCM.

3.2.5 Configure an IEEE 802.1X Access Service

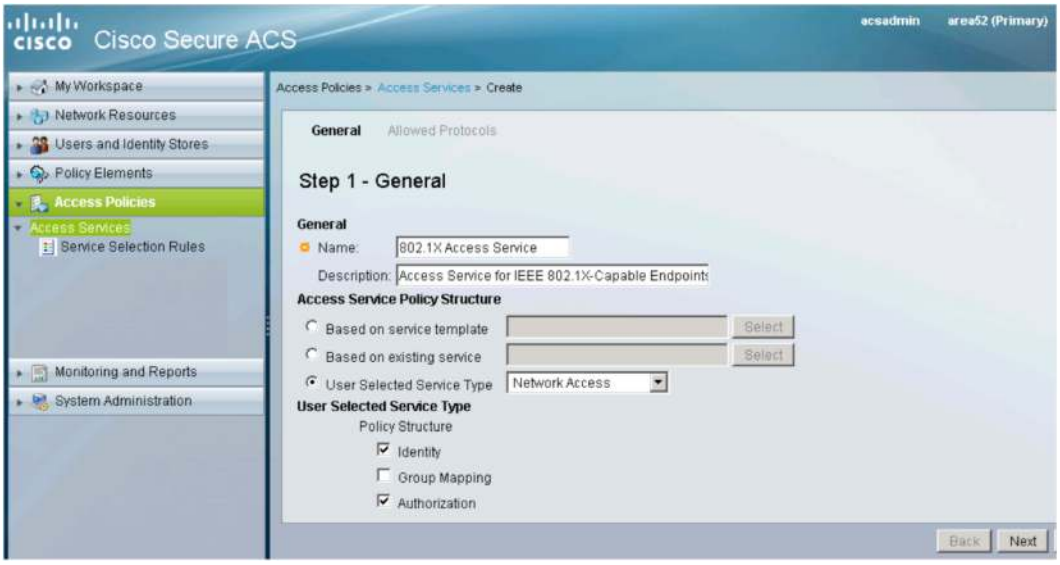
In this section, an IEEE 802.1X access service is created in Cisco Secure ACS. This access service will be used in the service selection rules in a subsequent step. The access service profile has four parts: the service name, the allowed protocol filter, the identity policy, and the authorization policy.

3.2.5.1 Create the IEEE 802.1X Access Service and Protocol Filter

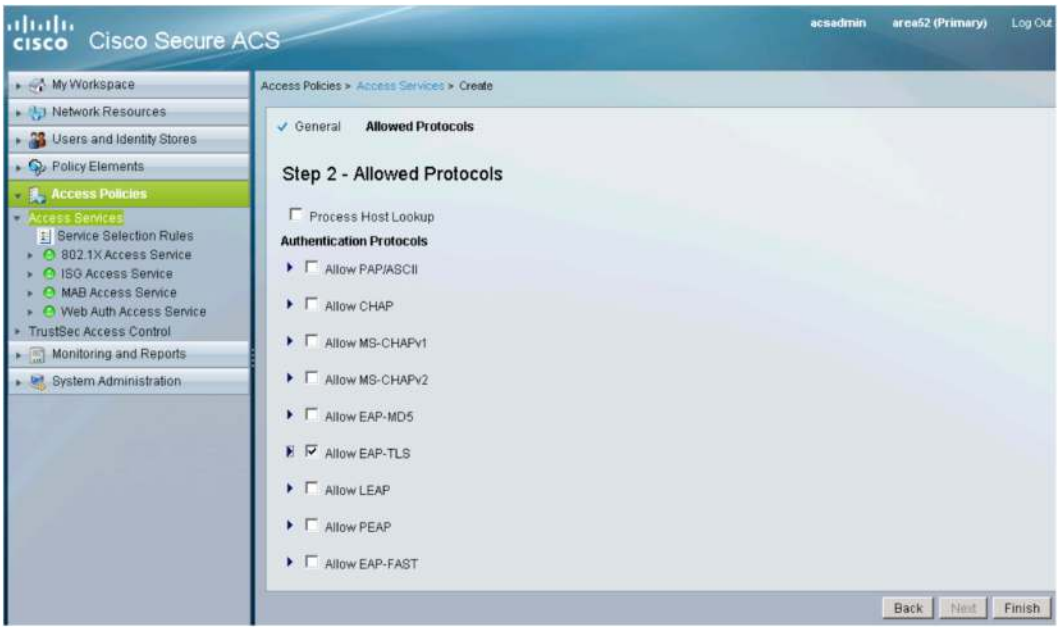
Open the Cisco Secure ACS Management interface.

In the left navigation column, under **Access Policies**, click **Access Services**. The list of existing access services will appear.

At the bottom of the right window pane, click **Create**. The following window will appear:



1. In **Step 1—General**, specify a name for this service. Under **Access Service Policy Structure**, select **User selected policy structure**. For **Access Service Type**, choose **Network Access**. Under **Policy Structure**, select **Identity and Authorization**. Click **Next**. The following window appears:



2. In **Step 2—Allowed Protocols**, deselect **Process Host Lookup**. Select **Allow EAP-TLS**. If other devices (e.g. laptops) use a different EAP method, select that method as well. Click **Finish**. You will be prompted to modify the service selection policy. Click **No**.

Note: ACS 5.1 will attempt EAP-TLS before less secure methods such as EAP-MD5. Earlier versions of ACS, however, may attempt EAP-MD5 first if it's enabled. Since the phone will attempt whatever method ACS requests (even if it doesn't have a password), do not enable EAP-MD5 in the access service that will be used by IP Phones. If necessary, create separate access services for IP Phones and EAP-MD5-devices and use service selection rules to ensure that the correct access service is assigned to each device. For more information on service selection rules, see the product documentation for ACS.

3.2.5.2 Configure IEEE 802.1X Identity Policy

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Access Policies > 802.1X Access Service** and click **Identity**. The following window appears:

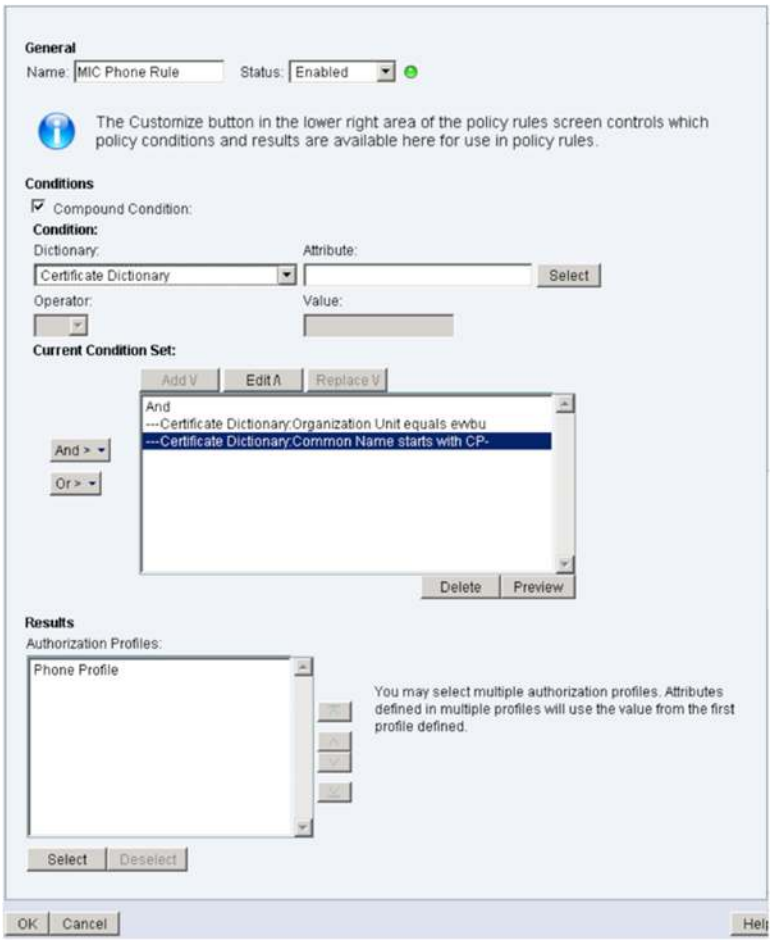
3. In the 802.1X Access Service Identity policy window, select **Select one result**. For **Identity Source**, choose **CN Username**. Click **Save Changes**.

Note: If you are using other EAP types that are not certificate based, you configure an Identity Store Sequence instead of CN Username so that ACS will check either the certificate or the password database as needed. See the ACS documentation for more information on Identity Store Sequences.

3.2.5.3 Create an LSC Authorization Rule

In this section, an Authorization rule for IP Phones with LSC is created. Omit this step if you are not authenticating IP Phones using LSCs.

1. Open the Cisco Secure ACS Management interface.
2. 2. In the left navigation column, expand **Access Policies** to list the access services. Expand **802.1X Access Service** and click **Authorization**. Click **Create**. The following window appears:



3. Specify a name for the LSC authorization rule. Select **Compound Condition**.
4. Under **Dictionary**, select **Certificate Dictionary**. Under **Attribute**, select **Organization Unit**. Under Operation select **starts with**. Under **Value**, enter the OU for your LSC. The actual value will depend on your CAPF configuration. In this example, the OU for this CAPF starts with “Cisco.” Click **Add V** to add the this condition to the Current Condition Set.

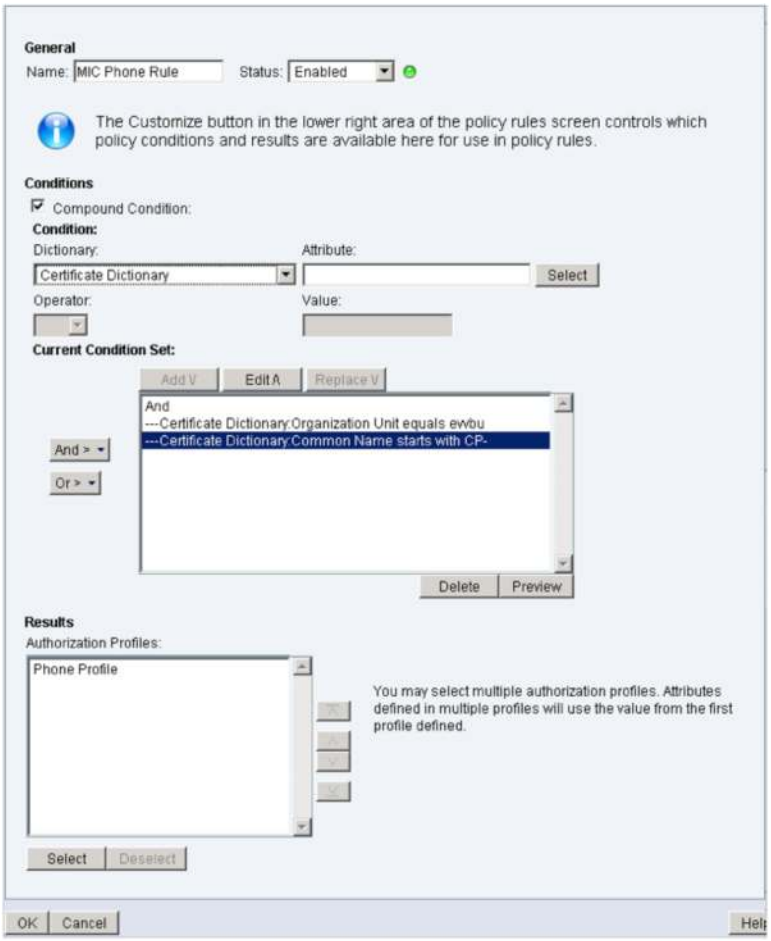
Note: If Compound Condition is not shown on this page, return to the 802.1X Access Service Authorization configuration page and select Customize to add Compound Condition to the set of allowed conditions.

5. Click **And >** to the left of the Current Condition Set.
6. Under **Dictionary**, select Certificate Dictionary. Under **Attribute**, select **Common Name**. Under **Operation** select **starts with**. Under **Value**, enter “SEP.” As discussed in section 2.3.1.1.1, the Common Name for Cisco IP Phones always begins with “SEP” for LSCs. Click **Add V** to add the this condition to the Current Condition Set.
7. Under Results, click **Select**. A list of all available authorization profiles is displayed. Select the Phone Profile that was created in section 3.7 and click **OK**.
8. Click **OK** to finish the LSC authorization rule.
9. Click **Save Changes**.

3.2.5.4 Create an MIC Authorization Rule

In this section, an Authorization rule for IP Phones with MIC is created. Omit this step if you are not authenticating IP Phones using MICs.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Access Policies** to list the access services. Expand **802.1X Access Service** and click **Authorization**. Click **Create**. The following window appears:



3. Specify a name for the MIC authorization rule. Select **Compound Condition**.
4. Under **Dictionary**, select **Certificate Dictionary**. Under **Attribute**, select **Organization Unit**. Under Operation select **equals**. Under **Value**, enter evvbu. Click **Add V** to add the this condition to the Current Condition Set.

Note: If Compound Condition is not shown on this page, return to the 802.1X Access Service Authorization configuration page and select Customize to add Compound Condition to the set of allowed conditions.

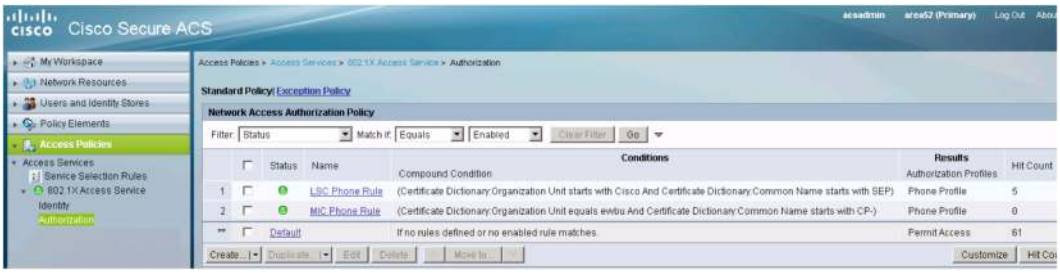
5. Click **And >** to the left of the Current Condition Set.
6. 6. Under **Dictionary**, select **Certificate Dictionary**. Under **Attribute**, select **Common Name**. Under Operation select starts with. Under **Value**, enter “CP-.” As discussed in section

2.3.1.1.1, the Common Name for Cisco IP Phones always begins with “CP-” for MICs. Click **Add V** to add the this condition to the Current Condition Set.

7. Under Results, click **Select**. A list of all available authorization profiles is displayed. Select the Phone Profile that was created in section 3.7 and click **OK**.
8. Click **OK** to finish the MIC authorization rule.
9. Click **Save Changes**.

3.2.5.5 Validate the IEEE 802.1X Phone Authorization Policy for ACS

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Access Policies** to list the access services. Expand **802.1X Access Service** and click **Authorization**. The following window will appear with a summary of the configured authorization rules.

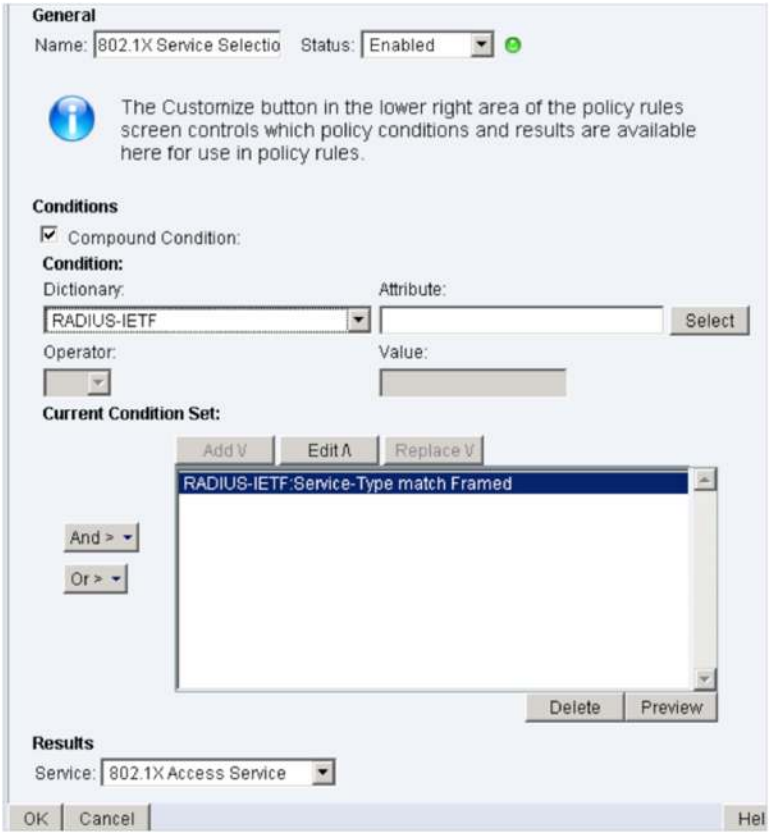


3. Verify that the LSC and/or MIC rules that you created have a Result of **Phone Profile**.
4. Verify that the Default rule at the bottom of the table has a Result of **Permit Access**. This is the rule that will be matched for data devices that authenticate using IEEE 802.1X.

3.2.6 Create an IEEE 802.1X Service Selection Rule

This section describes how to create a service selection rule for IEEE 802.1X in Cisco Secure ACS. This service selection rule ensures that the authorization policies defined in the IEEE 802.1X access service are applied to IP Phones.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, under **Access Policies**, click **Service Selection**. The list of existing service selection rules will appear.
3. At the bottom of the right window pane, click **Create**. The Service Selection rule dialog box will appear and should be filled out as described in the following steps:



4. Specify a name for the rule (802.1X Service Selection is used here).
5. Under **Conditions**, select **Compound Condition**.
6. Under **Dictionary**, choose **RADIUS-IETF**.
7. Under **Attribute**, select **Service-Type**.
8. Under **Operator**, choose **match**.
9. Under **Value**, select **Framed**.
10. Under **Current Condition Set**, click **Add**.
11. Under **Results**, select the access service that was created in the previous step (802.1X Access Service).
12. Click **OK**. The Service Selection rule summary will appear with the new rule:

13. Click **Save Changes**.

3.3 Non-IEEE-802.1X Capable Phones

The following sections described the configuration steps for CUCM and ACS that are required to authenticate phones using MAB.

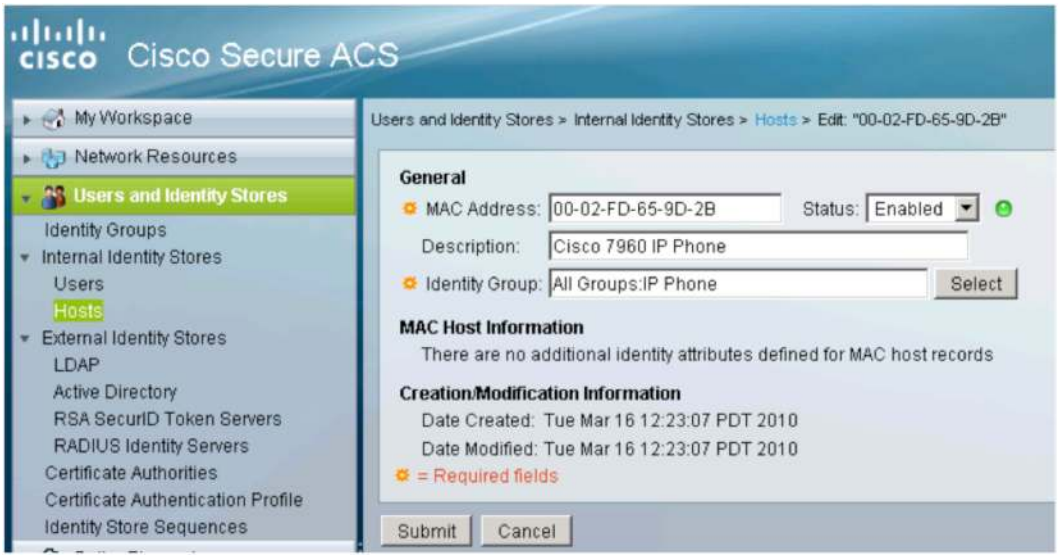
3.3.1 Enter Phone MAC Address in Cisco Secure ACS Internal Host Database

In this section, a phone MAC address is entered in the Cisco Secure ACS internal host database. This section is only required for non-IEEE 802.1X-capable Cisco IP Phones.

Best Practice Recommendation: For Multiple Phones, Use Import / Export Tools

To enter MAC addresses for multiple phones, use the export function in CUCM to extract the MAC addresses of registered IP Phones that are not IEEE 802.1X capable. Once exported, the MAC addresses can be formatted and entered into ACS using the import function.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, under **Users and Identity Stores**, expand **Internal Identity Stores** and select **Hosts**.
3. Click **Create**. The following window will appear:



4. Enter the phone's MAC address and assign it to an Identity Group that identifies this device as a phone.
5. Click **Submit**.

3.3.2 Configure an MAB Access Service

In this section, MAB access service is created in Cisco Secure ACS. This access service will be used in the service selection rules in a subsequent step. The access service profile has four parts: the service name, the allowed protocol filter, the identity policy, and the authorization policy.

3.3.2.1 Create the MAB Access Service and Protocol Filter

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, under **Access Policies**, click **Access Services**. The list of existing access services will appear.

3. At the bottom of the right window pane, click **Create**. The following window will appear:

4. In **Step 1—General**, specify a name for this service, and optionally, a description. Under **Access Service Policy Structure**, select **User selected policy structure**. For **Access Service Type**, choose **Network Access**. Under **Policy Structure**, select **Identity** and **Authorization**. Click **Next**. The following window appears:

5. In **Step 2—Allowed Protocols**, select **Process Host Lookup**. Click **Finish**. You will be prompted to modify the service selection policy. Click **No**.

3.3.2.2 Configure MAB Identity Policy

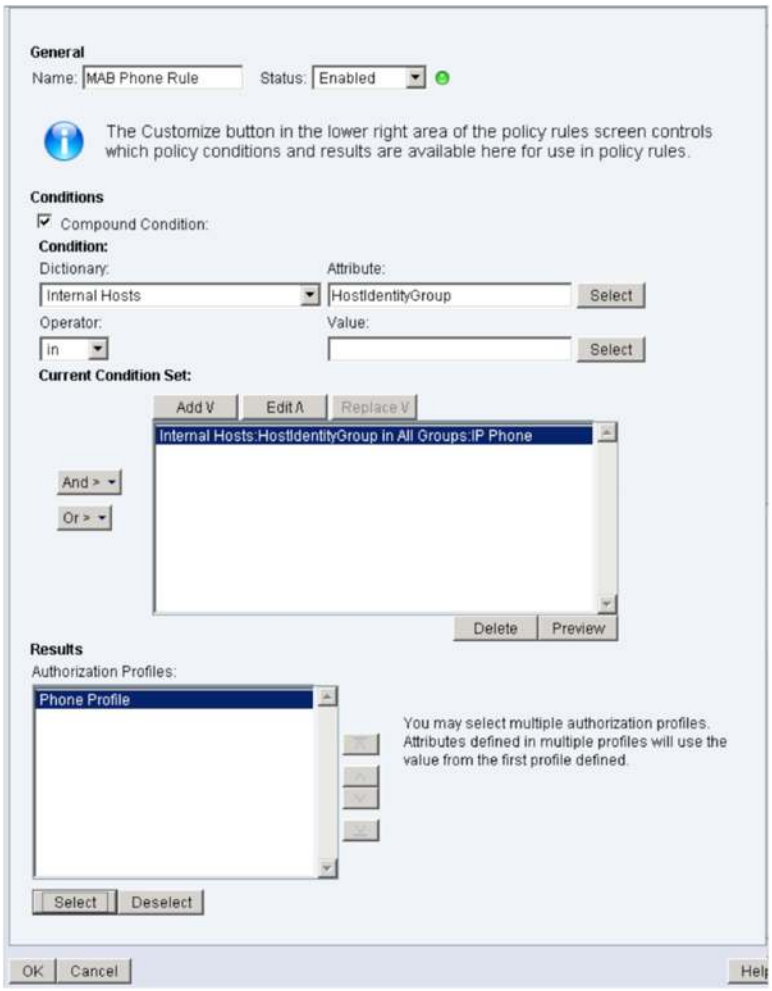
1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Access Policies > MAB Access Service** and click **Identity**. The following window appears:

3. In the 802.1X Access Service Identity policy window, select **Select one result**. For **Identity Source**, choose **Internal Hosts**. Click **Save Changes**.

3.3.2.3 Create Phone MAB Authorization Rule

In this section, an Authorization rule for MAB-Authenticated IP Phones is created. Omit this step if you are not authenticating IP Phones with MAB.

1. Open the Cisco Secure ACS Management interface.
2. 2. In the left navigation column, expand **Access Policies** to list the access services. Expand **MAB** and click **Authorization**. Click **Create**. The following window appears:



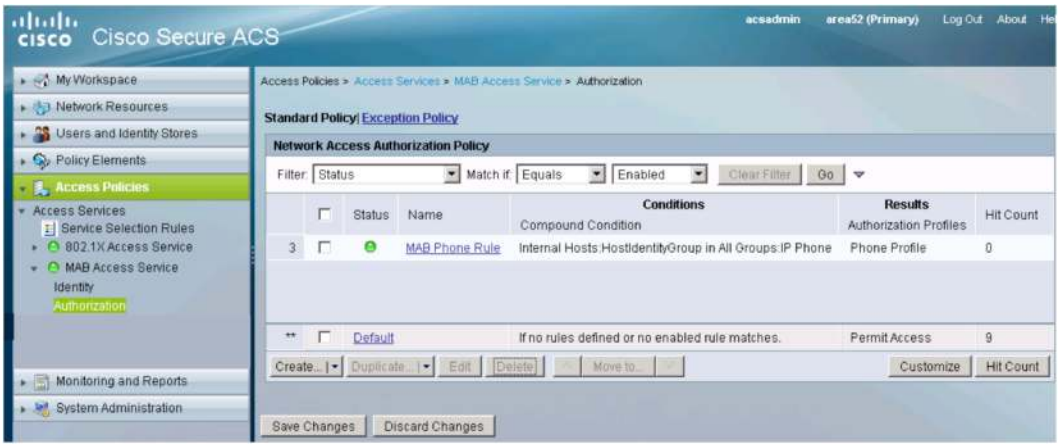
3. Specify a name for the MAB authorization rule. “MAB Phone Rule” is used here.
4. Select **Compound Condition**.
5. Under **Dictionary**, select **Internal Hosts**. Under **Attribute**, select **HostIdentityGroup**. Under **Operation** select **in**. Under **Value**, enter the Phone group name that was assigned to the phone MAC in the Internal Host database in Section 3.5. The group used in this document is “All Groups:IP Phone.” Click **Add V** to add the this condition to the Current Condition Set.

Note: If **Compound Condition** is not shown on this page, return to the MAB Access Service Authorization configuration page and select **Customize** to add Compound Condition to the set of allowed conditions.

6. Click **And >** to the left of the Current Condition Set.
7. Under **Results**, click **Select**. A list of all available authorization profiles is displayed. Select the Phone Profile that was created in section 3.7 and click **OK**.
8. Click **OK** to finish the MAB authorization rule.
9. Click **Save Changes**.

3.3.2.4 Validate the MAB Phone Authorization Policy for ACS

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, expand **Access Policies** to list the access services. Expand **MAB Access Service** and click **Authorization**. The following window will appear with a summary of the configured authorization rules.

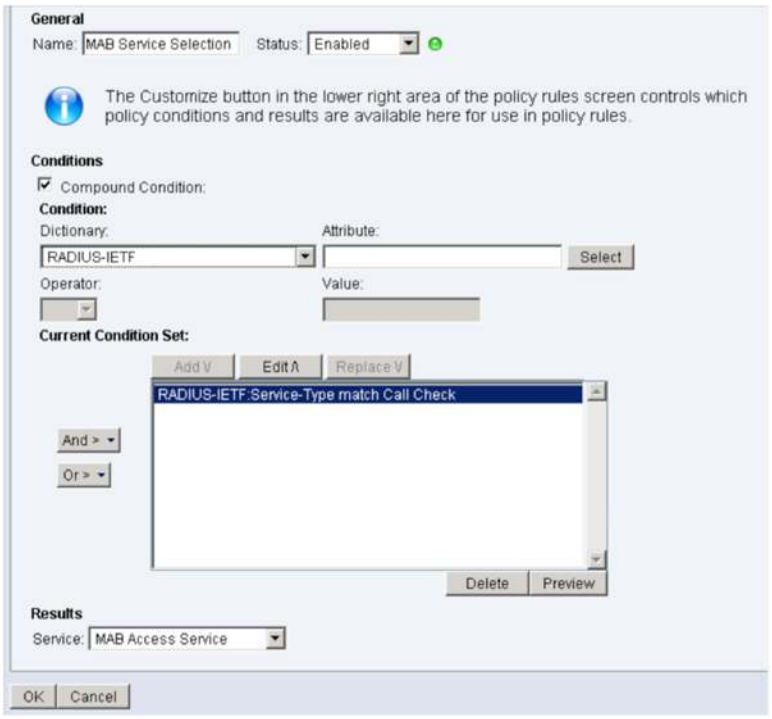


3. Verify that MAB Phone Rule that you created have a Result of **Phone Profile**.
4. Verify that the Default rule at the bottom of the table has a Result of **Permit Access**. This is the rule that will be matched for data devices that authenticate using MAB.

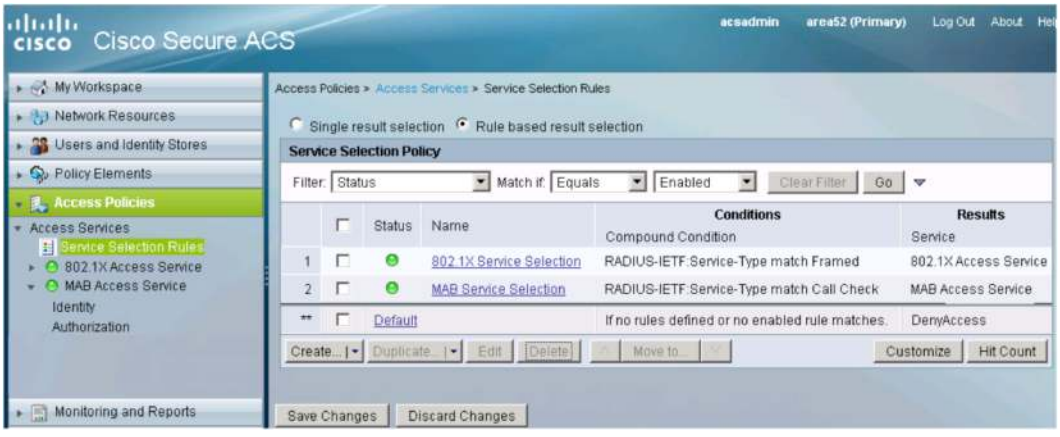
3.3.3 Create an MAB Service Selection Rule

This section describes how to create a service selection rule for MAB in Cisco Secure ACS. This service selection rule ensures that the authorization policies defined in the MAB access service are applied to IP Phones.

1. Open the Cisco Secure ACS Management interface.
2. In the left navigation column, under **Access Policies**, click **Service Selection**. The list of existing service selection rules will appear.
3. At the bottom of the right window pane, click **Create**. The Service Selection rule dialog box will appear and should be filled out as described in the following steps:



4. Specify a name for the rule (MAB Service Selection is used here).
5. Under **Conditions**, select **Compound Condition**.
6. Under **Dictionary**, choose **RADIUS-IETF**.
7. Under **Attribute**, select **Service-Type**.
8. Under **Operator**, choose **match**.
9. Under **Value**, select **Call Check**.
10. Under **Current Condition** Set, click **Add**.
11. Under **Results**, select the access service that was created in the previous step (MAB Access Service).
12. Click **OK**. The Service Selection rule summary will appear with the new rule:



13. Click **Save Changes**.

3.4 Configure Switch (All Phone Authentication Types)

In this section, the Cisco IOS Software switch is configured to support IP Telephony and IEEE 802.1X. Optional features and optimizations are also discussed.

3.4.1 Verify Existing Configuration

The configuration instructions in the following sections assume that the existing configuration on the switch contains the necessary elements to support IP telephony. A basic port configuration should minimally include an access VLAN and a voice VLAN. Other features that may be required by your security policy, such as spanning-tree portfast and bpduguard, may also be enabled. A working example is given below.

```
interface FastEthernet2/48
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 41
 spanning-tree portfast
 spanning-tree bpduguard enable
```

After validating that the IP Telephony infrastructure is fully operational, you can enable IEEE 802.1X.

3.4.2 IEEE 802.1X and MAB Configuration for IP Telephony

A basic configuration of IEEE 802.1X and MAB includes global AAA settings, global RADIUS settings, global IEEE 802.1X settings, and interface IEEE 802.1X settings. These settings are summarized in Table 4. An example of a working configuration appears at the end of this section.

Table 4. Cisco IOS Software IEEE 802.1X Configuration

Cisco IOS Software AAA Settings for IEEE 802.1X and MAB	
aaa new-model	Enables the AAA control model
aaa authentication dot1x default group {radius | *group-name*}	Specifies the authentication method for IEEE 802.1X • **radius**: Uses the list of all RADIUS servers configured with the **radius-server host** command • ***group-name*:** Uses a subset of RADIUS servers as defined by the **aaa group server radius** *group-name* argument
aaa authorization network default group {radius | *group-name*}	Specifies the authorization method for IEEE 802.1X; this command allows the switch to enforce authorization policies sent by the AAA server • **radius:** Uses the list of all RADIUS servers configured with the **radius-server host** command • ***group-name:*** Uses a subset of RADIUS servers as defined by the **aaa group server radius** *group-name* argument
aaa accounting dot1x default start-stop group {radius | *group-name*}	Specifies the accounting method for IEEE 802.1X • **radius:** Uses the list of all RADIUS servers configured with the **radius-server host** command • ***group-name:*** Uses a subset of RADIUS servers as defined by the **aaa group server radius** *group-name* argument

Cisco IOS Software RADIUS Settings	
radius-server host {*hostname* | *ip-address*} [key *string*]	Specifies a RADIUS server The value of the key string defined here must match the shared secret configured for this switch on the Cisco Secure ACS in Section 3.1.
ip radius source-interface *subinterface-name*	Specifies a source interface for RADIUS traffic sourced from the switch If there is more than one Layer 3 interface on the switch, use this command to help ensure that the switch sends RADIUS traffic with the same source address used to define the switch in the Cisco Secure ACS configuration in Section 3.1.

Cisco IOS Software IEEE 802.1X Global Settings	
dot1x system-auth-control	Globally enables IEEE 802.1X port-based access control

Cisco IOS Software IEEE 802.1X Interface Settings	
authentication host-mode multi-domain	Enables multi-domain authentication host-mode to support one phone in the voice domain and one data device in the data domain.
authentication port-control auto	Enables port-based authentication and causes the port to begin in the unauthorized state
mab	Enables MAC authentication bypass (MAB) as a fallback to IEEE 802.1X. If either the phone or the data device needs to authenticate using MAB, this command must be configured.
dot1x pae authenticator	Configures the interface to act only as an IEEE 802.1X authenticator and ignore any messages meant for a supplicant
dot1x timeout tx-period *seconds*	Sets the number of seconds that the switch waits for a response to an EAPoL Identity-Request packet before retransmitting the request; the default is 30 The total value of the IEEE 802.1X timeout is determined by a combination of tx-period and max-reauth-req (see below).
dot1x max-reauth-req *count*	Specifies the number of times EAPoL Identity-Request packets are retransmitted (if lost or not replied to); the default value is 2 To calculate the total timeout period when there is no IEEE 802.1X supplicant present, use the following formula: **tx-period * (max-reauth-req +1)**.

The following example shows a basic IEEE 802.1X configuration that will support IP telephony using MDA. To give MAB devices faster network access, the IEEE 802.1X timeout using the configuration below will be 9 seconds: tx-period * (max-reauth-req +1) = 3 * 3 = 9 seconds.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
dot1x system-auth-control
!
interface FastEthernet2/48
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 41
 authentication host-mode multi-domain
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

```
 spanning-tree bpduguard enable
!
radius-server host 10.200.1.52 key cisco123
```

Note: For detailed information about configuring IEEE 802.1X on Cisco IOS Software, see the Identity-Based Networking Services (IBNS) configuration guide at

3.5 Monitor IP Telephony in an IEEE 802.1X Environment

This section describes how to monitor IP Telephony in an IEEE 802.1X environment.

3.5.1 Monitoring Sessions from The CLI

The most comprehensive CLI for monitoring IP Phones in an IEEE-802.1X enabled network is the "show authentication sessions" command. Two example are shown below.

Example 1: IEEE-802.1X-authenticated phone

In the output below, you see one authenticated session for an IEEE 802.1X-authenticated Cisco IP Phone. In this case, there is no data device plugged in behind the phone. Note that you can determine that this phone used an LSC to authenticate since the User-Name listed below begins with "SEP."

```
switch#show authentication sessions interface fastEthernet 2/48
            Interface:  FastEthernet2/48
          MAC Address:  001e.4aa9.00a8
           IP Address:  10.100.41.200
            User-Name:  SEP001E4AA900A8
               Status:  Authz Success
               Domain:  VOICE
      Oper host mode:  multi-domain
    Oper control dir:  both
       Authorized By:  Authentication Server
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A640A04000000107633FEDF
     Acct Session ID:  0x00000014
              Handle:  0x07000011

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not Run
```

Example 2: IEEE 802.1X-authenticated data device plugged in to MAB-authenticated phone.

In the output below, you see two sessions on interface fastEthernet 2/47: an IEEE 802.1X-authenticated data device in the DATA domain and a MAB-authenticated phone in the VOICE domain.

```
switch#show authentication sessions interface fastEthernet 2/47
           Interface:  FastEthernet2/47
         MAC Address:  0018.f809.cfc4
          IP Address:  10.100.40.200
           User-Name:  IDENTITY\Administrator
              Status:  Authz Success
              Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A640A04000000217AAB4001
     Acct Session ID:  0x00000029
              Handle:  0x58000022
Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
---------------------------------------
           Interface:  FastEthernet2/47
         MAC Address:  0018.bac7.bccc
          IP Address:  10.100.41.203
           User-Name:  00-18-BA-C7-BC-CC
              Status:  Authz Success
              Domain:  VOICE
      Oper host mode:  multi-domain
    Oper control dir:  both
       Authorized By:  Authentication Server
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A640A04000000207AAAF309
     Acct Session ID:  0x00000028
              Handle:  0xF0000021

Runnable methods list:
      Method   State
      dot1x    Failed over
      mab      Authc Success
```

Another useful CLI for monitoring the link state of the phone's second port is "show cdp neighbors detail." Note that even though one phone (the 7961) is IEEE 802.1X-capable and the other (the 7960) is not, both phones can use CDP to accurately report the status of the second port.

Example 3: Reported link state with no device connected behind IP Phone.

As you can see in the highlighted section below, the phone is reporting that its second port is down (no data device is connected).

```
switch#show cdp neighbors fastEthernet 2/48 detail
-------------------------
Device ID: SEP001E4AA900A8
Entry address(es):
  IP address: 10.100.41.200
Platform: Cisco IP Phone 7961,  Capabilities: Host Phone Two-port Mac
Relay
Interface: FastEthernet2/48,  Port ID (outgoing port): Port 1
Holdtime : 141 sec
Second Port Status: Down
Version : SCCP41.8-5-2S
advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Power request id: 168, Power management id: 3
Power request levels are:6300 0 0 0 0
Management address(es):
```

Example 4: Reported link state with a device connected behind IP Phone.

As you can see in the highlighted section below, the phone is reporting that its second port is up (data device is connected).

```
Switch #show cdp neighbors fastEthernet 2/47 detail
-------------------------
Device ID: SEP0018BAC7BCCC
Entry address(es):
  IP address: 10.100.41.203
Platform: Cisco IP Phone 7960,  Capabilities: Host Phone Two-port Mac
Relay
Interface: FastEthernet2/47,  Port ID (outgoing port): Port 1
Holdtime : 173 sec
Second Port Status: Up
Version : P00308010100
advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):
```

3.5.2 Monitoring Sessions from ACS

Use the reporting capabilities on Cisco Secure ACS to verify the session details. The following output shows the ACS report for the three authenticated sessions (one voice session and one data session on fastEthernet 2/47 and one voice session on fastEthernet 2/48).

Logged At	RADIUS Status	Details	Username	MAC/IP Address	Access Service	Selected Authorization Profiles	Authentication Method	Network Device	NAS Port ID
Mar 19,10 12:30:02.660 PM	✔		SEP001E4AA900A8	00-1E-4A-A9-00-A8	802.1X Access Service	Phone Profile	x509_PKI	IDF-SJ-24-2-4503-1	FastEthernet2/48
Mar 19,10 10:31:33.363 AM	✔		IDENTITY\Administrator	00-18-F8-09-CF-C4	802.1X Access Service	Permit Access	PEAP (EAP-MSCHAPv2)	IDF-SJ-24-2-4503-1	FastEthernet2/47
Mar 19,10 10:31:23.023 AM	✔		00-18-BA-C7-BC-CC	00-18-BA-C7-BC-CC	MAB Access Service	Phone Profile	Lookup	IDF-SJ-24-2-4503-1	FastEthernet2/47

3.6 Troubleshoot IP Telephony In an IEEE 802.1X-enabled environment

Table 5 summarizes some common problems encountered when configuring IP telephony in an IEEE 802.1X-enabled environment.

Table 5. IP Telephony Troubleshooting

Symptom	Possible Root Causes	Resolution
Phone authenticates but does not get access to the voice VLAN.	• AAA server did not send device-traffic-class=voice VSA when phone authenticated.	• Correct the configuration on the AAA server.
Port err-disables when PC is connected behind phone.	• Phone did not pass IEEE 802.1X or MAB • Phone authenticated successfully but AAA server did not send device-traffic-class=voice VSA. • Switch was not configured to accept authorization from the AAA server.	• Correct the configuration on the AAA server and/or the switch. • Change the security violation handling configuration on the switch to “restrict” instead of “shutdown” to mitigate the behavior under these conditions.
	• Session from previously connected data device was not properly cleared (i.e. the link state issue).	• Implement a link-state solution (e.g. CDP Enhancement for 2nd Port Disconnect, Inactivity Timer)
IEEE 802.1X-capable devices behind phones get MAB authenticated or put in Guest VLAN	• Phone does not pass EAPoL messages correctly from data device	• Upgrade phone firmware
IEEE 802.1X-capable Cisco IP Phones are authenticated by MAB	• The phone is not enabled for IEEE 802.1X by default	• Use CUCM to enable the phone for IEEE 802.1X
Cisco IP Phone fails IEEE 802.1X	• ACS requested EAP-MD5 instead of EAP-TLS and phone has no password by default.	• Configure ACS to request EAP-TLS when authenticating IP Phones.

4. Conclusion

By leveraging the intelligence of the Catalyst switching platforms, the Cisco Unified Communications infrastructure, and the flexible policy engine of ACS, an end-to-end Cisco solution provides unparalleled integration between IP Telephony and IEEE-802.1X. By following the recommendations and best practices outlined in this document, customers can enjoy the benefits of IP telephony without having to sacrifice the security and visibility of an IEEE-802.1X-enabled network.

5. Appendix A: References

This section provides a list of references.

5.1 Cisco Product Documentation

- Scenario-based IEEE 802.1X design guide: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html
- Scenario-based IEEE 802.1X configuration guide: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/Whitepaper_c11-532065.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Printed in USA C17-605524-02 01/11