IP Telephony for 802.1X Design Guide

Last Updated: December 16, 2013

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

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

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

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

IP Telephony for 802.1X Design Guide

IP Telephony for 802.1X Design Guide

IP telephony is one of the most widely deployed technologies, and has specific requirements and expectations at the access layer. This design guide addresses deployment considerations and best practices when integrating IP telephony with an 802.1X-enabled network. This document includes the following sections:

IP Telephony for 802.1X Overview

This section introduces the integration of IP telephony with an 802.1X-enabled network, and includes the following topics:

About IP Telephony in Identity-Enabled Networks

As 802.1X becomes more widely deployed in wired networks, organizations must reconcile access controls provided by IEEE 802.1X with the unique requirements of other network technologies.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco IOS Software enables standards-based network access control by using the IEEE 802.1X protocol to secure the physical ports where end users connect. 802.1X is an IEEE standard that permits or denies network connectivity based on the identity of the end user or device. However, the IEEE standard was not designed to accommodate the unique requirements of IP telephony. In particular, IP phones complicate the implementation of 802.1X in the following ways:

- Assumption of network access—By default, 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 IP telephony allows 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. The phone can only send tagged traffic on the voice VLAN and the PC can only send untagged traffic on the data VLAN. This is done to cut down on cabling, capital equipment, and administrative costs. However, 802.1X does not directly address this issue.
- 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. However, 802.1X-enabled ports rely heavily on link state to determine when to start and stop the authentication state machine. This helps to ensure the validity of the authenticated session, and to prevent security holes or attacks.

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

- Phones that support 802.1X must be configured correctly.
- Phones that do not support 802.1X must be provided with some other means to access the voice network.
- 802.1X-enabled ports must address IP telephony deployments with a phone and a data device on the same port.
- Compensation for the lack of link state awareness.

An 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, known as TrustSec, for an 802.1X-enabled network that fully integrates IP telephony.

An end-to-end Cisco solution provides unparalleled integration between IP telephony and 802.1X by taking advantage of the intelligence of the Cisco Catalyst switching platforms, the Cisco Unified Communications infrastructure, and the flexible policy engine of the Cisco Access Control Server (ACS). 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 802.1X-enabled network.

Features and Benefits

An 802.1X-aware IP telephony system and a flexible policy server must be part of an intelligent infrastructure. TrustSec is an end-to-end solution for an 802.1X-enabled network that fully integrates IP telephony. Key features in the TrustSec system include the following:

- Multi-domain authentication (MDA)—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—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, including the following:

- 802.1X-capable IP phones—Many Cisco IP phone versions support 802.1X. They can use either pre-provisioned manufacturing installed certificates (MIC) or customer-controlled locally significant certificates (LSCs) for 802.1X authentication.
- Touchless phone configuration and certificate enrollment—Starting in Version 7.1.2, the Cisco Unified Communication Manager (Unified CM) can centrally enable phones for 802.1X via a downloaded configuration file. In addition, Unified CM provides a Certificate Authority Proxy Function (CAPF) that enables phones to enroll locally-signed LSCs to use for authentication. Because these functions are performed over the network, there is no need to physically touch the phones.
- Touchless phone authentication—Cisco ACS can be configured to authenticate IP phones and authorize them into the voice domain purely on the basis of a valid certificate. Because the certificate attributes alone can be used to determine the validity of a phone, there is no need to enter the names of the phones in any internal or external database. This significantly reduces the amount of configuration required to support IP phones.

Solution Components

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

- Cisco Catalyst 2960 and 2960S Series Switches with Cisco IOS Software Release 12.2(55)SE3
- Cisco Catalyst 3750, 3750E, and 3750X Series Switches with Cisco IOS Software Release 12.2(55)SE3
- Cisco Catalyst 4500E Series Switches with Cisco IOS Software Release 12.2(53)SG5
- Cisco Catalyst 6500 Series Switches with Cisco IOS Software Release 12.2(33)SXI7
- Cisco Secure ACS Version 5.2 + patch 3
- Cisco IP phone firmware 9.0.3
- Cisco Unified Communication Manager 8.0.3

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.

Additional Authentication Features

Although 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 or third-party devices, including the following:

- MAC authentication bypass (MAB)—A secondary authentication method that enables a Cisco Catalyst switch to check the MAC address of the connecting device in place of a successful 802.1X authentication. Phones that cannot perform 802.1X can be authenticated based on a MAC address.
- Flexible authentication (FlexAuth)—A combination of features that enables you to deploy a single configuration for every port in the network and know that the Cisco Catalyst switch intelligently applies the correct authentication and authorization policy. This works whether the device is a phone or a PC, or even if the device does not support 802.1X. 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 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 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. However, unlike CDP Enhancement for Second Port Disconnect, this feature works only for 802.1X-authenticated devices; not MAB or WebAuth.
- 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 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 is triggered. By default, some Cisco Catalyst switches err-disable (shutdown) the port in response to a violation. Shutting down the port immediately causes the phone to go offline as well. Configurable security violation handling allows Cisco Catalyst switches to take alternative actions that have a less drastic effect on the phone, such as dropping traffic from the new device.

Using Multi-Domain Authentication Host Mode

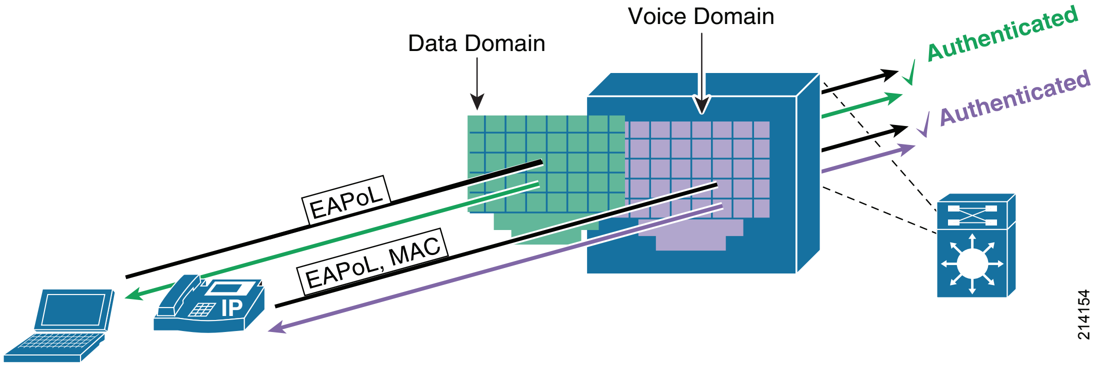
This section describes the recommended operation of IP telephony in an 802.1X-enabled network, and discusses the important stages of multi-domain authentication (MDA) host mode. It includes the following topics:

Multi-Domain Authentication Host Mode Overview

The most secure and flexible deployments of IP telephony start with MDA. MDA allows a Cisco Catalyst switch to retain 802.1X security and visibility, while modifying the default 802.1X restriction that otherwise prevents more than one device from connecting to a switchport.

When properly enabled for MDA, the switch divides the switchport into two virtual domains, equivalent to VLANs 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).

Figure 1 Multi-Domain Authentication



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, such as a phone or a data device, is connected to a given switchport, the switch authenticates that device into the correct domain.

The following sections describe the important stages of MDA operation.

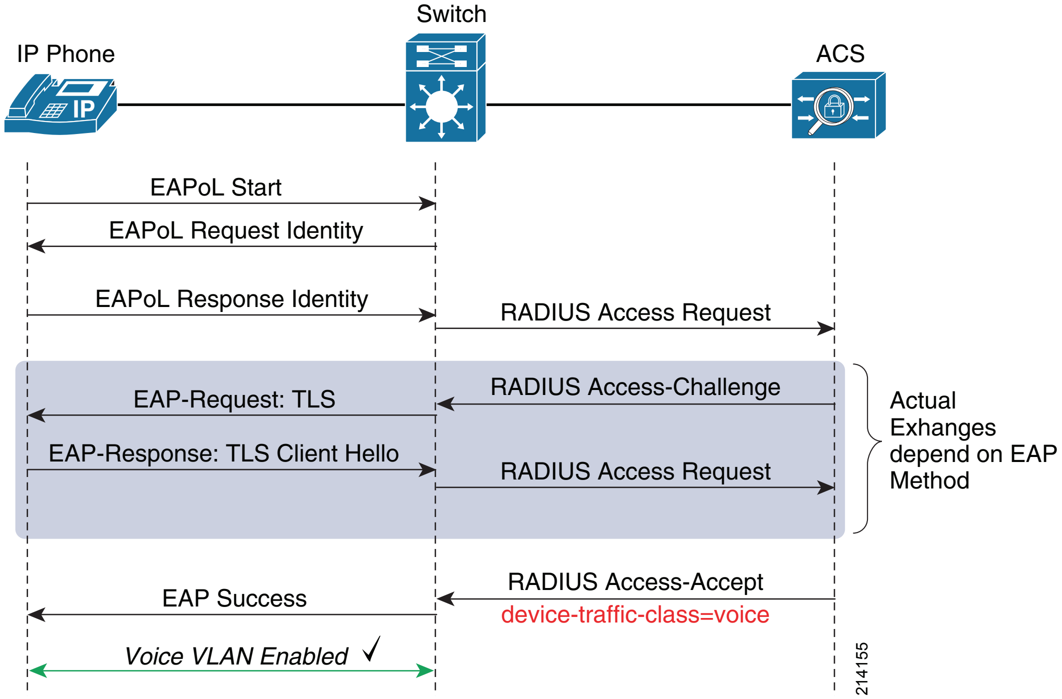
Phone Authenticates

When a phone first plugs into a switchport, the link-up event triggers the start of the 802.1X state machine on the port. To get network access, the phone must now authenticate. Phones can authenticate using either 802.1X or MAB. As part of a successful authentication, the AAA server must inform the switch that the authenticated device is a phone.

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

Figure 2 shows a typical 802.1X authentication for a phone.

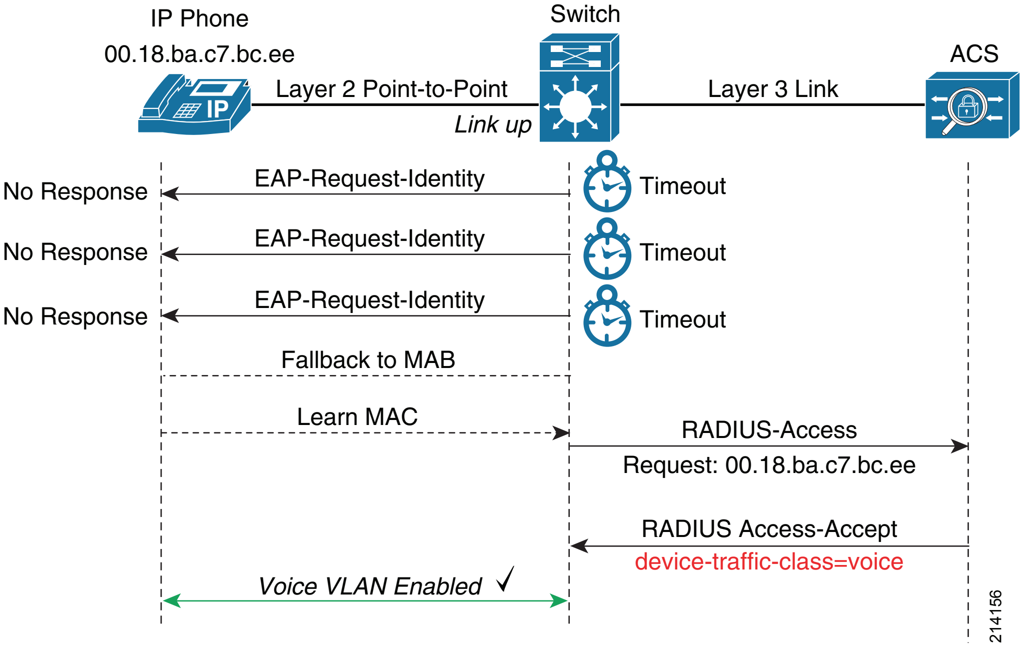
Figure 2 MDA with 802.1X Phone



Note: For more details on configuring 802.1X for IP phones, see the "Configuring Phones That Support 802.1X" section on page 38.

Figure 3 shows a typical MAB authentication for a phone. The switch initially tries to authenticate the phone using 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



Note For more operational details on MAB for IP phones, see the "Configuring Phones for MAB (Phones without 802.1X Support)" section on page 52.

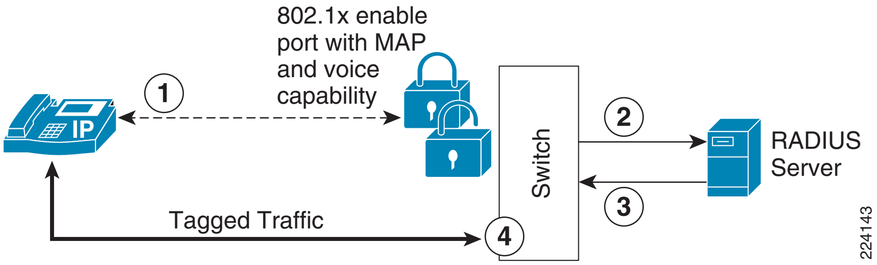
Regardless of whether the phone is authenticated via 802.1X or MAB, the most important message from the MDA perspective is the final RADIUS Access-Accept from the ACS. The Access-Accept message contains a special Cisco vendor-specific attribute (VSA) that includes the string *device-traffic-class* =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

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 Link Layer Discovery Protocol (LLDP). Other third-party phones rely on different mechanisms such as Dynamic Host Configuration Protocol (DHCP) or Trivial FTP (TFTP). MDA is flexible enough to handle both kinds of phones.

Cisco IP Phones and LLDP-Enabled Phones

After a Cisco IP phone is plugged into an MDA-enabled switch port, the sequence of steps shown in Figure 4 occurs.

Figure 4 MDA with Cisco IP Phones



The following sequence takes place:

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, such as power level, voice VLAN ID (VVID), and so on) 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.

   Traffic Allowed Prior to Authentication: By default, 802.1X ensures that all traffic is dropped except for traffic needed for authentication. However, when MDA is enabled, the switch makes a few exceptions to this rule. Most notably, both CDP and LLDP are allowed before 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 before authentication, the switch drops all other traffic, whether tagged with the voice VLAN or not, if the phone has not authenticated.

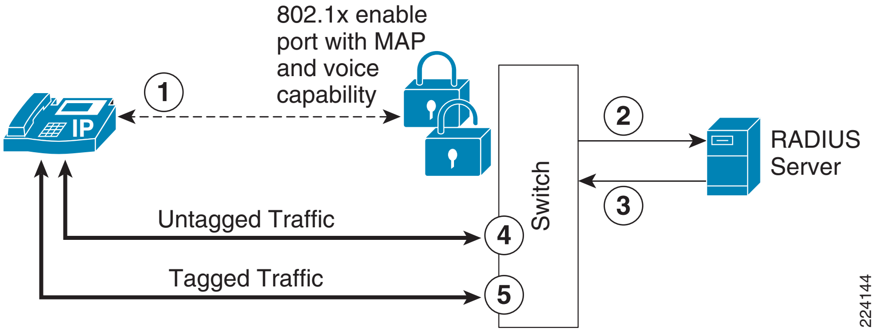
Tip **Best Practice Recommendation—Enable Control Plane Policing (CoPP)**. Because LLDP and CDP are allowed before authentication, CoPP can be used to rate-limit these types of traffic, thus preventing them from being used as a denial-of-service (DoS) attack vector. Consider enabling CoPP if your platform 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. After the Cisco IP phone is successfully authenticated via 802.1X or MAB, the AAA server sends a RADIUS-Accept message to the switch with the device-traffic-class=voice VSA. After this attribute is received, the switch authorizes the MAC address of the phone and allows it access to the voice VLAN. The switch also temporarily allows the MAC address of the phone 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. This traffic is allowed through the switch port as a result of authenticating the MAC address of the Cisco IP phone in the voice domain. After the switch receives tagged traffic from the phone, indicating that the phone has learned the VVID, the switch no longer allows the MAC address of the phone 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 than a Cisco IP phone. This is because third-party phones may not be capable of sending LLDP frames to learn the voice VLAN. Figure 5 shows the operation of MDA with third-party IP phones.

Figure 5 MDA with Third-Party IP Phones



The sequence is as follows:

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. After the connecting IP phone is successfully authenticated via 802.1X or MAB, the AAA server responds with a RADIUS-Access-Accept message with the *device-traffic-class=voice* VSA, and the switch port is authorized in the voice domain.
4. Port forwarding is still authorized on both the voice and data VLANs at this point. Although 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.

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 802.1X supplicant, or DHCP or ARP traffic from a non-IEEE-802.1X-capable device. The switch then sends a unicast EAPoL-Request packet to the device to initiate the authentication.

An IP phone usually sends multicast Extensible Authentication Protocol over LAN (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 MAC address of the IP phone. 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. However, when a device connects behind the phone, the switch sends no EAPoL frames until the MAC address of the device is learned. This way, the switch does not risk disturbing the authenticated session of the phone. 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 times out and continue to the next authentication method, such as MAB, and/or authorization type, such as Guest VLAN. If the device later becomes capable of performing 802.1X, perhaps because the operating system finished booting or a supplicant was manually enabled, the data device should send an EAPoL-Start message to explicitly tell the switch to begin authentication.

Tip **Best Practice Recommendation—Configure supplicants to send EAPoL-Start messages.** 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 802.1X. If your supplicant does not send EAPoL-starts by default, Cisco recommends enabling them.

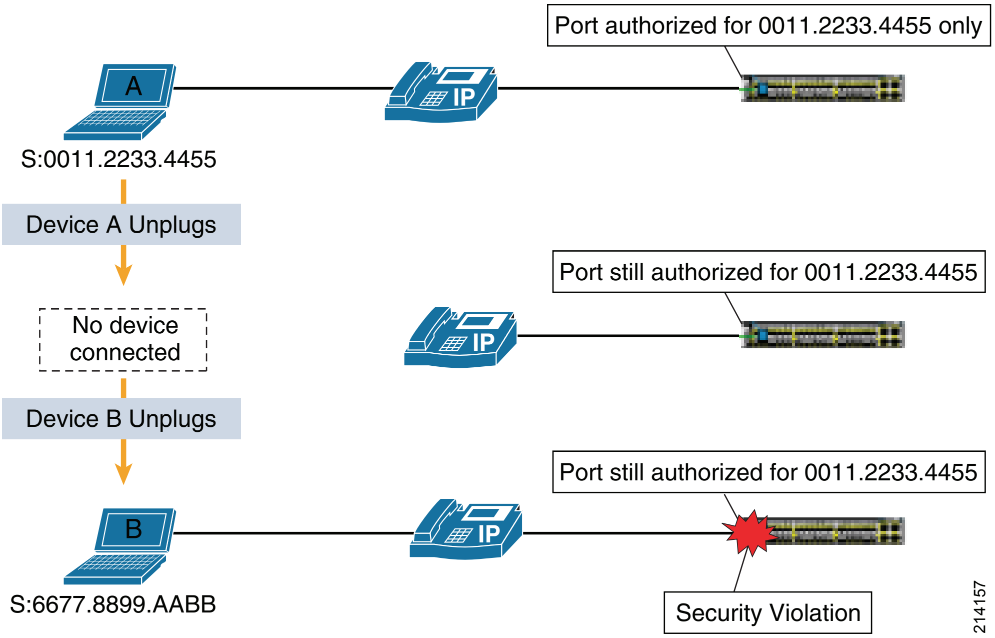
If the data device passes authentication, either via 802.1X or MAB, it is allowed access to the data domain only. If the device fails authentication, it is not allowed access to either domain, unless the Auth-Fail VLAN has been configured, but the phone continues to operate normally.

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 is triggered. This can be a problem when a phone fails to authenticate properly. If a phone fails authentication, the switch does not receive the device-traffic-class=voice VSA from the AAA server, and the switch assumes that the failed device was in the data domain. However, if there is already a data device behind the phone, there are two devices in the data domain, and a security violation is triggered. Therefore, although 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.

Device Behind Phone Disconnects (Link State Issues)

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. Figure 6 shows an example of the link state issue.

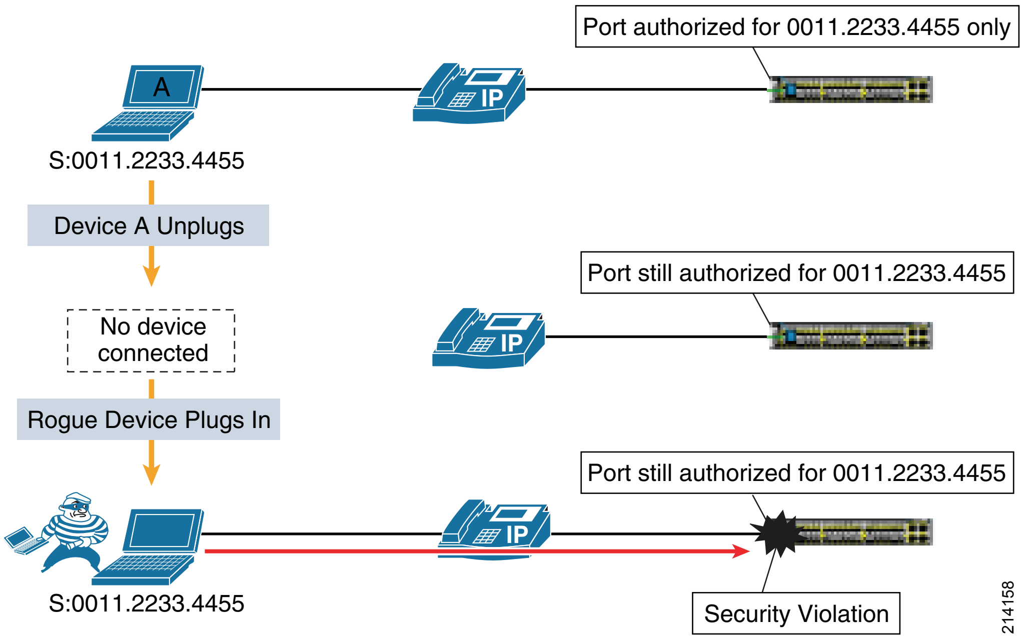
Figure 6 Link State Problem 1—Authorized User B Triggers Security Violation


Port authorized for 0011.2233.4455 only
A
IP
S:0011.2233.4455
Device A Unplugs
Port still authorized for 0011.2233.4455
No device connected
IP
Device B Unplugs
Port still authorized for 0011.2233.4455
B
IP
S:6677.8899.AABB
Security Violation
214157

In Figure 6, 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 the MAC address of Device A 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 perspective of the switch, Device B is an unauthorized device that may be trying to piggyback on the authenticated session of Device A. Therefore, the switch immediately triggers a security violation.

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

Figure 7 Link State Problem 2—Rogue User Spoofs Authenticated User Session


Port authorized for 0011.2233.4455 only
A
IP
S:0011.2233.4455
Device A Unplugs
Port still authorized for 0011.2233.4455
No device connected
IP
Rogue Device Plugs In
Port still authorized for 0011.2233.4455
IP
S:0011.2233.4455
Security Violation
214158

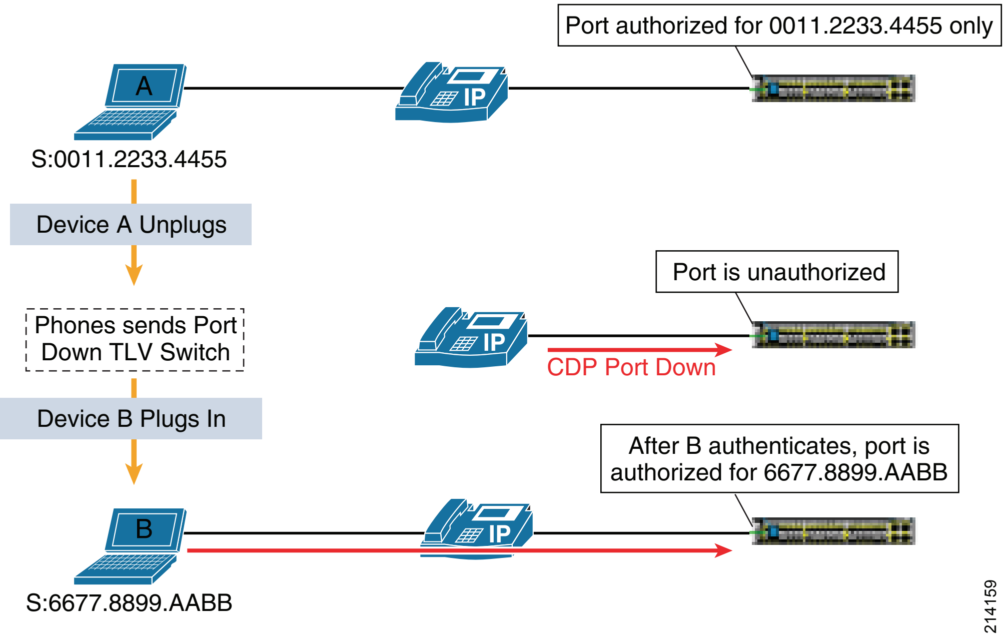
In Figure 7, Device A has previously authenticated behind the IP phone. Device A unplugs, but the switch, not knowing A has left, keeps the port authorized for the MAC address of Device A. Sometime later, a rogue user plugs in and spoofs the MAC address of Device A. Because there is still an existing 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. The following sections discuss three possible solutions, in order of preference. One or more of these methods must be operational to ensure smooth integration of IP telephony and 802.1X.

Cisco Discovery Protocol 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 data port of the phone (the second port), but the phone does. Therefore, if the phone can communicate link state to the switch, the switch can immediately clear the session. This is exactly what the CDP Enhancement for Second Port Disconnect, also known as host movement detection, does. Cisco IP phones can send a CDP message to the switch indicating that the link state for the port of the data device is down, allowing the switch to immediately clear the session of the data device, as shown in Figure 8.

Figure 8 Recommended Link State Solution—CDP Enhancement for Second Port Disconnect


Port authorized for 0011.2233.4455 only
A
S:0011.2233.4455
Device A Unplugs
Phones sends Port Down TLV Switch
Port is unauthorized
CDP Port Down
Device B Plugs In
After B authenticates, port is authorized for 6677.8899.AABB
B
S:6677.8899.AABB
214159

Cisco IP phones and Cisco Catalyst switches with the appropriate releases of code automatically perform CDP Enhancement for Second Port Disconnect. It works for all authentication methods, including 802.1X, MAB, and WebAuth, and no configuration is required.

Tip **Best Practice Recommendation—Use CDP Enhancement for Second Port Disconnect.** This feature works for all authentication methods, takes effect as soon as the device disconnects, and requires no configuration. If you are using Cisco IP phones and Cisco 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 inability of the switch to detect link state for devices connected behind IP phones.

Table 1 lists the minimum firmware needed by various Cisco IP Phones to use CDP Enhancement for Second Port Disconnect.

Table 1 Cisco IP Phone Models and Firmware Needed

Cisco IP Phone Model	Minimum firmware for CDP Enhancement for Second Port Disconnect
7902, 7905, 7910, 7912, 7920, 7935, 7936	Not supported
7940, 7960	8.1(1)
7906, 7911, 7931, 7937, 7941, 7942-G, 7945-G, 7961, 7962-G, 7965-G, 7970, 7971, 7975-G	8.4(1)
8941, 8945, 8961	9.1(2)
9951, 9971	9.1(2)

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 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 802.1X device has unplugged from behind the phone. The phone substitutes the MAC address of the data device, so the proxy EAPoL-Logoff message is indistinguishable from an actual EAPoL-Logoff from the data device itself. The switch immediately clears 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 because the EAPoL-Logoff message is fully supported as per the IEEE standard.

Although effective for 802.1X-authenticated endpoints, Proxy EAPoL-Logoff does not work for MAB or WebAuth, because these authentication methods do not use EAP to authenticate. Another method, such as the 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 counts down. When the timer expires, the switch removes the authenticated session. The inactivity timer applies to 802.1X and MAB sessions.

Note The current implementation of WebAuth uses a different, IP Device Tracking-based inactivity timer than 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 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 because this provides 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, there is no need to assign an inactivity timer for 802.1X-authenticated sessions. In this scenario, you can prevent the inactivity timer from being needlessly assigned to 802.1X-authenticated devices by sending RADIUS Attribute 28 only to MAB-authenticated devices.

The following are important caveats when using the inactivity timer to clear sessions from behind IP phones:

- While the inactivity timer is counting down, the port is still subject to the potential security violation and security hole described above.
- 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. Therefore, a quiet device that does not send traffic for long periods of time, such as a network printer that services occasional requests but is otherwise silent, may have its session cleared even though it is still connected. That device must then send traffic before it can be authenticated again and have access to the network.

Tip **Best Practice Recommendation—Enable IP Device Tracking** to keep quiet devices connected. If IP Device Tracking is enabled, the switch periodically sends ARP probes to devices in the IP Device Tracking table, which is initially populated by DHCP requests or ARP from the end point. As long as the device is connected and responds to these probes, the inactivity timer is not triggered and the device is not inadvertently removed from the network.

In general, testing is required to find an optimal value for the inactivity timer in your network: short enough to minimize the impact of security violations and holes, and 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:

- Use the inactivity timer only 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 802.1X or MAB.
- If your phones support proxy EAPoL-Logoff, rely on that feature to clear sessions for 802.1X-authenticated devices, and use the RADIUS-assigned inactivity timer for MAB devices.
- Enable IP Device Tracking to send keepalives to quiet devices.
- Test your network to find the optimal value for this timer. Use the smallest possible value that does not impact your quiet devices.

Authentication with IP Phones

This section describes methods of authentication supported using IP phones, and includes the following topics:

- Using Certificates, page 17
- Using Passwords, page 23

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

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

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

Using Certificates

This section describes how to use certificates with IP phones in an 802.1X deployment and includes the following topics:

- Certificate Support with IP Phones, page 18
- Certificate Types, page 18
- Self-Signed CAPF vs. CA-Signed CAPF, page 20

Tip **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 passwords.

Certificate Support with IP Phones

The Cisco IP phones listed in Table 2 support authentication via X.509 certificates using the EAP-Transport Layer Security (EAP-TLS) or EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) methods of authentication.

Table 2 Cisco IP Phones that Support Authentication via Xs.509 Certificates

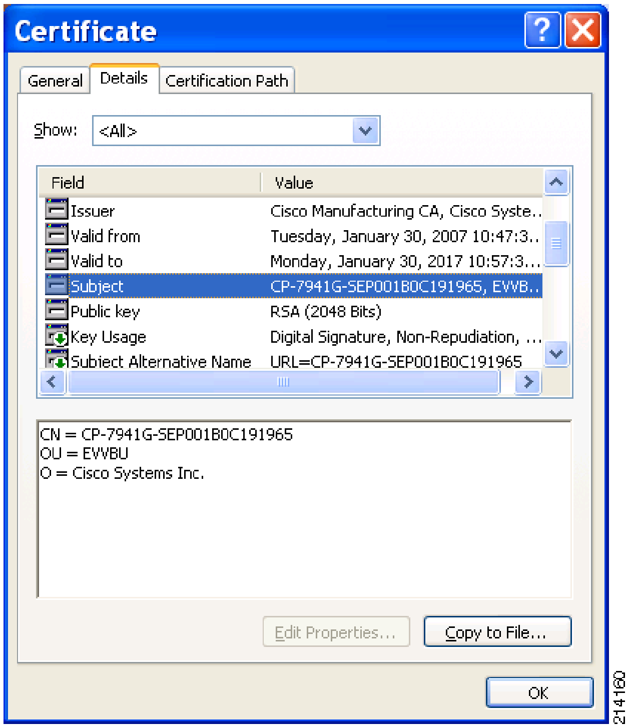
Cisco IP Phone Models	Minimum firmware for X.509 Certificate-based 802.1X using EAP-TLS or EAP-FAST	Recommended firmware for 802.1X
7906, 7911	8.5(2)	9.0(3)
7931, 7937	8.5(2)	9.0(3)
7941, 7942-G, 7945-G	8.5(2)	9.0(3)
7961, 7962-G, 7965-G	8.5(2)	9.0(3)
7970, 7971, 7975-G	8.5(2)	9.0(3)
All newer Cisco Phones should support EAP-TLS or EAP-FAST		

Certificate Types

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 to secure the signaling and voice path used for IP telephony, but the same certificates can be used for 802.1X.

As the name suggests, the MIC is pre-loaded on the phone at the time of manufacture. The Cisco Manufacturing Certificate Authority signs it. Figure 9 shows a sample MIC.

Figure 9 Sample MIC



Show: <All>

Field	Value
Issuer	Cisco Manufacturing CA, Cisco Syste...
Valid from	Tuesday, January 30, 2007 10:47:3...
Valid to	Monday, January 30, 2017 10:57:3...
Subject	CP-7941G-SEP001B0C191965, EVVB...
Public key	RSA (2048 Bits)
Key Usage	Digital Signature, Non-Repudiation, ...
Subject Alternative Name	URL=CP-7941G-SEP001B0C191965

CN = CP-7941G-SEP001B0C191965
OU = EVVBU
O = Cisco Systems Inc.

Table 3 lists the fields and values for the sample MIC shown in Figure 9.

Table 3 MIC Details

Field	Value
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

Table 3 MIC Details

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

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 Unified CM. 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, Unified CM 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 Unified CM, LSC and MIC certificates are stored in following location on Unified CM: /var/log/active/cm/trace/capf/sdi. The files can be retrieved using the Unified CM CLI command **file get activelog cm/trace/capf/sdi/*.cer**. Another way to view the certificate of the phone 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 whether 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 CAPF of the Unified CM, which is the central call control and configuration engine for Cisco IP Telephony.

Self-Signed CAPF vs. CA-Signed CAPF

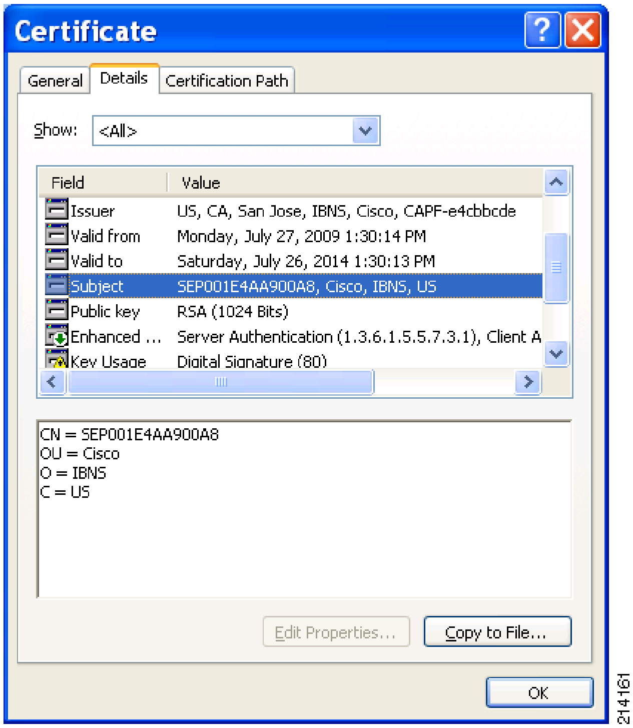
Unified CM can sign LSCs using the following types of CAPF:

- Self-signed CAPF—Acts as a standalone CA, signing the LSCs with its own self-signed certificate.
- CA-signed CAPF—Signed by an external CA. A CA-signed CAPF signs the LSCs with the externally signed certificate in a subordinate manner.

Self-signed CAPF CAs have a lifetime of five years. Therefore, if you use a self-signed CAPF, the CAPF certificate must be renewed after five years and all the LSCs must be reissued. Cisco ACS does not allow network access to the phones if the LSCs have expired. The lifetime of the CA-signed CAPF is determined by the CA when it issues the certificate to Unified CM. Whatever lifetime you choose, be sure to renew the CAPF certificate and reissue the LSCs before expiration.

Because the LSC has been issued by your own Unified CM CA, you can be certain that a phone presenting a valid LSC is in fact a corporate-owned and managed asset. Figure 10 shows a sample LSC.

Figure 10 Sample LSC



Field	Value
Issuer	US, CA, San Jose, IBNS, Cisco, CAPF-e4cbbcde
Valid from	Monday, July 27, 2009 1:30:14 PM
Valid to	Saturday, July 26, 2014 1:30:13 PM
Subject	SEP001E4AA900A8, Cisco, IBNS, US
Public key	RSA (1024 Bits)
Enhanced ...	Server Authentication (1.3.6.1.5.5.7.3.1), Client A
Key Usage	Digital Signature (80)

CN = SEP001E4AA900A8
OU = Cisco
O = IBNS
C = US

Table 3 lists the fields and values for this sample LSC.

Table 4 LSC Fields and Values

Field	Value
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

Because you control the enrollment of LSCs on phones, LSCs represent a more tightly controlled and trusted credential than MICs. Cisco recommends that you use MICs for LSC installation only. If you configure phones to use MICs for 802.1X or for any other purpose, you must be aware that MIC certificate security relies on the security of Cisco CA root private keys that are not under your control and can, in theory, be compromised.

Table 5 lists some key differences between MICs and LSCs.

Table 5 MIC and LSC Comparison

	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-SEPYYYYYYYYYYYYY 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 Unified CM at end of lifetime
Revocation	Not supported.	Not supported
Best Use Cases	Lab testing, bootstrapping a phone onto the network	General use

In an 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 certificate of the phone. The root certificates for both LSCs and MICs can be exported from the Unified CM Operating System Administration interface and imported into your AAA server.

After 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, because 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.

Tip **Best Practice Recommendation—Use certificate attributes for phone authorization**. This method avoids the need to enter individual phones in a database, thus significantly reducing the effort needed to deploy 802.1X for phones. ACS 5.x supports certificate attribute-based authorization for EAP-TLS. Note that as of release 5.x, only the attributes of the certificate subject, listed in Table 5, can be used in an ACS 5.x authorization policy. The attributes of the issuer cannot be used. ACS 4.2 supports certificate-only authorization for enabling EAP-FAST PKI authorization bypass.

If your AAA server does not support authorization based on certificate attributes alone, it requires an additional lookup, using the Common Name (CN) or another attribute in the certificate to query another database to gather sufficient information to authorize the phone. Thus, the name of every phone must be entered into an internal or external database for validation.

Certificate Revocation

There is currently no mechanism within Unified CM for revoking MICs and LSCs. If the certificate of a phone becomes invalid or a phone is stolen, that phone must be removed from, or renamed in, Unified CM to prevent it from gaining access to the call control resources in Unified CM. Although the phone is not able to register or make calls, the lack of an explicit certificate revocation mechanism means that the phone is still able to authenticate using 802.1X, because its certificate is still valid as far as the AAA server can determine. To keep the phone with a revoked certificate from gaining network access via 802.1X, use an exception policy in ACS 5 to specifically disallow that phone when it attempts to authenticate.

Note For more information on exception policies, see the ACS product documentation.

Using Passwords

Table 6 lists the Cisco IP phones that support authentication via username and password using the EAP-MD5 method of authentication.

Table 6 Cisco IP Phones that Support EAP-MD5

Cisco IP Phone Model	Minimum firmware for password-based 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 (for example, 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 IP **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.

MAC Authentication Bypass

MAB enables a Cisco Catalyst switch to check the MAC address of the connecting device in place of a successful 802.1X authentication. This section includes key information you should know when implementing IP telephony with MAB and includes the following topics:

- MAB Overview, page 24
- Network Access Timing, page 24
- MAC Databases, page 25

MAB Overview

MAC Authentication Bypass (MAB), if configured, is attempted when 802.1X times out by default or fails. When MDA is enabled, both the phone and the device behind the phone can authenticate using MAB. Table 7 lists Cisco IP phones that do not support 802.1X and should therefore be authenticated using MAB.

Table 7 Cisco IP Phones that do not Support 802.1X

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

When deploying MAB for phones that cannot perform 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 are subject to delays in network access. The switch first attempts 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. There are the following three options to give non-IEEE-802.1X phones faster access:

- Adjust the default timers.
- Use FlexAuth to configure the port to attempt MAB before 802.1X.
- Use a deployment scenario such as low impact mode that allows some network access before 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 Unified CM and import them into your AAA server or an identity store, such as an LDAP directory, that your AAA server can query. Both Unified CM 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 802.1X on your network, you can run NAC Profiler for a period of time. Using DHCP fingerprinting, Simple Management Network Protocol (SNMP) polling of switch CDP tables, and other sources of information, NAC Profiler can determine which MAC addresses on your network are likely to be phones. After 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 tell you only what MAC addresses 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 Unified CM, is required.

Another possible option for third-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 exclusively assigned to IP phones, 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 because Cisco uses many OUIs for its products, none of which are used exclusively for IP phones.

After a database has been created, it must 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 802.1X on every device in your network that supports it.

Best Practices

This section discusses deployment considerations and best practices for enabling 802.1X on IP phones. Although the focus is on Cisco IP phones, many of these same principles apply to other kinds of IP phones as well.

This section includes the following topics:

Enabling 802.1X On Phones

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

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

Tip **Best Practice Recommendation—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 accepts any EAP method that the ACS requests. For example, if ACS requests EAP-MD5, the phone accepts that method, even if a password has not been configured. If a password was not configured, the phone fails 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 and most secure EAP method when authenticating a phone.

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

Tip **Best Practice Recommendation—Enable 802.1X on phones first.** Otherwise, the phones need access to the network to enable 802.1X, but they cannot get access without first doing 802.1X.

Although enabling 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 802.1X. In those situations, you have several options:

- Bring up new phones in a physically secure staging area where the access ports are not enabled for 802.1X. This allows the phones to access the network and download the needed configuration files.
- Manually enable 802.1X on each phone using the keypad. Although not practical for initial deployments of large numbers of phones, it may work for small numbers of phones.
- Authenticate the phone using MAB to give the phone enough access to the network to download its configuration file.
- Use a low impact deployment scenario to allow the phone enough access to the network before 802.1X authentication. Low impact mode allows you to deploy 802.1X on access ports with selectively open access, as specified by a port ACL, before authentication. For more information on low impact mode, see the "Low-Impact Mode" section on page 33.

WebAuth

WebAuth enables a Cisco Catalyst switch to check the credentials of a user submitted through a web login portal on the switch. WebAuth is supported with IP telephony deployments with the following important design considerations:

- When MDA is enabled, only the device behind the phone can authenticate using WebAuth. Cisco IP phones cannot be authenticated using WebAuth.
- The Cisco implementation of WebAuth on Cisco Catalyst switches uses access control lists (ACLs) to control access.

  Before WebAuth succeeds, a port ACL controls access. 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 allows traffic only 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.
- The only way to clear a WebAuth session behind a phone is using CDP Enhancement for Second Port Disconnect.

  As discussed in "Device Behind Phone Disconnects (Link State Issues)" section on page 12, inactivity timers cannot currently be used to clear WebAuth session behind phones. Because the CDP Enhancement feature is currently supported on Cisco phones and switches only, third-party phones cannot be securely 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 are not cleared correctly. Dangling sessions behind phones can lead to security violations and security holes, so this is not a viable deployment option.

Guest VLAN

If an 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 supported only for devices in the data domain. Phones that inadvertently get assigned to the Guest VLAN because of a failed MAB authentication do not function properly because they do not have access to the voice VLAN, and may cause a security violation if there is already an authenticated device in the data domain.

Auth-Fail VLAN

If an 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 supported only for devices in the data domain. Phones that inadvertently get assigned to the Auth-Fail VLAN because of a failed 802.1X authentication do not function properly because they do not have access to the voice VLAN, and may cause a security violation if there is already an authenticated device in the data domain.

Inaccessible-Auth Bypass

If an 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, which is either the statically configured voice VLAN or a dynamically assigned voice VLAN from the AAA server. IP connectivity is not disrupted for previously authenticated phones.

If a phone plugs into the port when the AAA server is down, the switch places the port in the critical VLAN. Phones that get assigned to the critical VLAN do not function properly because they do 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.

Although 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 are 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 are affected. Because this is a rare occurrence, the current behavior of Inaccessible-Auth Bypass is usually not a significant operational issue for IP telephony deployments

Tip Embedded Event Manager (EEM) has been used in the past as a workaround.

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 permits and denies traffic only from the authenticated device. To prevent ACLs in one domain from adversely affecting the other domain, if an ACL is assigned for a device in the data domain, an ACL must also be assigned to IP phones in the voice domain and vice versa.

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.

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 is necessary to have some other process to synchronize the VLAN assigned by RADIUS with the VLAN that the phone is configured to use.

Re-Authentication

IP telephony is compatible with re-authentication. The phone and 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:

- Re-authentication is not always necessary—Because 802.1X is a port-based authentication technique, the physical status of the port directly affects how long the authenticated session remains active. After a successful 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 is required to authenticate again. In the absence of link-down or logoff events, there is usually no need to re-authenticate a previously authenticated phone that remains connected to the network. Because 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 credentials of the phone serves no purpose.
- Re-authentication adds load to the AAA server—Each re-authentication adds to the load on the AAA server.
- Limitations of switch-based re-authentication—If re-authentication is locally configured on the switch, the switch does not relearn the MAC address of a MAB-authenticated device when the re-authentication timer expires. Instead, the switch simply sends the previously-learned MAC address to the AAA server again. In addition, switch-based re-authentication applies to all 802.1X and MAB sessions, so it cannot be selectively enabled for certain devices.

- Limitations of server-based re-authentication—The AAA server can force the switch to relearn 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 802.1X, so the phone loses network connectivity until 802.1X times out and MAB is re-attempted. Setting the Termination-Action attribute to RADIUS-Request causes the switch to send the previously-learned MAC address to the AAA server without impacting the network connectivity of the phone.

Re-authentication may have some value for devices in the data domain. Because 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 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 the "Device Behind Phone Disconnects (Link State Issues)" section on page 12, the CDP Enhancement for Second Port Disconnect provides a more direct way to solve this problem.

Tip **Best Practice Recommendation—Use re-authentication selectively**, **if at all**. Because it adds unnecessary load on the AAA control plane without offering additional security or functionality, re-authentication should be disabled for IP phones in most cases. If re-authentication is desired for data devices, use server-based re-authentication, which 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, such as 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 such as a phone, configure the AAA server to not send either Attribute 27 or Attribute 29 for that session.

Wake On LAN

IP telephony is compatible with the Wake on LAN (WoL) feature for 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.

Open Access

IP telephony is compatible with the open access feature. By default, 802.1X drops all traffic before a successful 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 before 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 the "Deployment Scenarios" section on page 32.

Host Modes

This section describes the different host modes, which determine the number and type of devices allowed on a port. It includes the following topics:

- Single-Host Mode, page 31
- MDA Host Mode, page 31
- multiauth Host Mode, page 31
- Multi-Host Mode, page 32

As discussed earlier, the current best practice for IP telephony is to use MDA host mode. Note that, with the only other host mode that is recommended for IP telephony is multiauth host mode. The other host modes are discussed below for the sake of completeness.

Single-Host Mode

In single-host mode, only one 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, a security violation is 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 is silently allowed onto the network by way of a feature known as CDP Bypass. The phone, or any device, that sends the appropriate type-length-value (TLV) messages in a CDP message is 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 because they access the network without generating any kind of accounting record or syslog.
- Lack of access control—Because the phones are not authenticated, their identity is not validated before 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 third-party phones—CDP Bypass works only with Cisco phones. LLDP as an authentication bypass mechanism is not supported; it might be used just for announcing Voice VLAN.
- Not supported across all switch platforms—The Cisco 3560e and 3750e platforms do not support CDP Bypass.

MDA Host Mode

MDA is the recommended host mode for IP telephony deployments.

multiauth Host Mode

multiauth host mode is essentially a superset of MDA. When multiauth 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 allows only a single device in the data domain).

multiauth is supported for IP telephony deployments when more than one data device needs to authenticate behind a phone. A common use case for multiauth behind a phone is a virtualized device with multiple host OSes. Note, however, that multiple data devices behind a phone, whether virtualized devices or physical devices connected to a hub, can exacerbate the link state awareness issue discussed in the "Device Behind Phone Disconnects (Link State Issues)" section on page 12.

Multi-Host Mode

Note Multi-host mode is not recommended for IP telephony.

Using Other Features with 802.1X

Note the following information about using other features in an 802.1X network:

- **RADIUS accounting**—Supported for IP telephony deployments. Cisco recommends enabling RADIUS accounting to ensure maximum visibility for all endpoints, voice and data, in the network.
- **AutoQoS**—Compatible with an 802.1X-enabled network.
- **Auto smart ports**—Not recommended when deploying VoIP in an 802.1X-enabled network.
- **Port security**—In general, Cisco does not recommend enabling port security when 802.1X is also enabled. When using MDA, 802.1X limits the port to one MAC address in the voice domain and one MAC address in the data domain. Therefore, port security is redundant and unnecessary.
- **DHCP snooping**—Fully compatible with IP telephony and should be enabled as a best practice.
- **Dynamic ARP Inspection**—Fully compatible with IP telephony and should be enabled as a best practice.
- **IP Source Guard**—Fully compatible with IP telephony.

Deployment Scenarios

When deploying 802.1X, Cisco recommends a phased deployment model that gradually deploys identity-based access control to the network. This section discusses three scenarios for phased deployment, and includes the following topics:

- Monitor Mode, page 32
- Low-Impact Mode, page 33
- High-Security Mode, page 34
- Deployment Summary for IP Telephony, page 34

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, configure your phones and backend databases to the fullest extent possible. Enable 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, 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 are correctly identified and assigned to the voice domain, allowing you to discover phones that cannot authenticate and phones that can authenticate but are not properly authorized into the voice domain. Because you are in monitor mode, you can identify and fix authentication and authorization problems without affecting the operation of the phone.

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

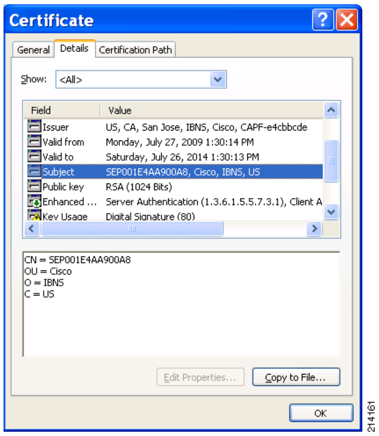
Low-Impact Mode

IP telephony is fully supported in low impact mode using MDA. 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 denying all access before authentication, as a traditional 802.1X deployment requires, low impact mode allows you to use ACLs to selectively allow traffic before authentication. This is particularly useful to devices that cannot perform 802.1X and rely on MAB to get access to the network, such as older generation IP phones. Waiting until 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 before authentication, enabling these devices to function effectively in an 802.1X-enabled environment.

As an example of the effectiveness of low impact mode, consider the issue discussed in the "Enabling 802.1X On Phones" section on page 26. New Cisco IP phones need access to the network to enable 802.1X, but they cannot get access without first doing 802.1X. Using low impact mode, you can selectively allow the traffic that the phone needs to contact the Call Manager and download a configuration file that enables 802.1X. Figure 11 shows a sample ACL.

Figure 11 Sample ACL



Show: <All>

Field	Value
Issuer	US, CA, San Jose, IBNS, Cisco, CAPF-e4cbbcde
Valid from	Monday, July 27, 2009 1:30:14 PM
Valid to	Saturday, July 26, 2014 1:30:13 PM
Subject	SEP001E4AA900A8, Cisco, IBNS, US
Public key	RSA (1024 Bits)
Enhanced ...	Server Authentication (1.3.6.1.5.5.7.3.1), Client A
Key Usage	Digital Signature (80)

```
CN = SEP001E4AA900A8
OU = Cisco
O = IBNS
C = US
```

Applied to a port in low impact mode, the ACL shown in Figure 11 allows the phone to get an IP address, resolve the hostname of its Call Manager, and download a configuration file and firmware load, all before authentication. Note, however, that the phone would not be able to place calls, because the ACL allows only DNS, DHCP, and TFTP. After 802.1X is enabled on the phone using the configuration file, the phone automatically authenticates and is assigned to the voice domain, on receipt of the *device-traffic-class=voice* VSA. As part of the authorization policy of the phone, the switch can be instructed to apply a dynamic ACL such as **permit ip any any** to the port of the phone. The successfully authenticated phone is now fully operational. Low impact mode has effectively enabled the phone to bootstrap itself onto the 802.1X-enabled network.

Tip **Best Practice Recommendation**—Use low impact mode to bootstrap phones. Because low impact mode allows limited access to the voice VLAN before authentication, it can be used to bootstrap phones onto the network.

High-Security Mode

IP telephony is fully supported in high security mode.

High security mode is a more traditional deployment model for 802.1X that denies all access before 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 802.1X would have to wait for 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 depends on the sensitivity of your phones to delays in network access. Always test your timer values before making large-scale changes.

Deployment Summary for IP Telephony

The major design decisions that must addressed before deploying IP telephony in an 802.1X-environment include the following:

- Use MDA host mode to support IP telephony in an 802.1X-enabled network.
- Supplicants on data devices behind IP phones should be configured to send EAPoL-Starts.
- 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.
- Use 802.1X to authenticate your phones if your phones support it. Otherwise, use MAB.
- Use Unified CM 7.1.2 or higher to enable phones for 802.1X over the network.
- For IEEE-802.1X-enabled-Cisco IP phones, use EAP-FAST for ACS 4.2 or EAP-TLS for ACS 5.0.
- For IEEE-802.1X-enabled-Cisco IP phones, use LSCs for 802.1X authentication.
- Use monitor mode in the initial phase of your deployment to assess the readiness of your voice and data endpoints.
- Use low impact mode to enable new IEEE-802.1X-capable-phones to perform 802.1X when access control has been enabled.

- For non-IEEE-802.1X-capable phones, export MAC addresses from Unified CM and import them into ACS to rapidly create a phone MAC database.
- Enable switch-based local WebAuth only if you are using Cisco IP phones that support CDP Enhancement for Second Port Disconnect.
- Use server-based re-authentication to selectively enable re-authentication for data devices only. Do not enable re-authentication for IP phones.
- Use multiauth host mode if you want to support multiple data devices plugging in behind a single phone.

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

Configuring IP Telephony

This section describes how to configure a system based on Cisco IOS Software for 802.1X with WebAuth fallback. This section includes the following topics:

Configuring ACS—All Phone Authentication Types

The following sections describe two configuration tasks for ACS 5.x 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 (802.1X or MAB) are covered in subsequent sections.

Configuring the Switch as a RADIUS Client in Cisco ACS

To add the switch that authenticates phones as a AAA client in Cisco Secure ACS, complete the following steps.

Procedure

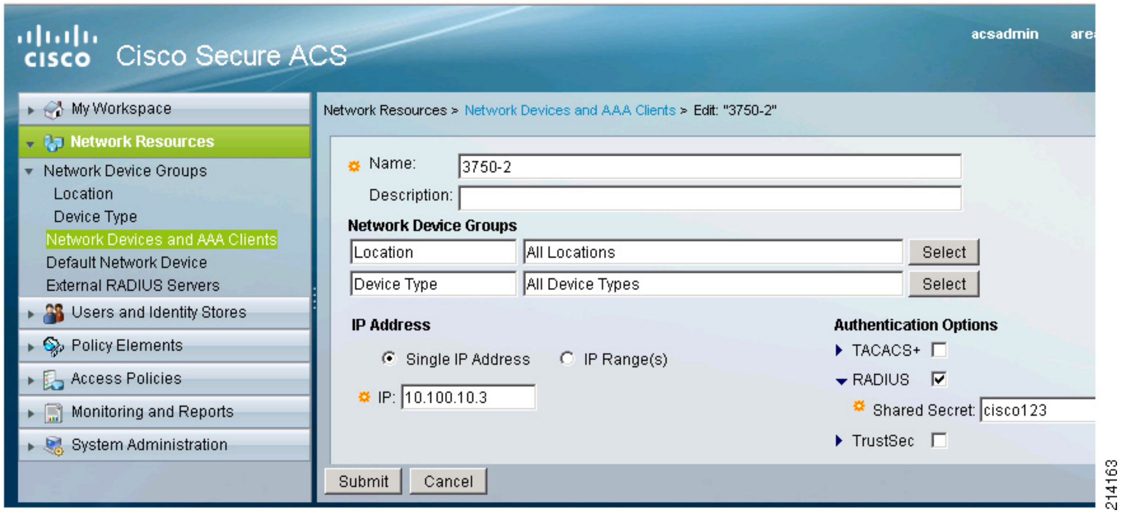
Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, expand **Network Resources** and select **Network Devices and AAA Clients**.

Step 3 Click **Create**.

The window shown in Figure 12 appears.

Figure 12 Network Devices and AAA Clients



Network Resources > Network Devices and AAA Clients > Edit: "3750-2"

Name: 3750-2

Description:

Network Device Groups

Location: All Locations

Device Type: All Device Types

IP Address

● Single IP Address ○ IP Range(s)

IP: 10.100.10.3

Authentication Options

TACACS+ □

RADIUS ☑

Shared Secret: cisco123

TrustSec □

Step 4 Specify the name, IP address, and RADIUS shared secret for this switch.

Step 5 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.

Step 6 Click **Submit**.

Creating a Phone Authorization Profile in Cisco Secure ACS

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

Procedure

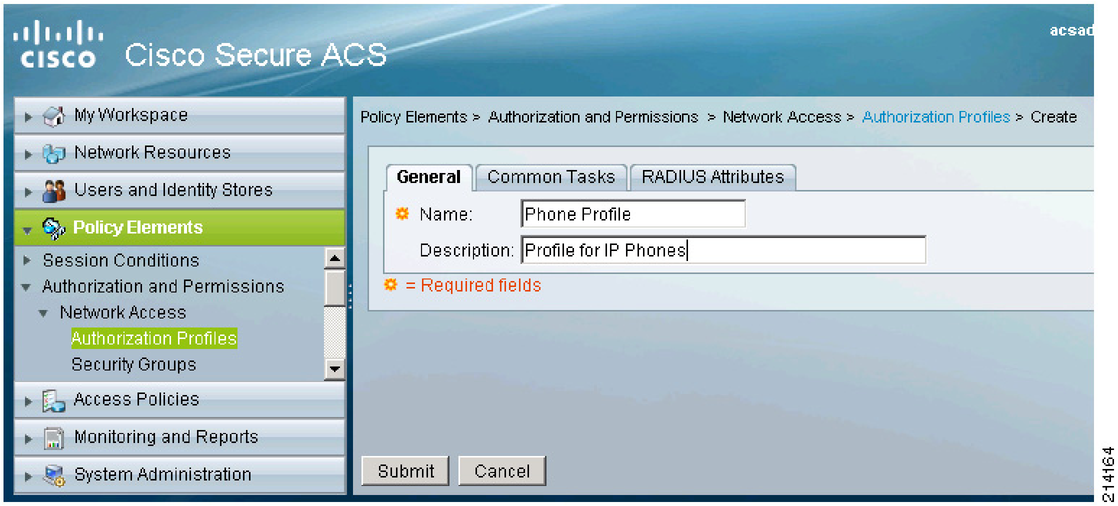
Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, go to **Policy Elements** > **Authorization and Permissions** > **Network Access** and select **Authorization Profiles**.

Step 3 Click **Create**.

The window shown in Figure 13 appears.

Figure 13 Creating Authorization Profiles



Name: Phone Profile

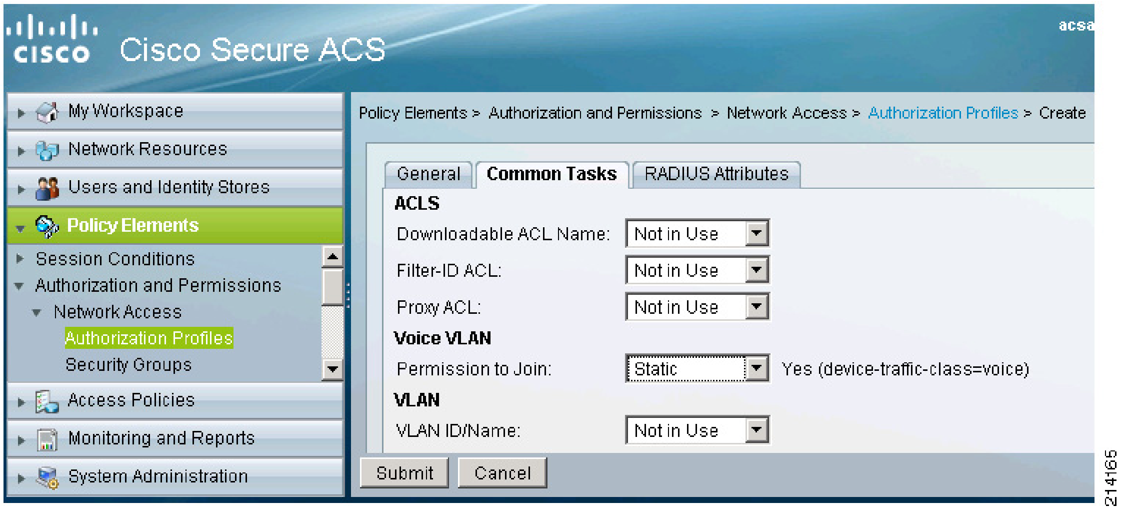
Description: Profile for IP Phones

= Required fields

Step 4 Under the General tab, specify a name for this profile.

Step 5 Click the **Common Tasks** tab, as shown in Figure 14.

Figure 14 Authorization Profiles—Common Tasks



ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Static Yes (device-traffic-class=voice)

VLAN

VLAN ID/Name: Not in Use

Step 6 In the Permission to Join drop-down menu under Voice VLAN, choose **Static**.

This is the setting that causes ACS to send the *device-traffic-class=voice* VSA to the switch when a phone authenticates.

Step 7 Click **Submit**.

Configuring Phones That Support 802.1X

The following sections describe the configuration steps for Unified CM and Cisco ACS that are required to authenticate phones using 802.1X.

Enabling Phones for 802.1X

In this section, the Unified CM administrative interface is used to enable a Cisco IP phone for 802.1X. This section is required only when using 802.1X-capable Cisco IP phones.

Tip **Best Practice Recommendation**—For multiple phones, use the Bulk Administration Tool (BAT). For changing the 802.1X configuration on multiple phones, use BAT inside Unified CM.

Complete the following steps.

Procedure

Step 1 In the Cisco Unified CM Administration window, choose **Device > Phone**.

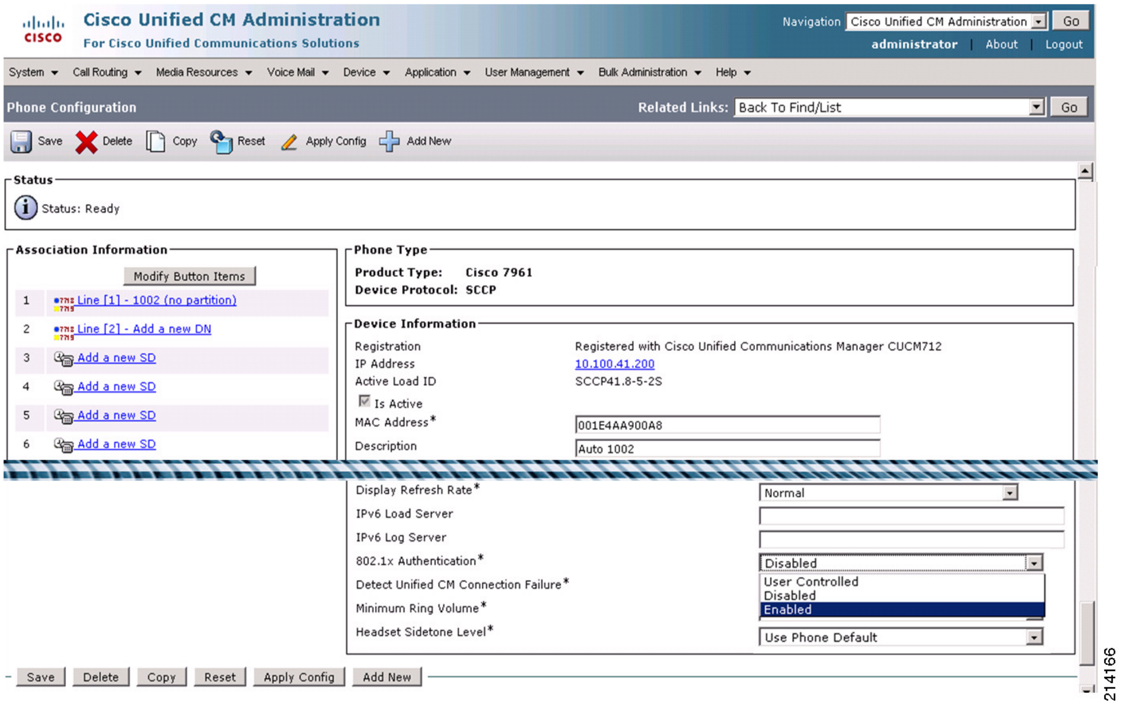
The Find and List Phone window appears.

Step 2 Find and select the phone you wish to enable for 802.1X.

The Phone Configuration window appears.

Step 3 Scroll down to the line titled **802.1x Authentication**. From the drop-down menu, select **Enabled**, as shown in Figure 15.

Figure 15 802.1X Authentication


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
administrator | About | Logout
System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Modify Button Items
214166

Phone Configuration

Status

Status: Ready

Association Information

1 Line [1] - 1002 (no partition)
2 Line [2] - Add a new DN
3 Add a new SD
4 Add a new SD
5 Add a new SD
6 Add a new SD

Phone Type

Product Type: Cisco 7961
Device Protocol: SCCP

Device Information

Registration	Registered with Cisco Unified Communications Manager CUCM712
IP Address	10.100.41.200
Active Load ID	SCCP41.8-5-2S
☑ Is Active	
MAC Address*	001E4AA900A8
Description	Auto 1002
Display Refresh Rate*	Normal
IPv6 Load Server	
IPv6 Log Server	
802.1x Authentication*	Disabled User Controlled Disabled Enabled
Detect Unified CM Connection Failure*	
Minimum Ring Volume*	
Headset Sidetone Level*	Use Phone Default

Step 4 Click **Save** and then **Apply Config** to enable 802.1X on the phone.

Deploying Locally Significant Certificates

In this section, the Unified CM administrative interface is used to install an LSC on an IP phone. This section is required only when using 802.1X-capable Cisco IP phones.

Note To deploy LSCs, Unified CM must first 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.

Complete the following steps.

Procedure

Step 1 In the Cisco Unified CM Administration user interface, choose **Device > Phone**.

The Find and List Phone window displays.

Step 2 Find and select the phone to which a certificate should be deployed.

The Phone Configuration window appears.

Step 3 Scroll down to the section entitled **Certificate Authority Proxy Function (CAPF) Information**.

Step 4 Under Certificate Operation, select **Install/Upgrade**.

Step 5 Under Authentication Mode, select **By Existing Certificate (precedence to LSC)**.

Step 6 Under **Operation Completes By**, enter the date and time the certificate should be deployed.

Step 7 Click **Save** and then **Apply Config** to begin the process of enrolling a certificate for the phone.

Exporting CA Certificates from Unified CM

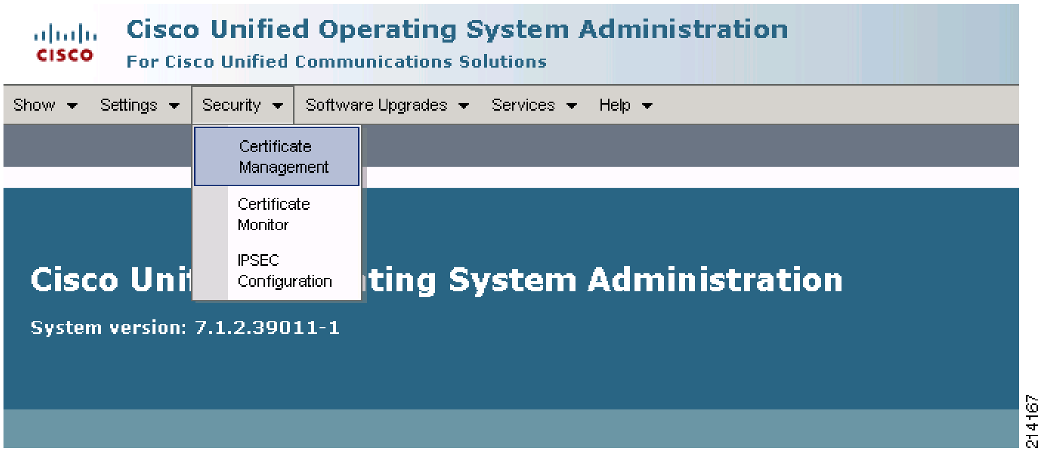
In this section, root CA certificates are exported from Unified CM, to be imported into ACS in the next section. This section is required only when using 802.1X-capable Cisco IP phones.

Complete the following steps.

Procedure

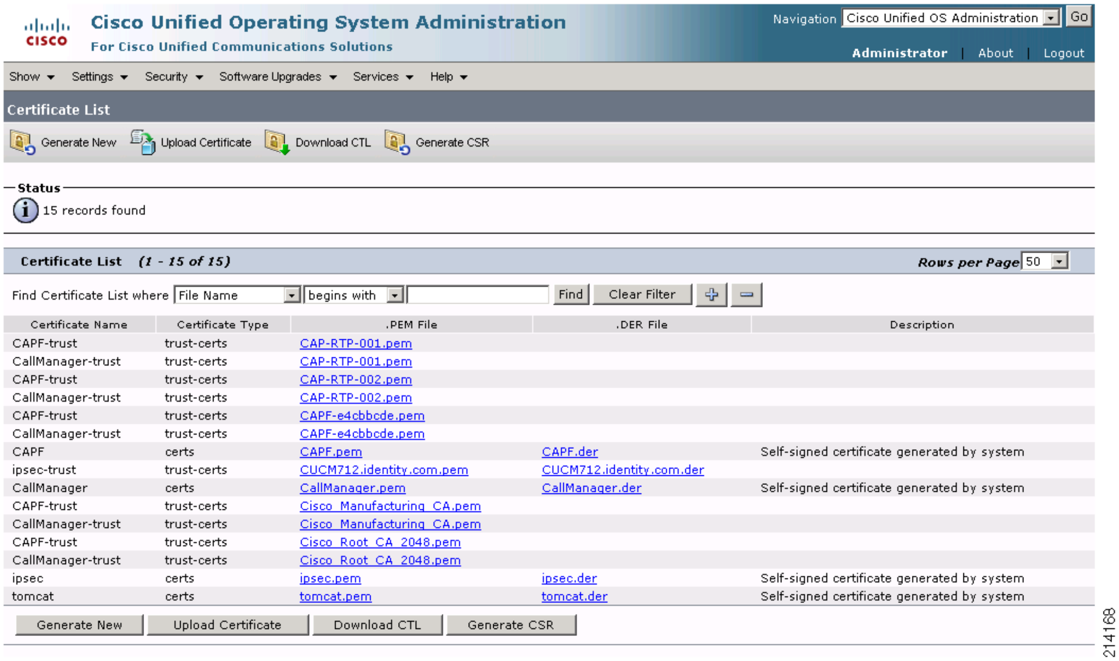
Step 1 In the Cisco Unified Operating System Administration window, choose **Security > Certificate Management**, as shown in Figure 16.

Figure 16 Certificate Management


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate Management
Certificate Monitor
IPSEC Configuration
Cisco Unified Operating System Administration
System version: 7.1.2.39011-1
214167

Step 2 Select **Find** to display all the certificates, as shown in Figure 17.

Figure 17 Certificate List


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
Administrator | About | Logout
Show Settings Security Software Upgrades Services Help
Certificate List
Generate New Upload Certificate Download CTL Generate CSR
Status
Certificate List (1 - 15 of 15)
Rows per Page 50
Find Certificate List where File Name begins with Find Clear Filter
Generate New Upload Certificate Download CTL Generate CSR
214168

15 records found

Certificate Name	Certificate Type	.PEM File	.DER File	Description
CAPF-trust	trust-certs	CAP-RTP-001.pem		
CallManager-trust	trust-certs	CAP-RTP-001.pem		
CAPF-trust	trust-certs	CAP-RTP-002.pem		
CallManager-trust	trust-certs	CAP-RTP-002.pem		
CAPF-trust	trust-certs	CAPF-e4cbbcde.pem		
CallManager-trust	trust-certs	CAPF-e4cbbcde.pem		
CAPF	certs	CAPF.pem	CAPF.der	Self-signed certificate generated by system
ipsec-trust	trust-certs	CUCM712.identity.com.pem	CUCM712.identity.com.der	
CallManager	certs	CallManager.pem	CallManager.der	Self-signed certificate generated by system
CAPF-trust	trust-certs	Cisco_Manufacturing_CA.pem		
CallManager-trust	trust-certs	Cisco_Manufacturing_CA.pem		
CAPF-trust	trust-certs	Cisco_Root_CA_2048.pem		
CallManager-trust	trust-certs	Cisco_Root_CA_2048.pem		
ipsec	certs	ipsec.pem	ipsec.der	Self-signed certificate generated by system
tomcat	certs	tomcat.pem	tomcat.der	Self-signed certificate generated by system

Step 3 For each required certificate, select the name of the certificate in .PEM format and then click **Download**.

Step 4 When prompted, save the certificate.

Step 5 Repeated for each required certificate.

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 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.

Importing CA Certificates into ACS

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

Complete the following steps.

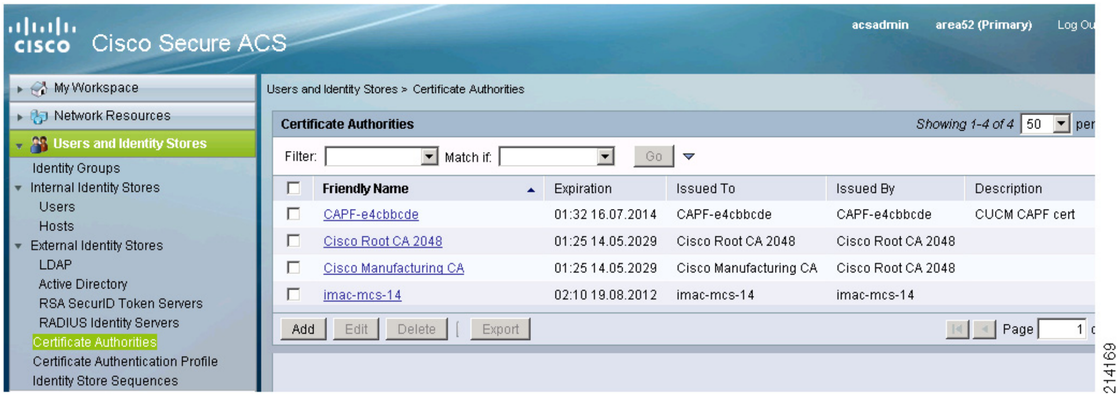
Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation panel, select **Users and Identity Stores > Certificate Authorities**.

The current list of trusted certificate authorities is displayed, as shown in Figure 18.

Figure 18 Certificate Authorities



Users and Identity Stores > Certificate Authorities

Certificate Authorities — Showing 1-4 of 4 | 50 per

Filter: Match if: Go

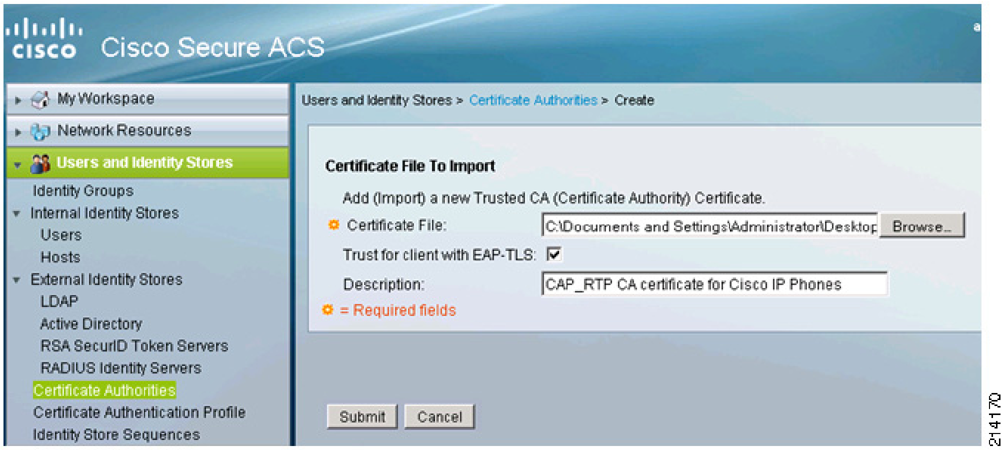
□	Friendly Name	Expiration	Issued To	Issued By	Description
□	CAPF-e4cbbcde	01:32 16.07.2014	CAPF-e4cbbcde	CAPF-e4cbbcde	CUCM CAPF cert
□	Cisco Root CA 2048	01:25 14.05.2029	Cisco Root CA 2048	Cisco Root CA 2048	
□	Cisco Manufacturing CA	01:25 14.05.2029	Cisco Manufacturing CA	Cisco Root CA 2048	
□	imac-mcs-14	02:10 19.08.2012	imac-mcs-14	imac-mcs-14	

Step 3 Select **Add**.

Step 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** (see Figure 19).

Optionally, enter a description for this certificate.

Figure 19 Certificate File to Import



Users and Identity Stores > Certificate Authorities > Create

Certificate File To Import

Add (Import) a new Trusted CA (Certificate Authority) Certificate.

✱ Certificate File: C:\Documents and Settings\Administrator\Desktop

Trust for client with EAP-TLS: ☑

Description: CAP_RTP CA certificate for Cisco IP Phones

✱ = Required fields

Step 5 Click **Submit**.

Repeat for each of the certificates exported from the Unified CM.

Configuring an 802.1X Access Service

In this section, an 802.1X access service is created in Cisco Secure ACS. This access service is 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.

Creating the 802.1X Access Service and Protocol Filter

To create the 802.1X access service and protocol filter, complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

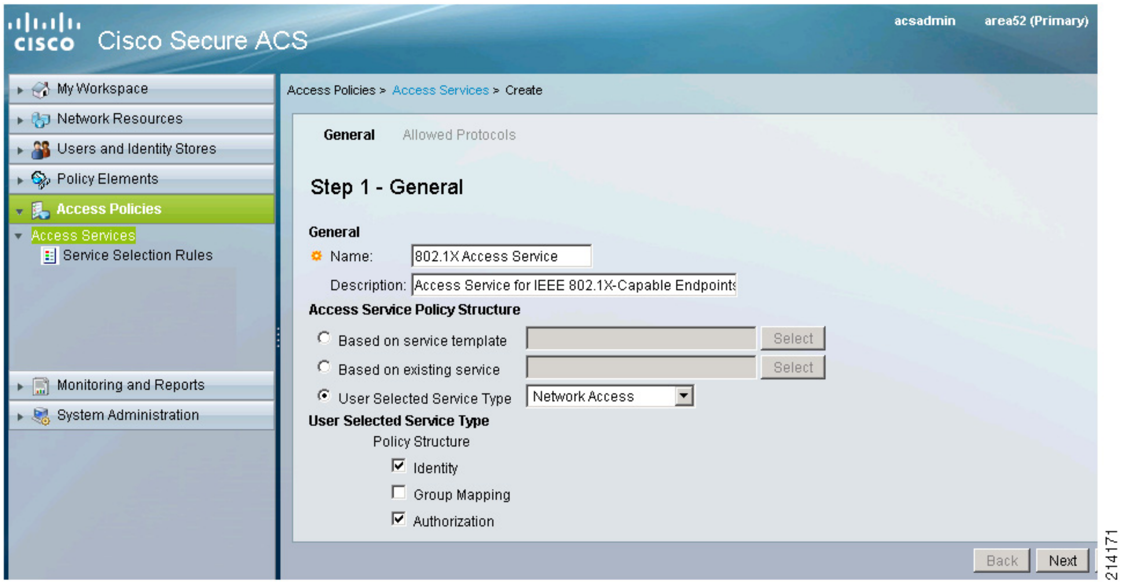
Step 2 In the left navigation column, under **Access Policies**, click **Access Services**.

The list of existing access services appears.

Step 3 At the bottom of the right windowpane, click **Create**.

The window shown in Figure 20 appears.

Figure 20 Access Services—General



Step 1 - General

General

Name: 802.1X Access Service

Description: Access Service for IEEE 802.1X-Capable Endpoint

Access Service Policy Structure

○ Based on service template

○ Based on existing service

● User Selected Service Type: Network Access

User Selected Service Type

Policy Structure

☑ Identity

☐ Group Mapping

☑ Authorization

Step 4 On the General screen, do the following:

a. In the Name field under General, specify a name for this service and optionally, a description.

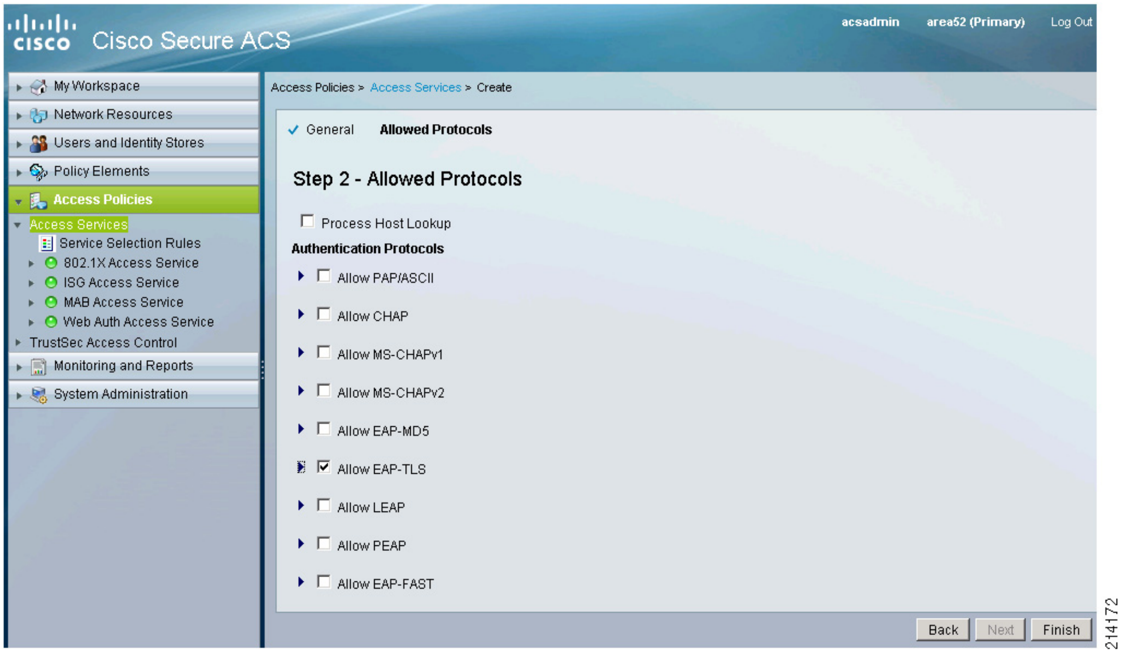
b. Under Access Service Policy Structure, select **User Selected Service Type** and in the drop-down menu, choose **Network Access**.

c. Under User Selected Service Type/Policy Structure, select **Identity** and **Authorization.**

d. Click **Next**.

The window shown in Figure 21 appears.

Figure 21 Access Services—Allowed Protocols



Step 2 - Allowed Protocols

□ Process Host Lookup

Authentication Protocols

- □ Allow PAP/ASCII
- □ Allow CHAP
- □ Allow MS-CHAPv1
- □ Allow MS-CHAPv2
- □ Allow EAP-MD5
- ☑ Allow EAP-TLS
- □ Allow LEAP
- □ Allow PEAP
- □ Allow EAP-FAST

Step 5 On the Allowed Protocols screen, do the following:

a. Deselect **Process Host Lookup**.

b. Select **Allow EAP-TLS**.

c. If other devices, such as laptops, use a different EAP method, select that method as well.

d. Click **Finish.**

e. When you are prompted to modify the service selection policy, click **No**.

ACS 5.x attempts EAP-TLS before less secure methods such as EAP-MD5. Earlier versions of Cisco ACS, however, may attempt EAP-MD5 first if it is enabled. Because the phone attempts whatever method ACS requests, even if it does not have a password, do not enable EAP-MD5 in the access service 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 Cisco ACS.

Configuring 802.1X Identity Policy

To configure an 802.1X identity policy, complete the following steps.

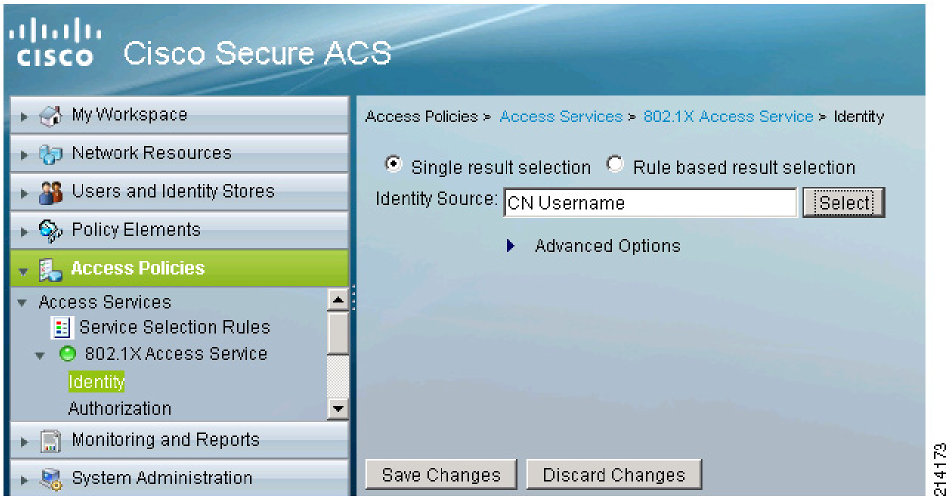
Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, expand **Access Policies** > **802.1X Access Service** and click **Identity**.

The window shown in Figure 22 appears.

Figure 22 Access Policies—Identity



Access Policies > Access Services > 802.1X Access Service > Identity

● Single result selection ○ Rule based result selection

Identity Source: CN Username

Step 3 On the 802.1X Access Service Identity policy window, do the following:

a. Select **Select one result**.

b. For Identity Source, choose **CN Username**.

c. Click **Save Changes**.

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

Creating 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.

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, do the following:

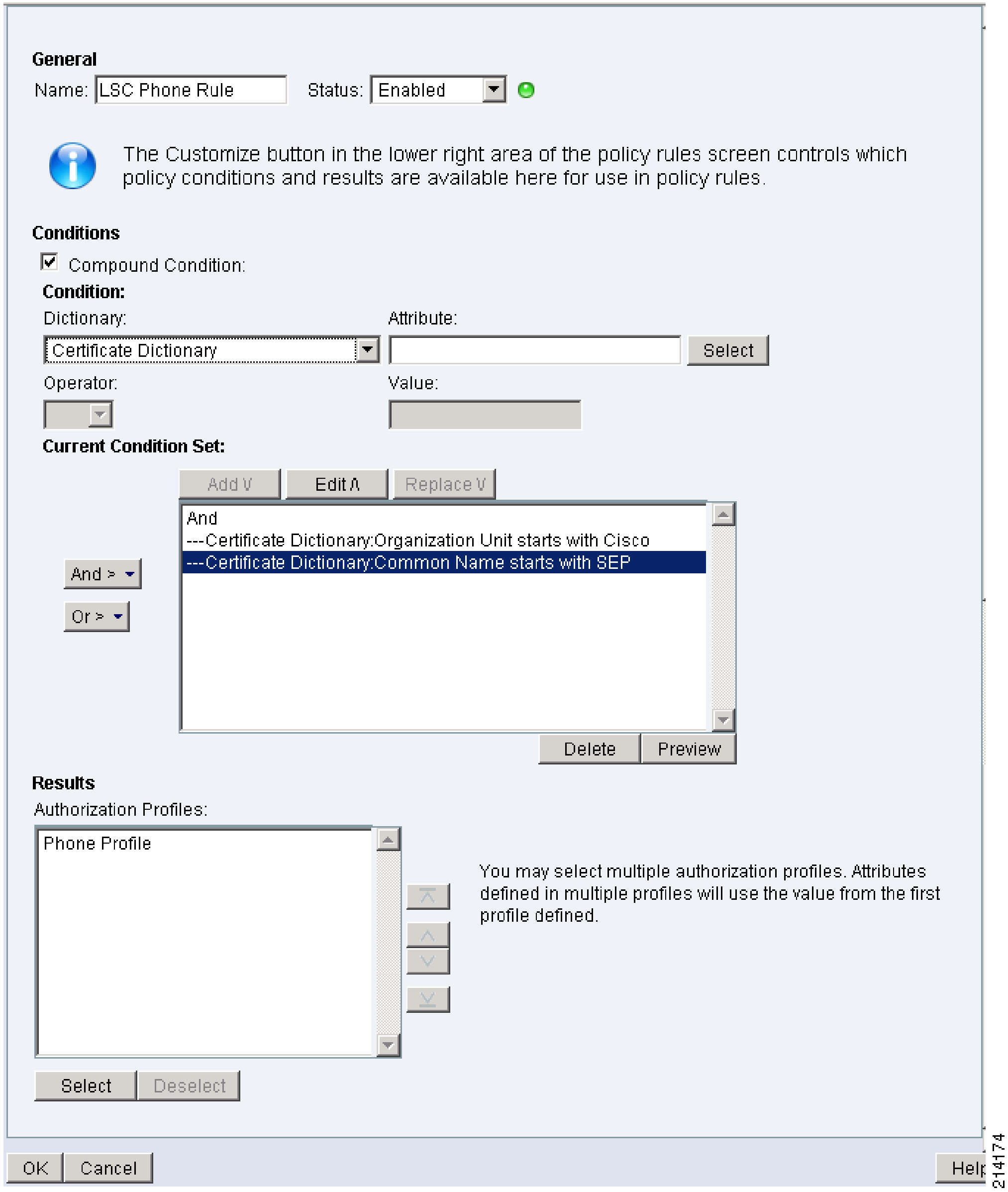
a. Expand **Access Policies** to list the access services.

b. Expand **802.1X Access Service** and click **Authorization**.

c. Click **Create**.

The window shown in Figure 23 appears.

Figure 23 Creating an LSC Authorization Rule



General

Name: LSC Phone Rule Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Compound Condition:

Condition:

Dictionary: Certificate Dictionary

Attribute:

Operator:

Value:

Current Condition Set:

And
---Certificate Dictionary:Organization Unit starts with Cisco
---Certificate Dictionary:Common Name starts with SEP

Results

Authorization Profiles:

Phone Profile

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 3 In the configuration window, do the following:

a. Specify a name for the LSC authorization rule and select **Compound Condition**.

b. Under Dictionary, select **Certificate Dictionary**.

c. Under Attribute, select **Organization Unit**.

d. Under Operation, select **starts with.**

e. Under Value, enter the OU for your LSC.

The actual value depends on your CAPF configuration. In this example, the OU for this CAPF starts with *Cisco*.

f. Click **Add V** to add 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.

g. Click **And >** to the left of the Current Condition Set.

h. Under Dictionary, select Certificate Dictionary.

i. Under Attribute, select **Common Name**.

j. Under Operation, select **starts with.**

k. Under Value, enter **SEP**.

As discussed in the "Using Certificates" section on page 17, the Common Name for Cisco IP phones always begins with *SEP* for LSCs. Click **Add V** to add this condition to the Current Condition Set.

l. Under Results, click **Select**.

A list of all available authorization profiles is displayed.

m. Select the Phone Profile that was created in the "Creating a Phone Authorization Profile in Cisco Secure ACS" section on page 36 and click **OK**.

n. Click **OK** to finish the LSC authorization rule.

Step 4 Click **Save Changes**.

Creating a 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.

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, do the following:

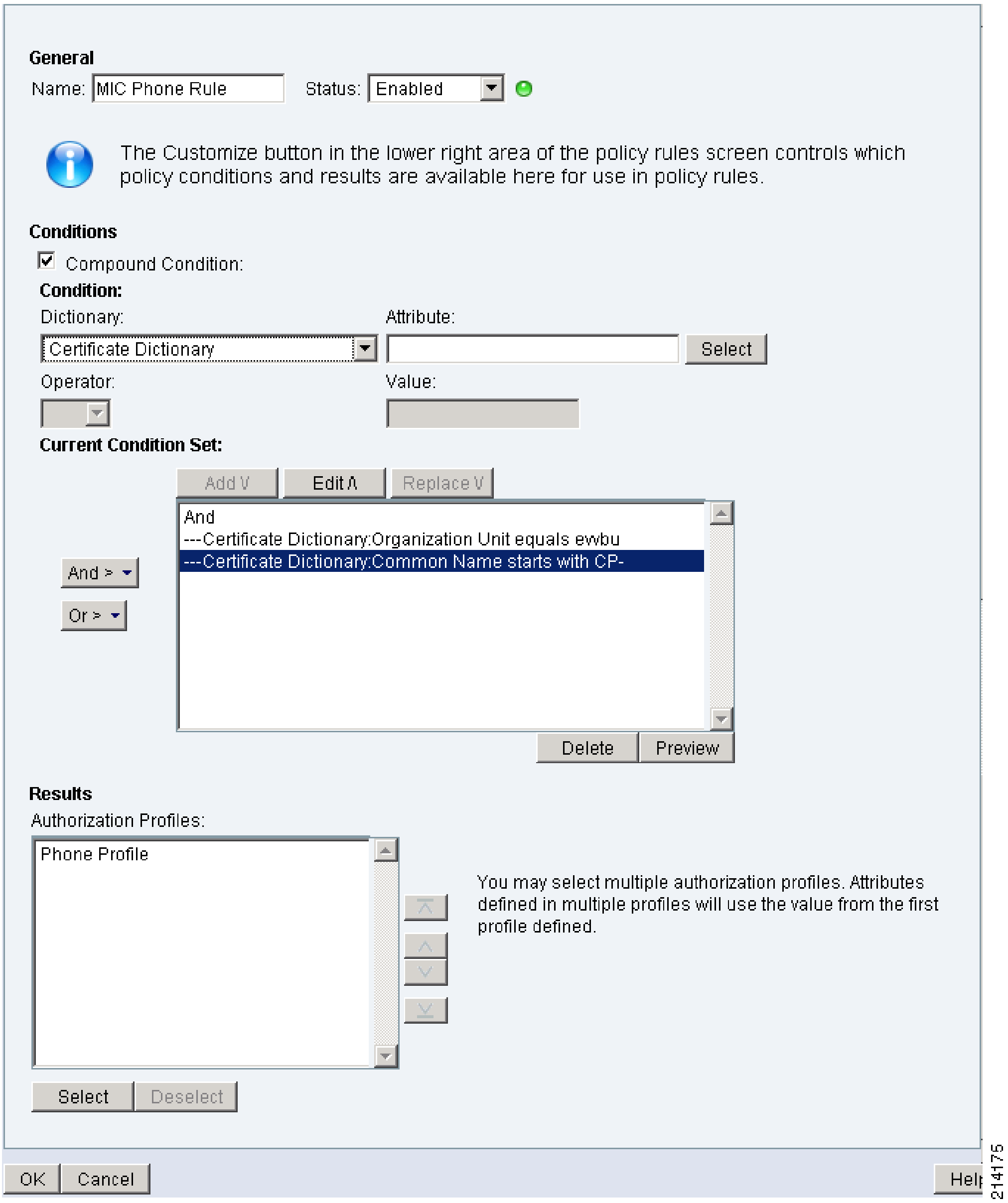
a. Expand **Access Policies** to list the access services.

b. Expand **802.1X Access Service** and click **Authorization**.

c. Click **Create**.

The window shown in Figure 24 appears.

Figure 24 Creating a MIC Authorization Rule



General

Name: MIC Phone Rule Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Compound Condition:

Condition:

Dictionary: Certificate Dictionary

Attribute:

Operator:

Value:

Current Condition Set:

```
And
---Certificate Dictionary:Organization Unit equals ewbu
---Certificate Dictionary:Common Name starts with CP-
```

Results

Authorization Profiles:

Phone Profile

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 3 In the configuration window, do the following:

a. Specify a name for the MIC authorization rule and select **Compound Condition**.

b. Under Dictionary, select **Certificate Dictionary**.

c. Under Attribute, select **Organization Unit**.

d. Under Operation, select **equals.**

e. Under Value, enter **evvbu**.

f. Click **Add V** to add 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.

g. Click **And >** to the left of the Current Condition Set.

h. Under Dictionary, select **Certificate Dictionary**.

i. Under Attribute, select **Common Name**.

j. Under Operation, select **starts with.**

k. Under Value, enter **CP-**.

As discussed in the "Using Certificates" section on page 17, the common name for Cisco IP phones always begins with "CP-" for MICs.

l. Click **Add V** to add the *CP-* condition to the Current Condition Set.

m. Under Results, click **Select**.

A list of all available authorization profiles is displayed.

n. Select the Phone Profile that you created and click **OK**.

o. Click **OK** to finish the MIC authorization rule.

Step 4 Click **Save Changes**.

Validating the 802.1X Phone Authorization Policy for ACS

To validate the 802.1X phone authorization policy for ACS, complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

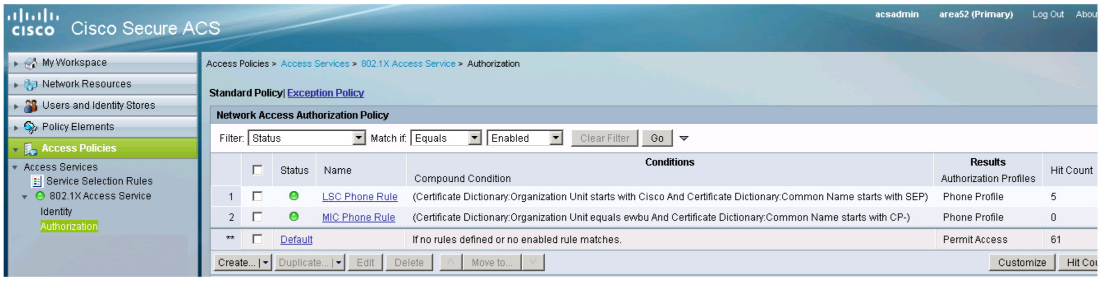
Step 2 In the left navigation column, do the following:

a. Expand **Access Policies** to list the access services.

b. Expand **802.1X Access Service** and click **Authorization**.

The window shown in Figure 25 appears with a summary of the configured authorization rules.

Figure 25 Validating the 802.1X Authorization Policy



	☐	Status	Name	Conditions Compound Condition	Results Authorization Profiles	Hit Count
1	☐	●	LSC Phone Rule	(Certificate Dictionary:Organization Unit starts with Cisco And Certificate Dictionary:Common Name starts with SEP)	Phone Profile	5
2	☐	●	MIC Phone Rule	(Certificate Dictionary:Organization Unit equals ewbu And Certificate Dictionary:Common Name starts with CP-)	Phone Profile	0
**	☐		Default	If no rules defined or no enabled rule matches.	Permit Access	61

Step 3 Verify that the LSC and/or MIC rules that you created have a Result of **Phone Profile**.

Step 4 Verify that the Default rule at the bottom of the table has a Result of **Permit Access**.

This is the rule that is matched for data devices that authenticate using 802.1X.

Creating an 802.1X Service Selection Rule

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

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

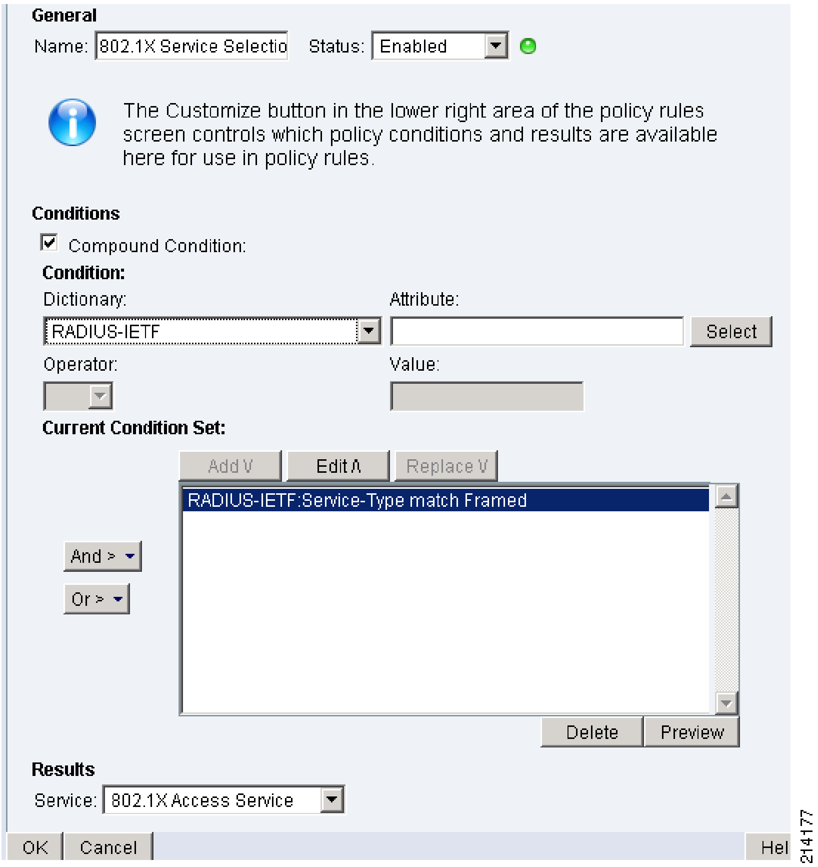
Step 2 In the left navigation column, under Access Policies, click **Service Selection**.

The list of existing service selection rules appears.

Step 3 At the bottom of the right windowpane, click **Create**.

The Service Selection rule dialog box appears, as shown in Figure 26, and should be filled out as described in the following steps.

Figure 26 Creating an 802.1X Service Selection Rule



General

Name: 802.1X Service Selectio Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Compound Condition:

Condition:

Dictionary: RADIUS-IETF

Attribute:

Operator:

Value:

Current Condition Set:

RADIUS-IETF:Service-Type match Framed

Results

Service: 802.1X Access Service

Step 4 In the configuration window, do the following:

a. Specify a name for the rule; *802.1X Service Selection* is used here.

b. Under Conditions, select **Compound Condition**.

c. Under Dictionary, choose **RADIUS-IETF**.

d. Under Attribute, select **Service-Type**.

e. Under Operator, choose **match**.

f. Under Value, select **Framed**.

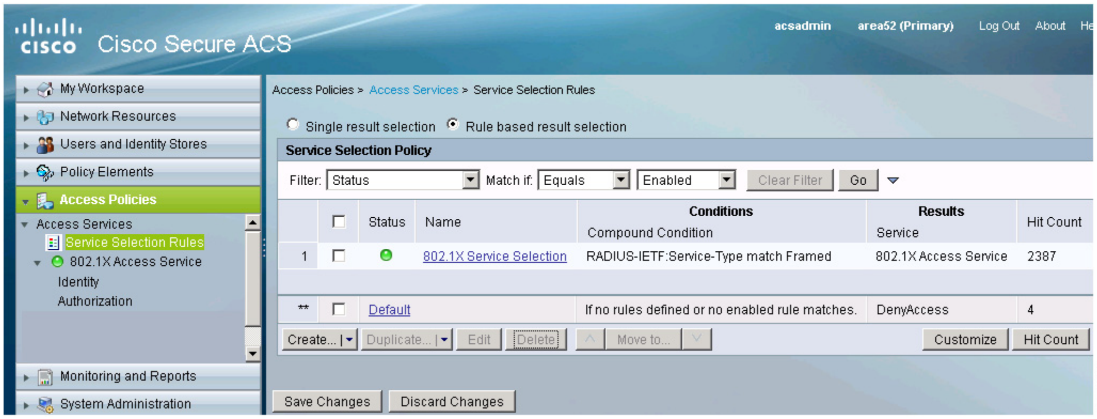
g. Under Current Condition Set, click **Add**.

h. Under Results, select the access service that was created in the previous step (*802.1X Access Service*).

i. Click **OK**.

The Service Selection rule summary appears with the new rule, as shown in Figure 27.

Figure 27 Service Selection Policy



Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled

	☐	Status	Name	Conditions Compound Condition	Results Service	Hit Count
1	☐	●	802.1X Service Selection	RADIUS-IETF:Service-Type match Framed	802.1X Access Service	2387
**	☐		Default	If no rules defined or no enabled rule matches.	DenyAccess	4

Step 5 Click **Save Changes**.

Configuring Phones for MAB (Phones without 802.1X Support)

The following sections describe the configuration steps for Unified CM and ACS that are required to authenticate phones using MAB.

Entering 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 required only for non-802.1X-capable Cisco IP phones.

Tip **Best Practice Recommendation—**For multiple phones, use import/export tools. To enter MAC addresses for multiple phones, use the export function in Unified CM to extract the MAC addresses of registered IP phones that are not 802.1X-capable. When exported, the MAC addresses can be formatted and entered into ACS using the import function.

Complete the following steps.

Procedure

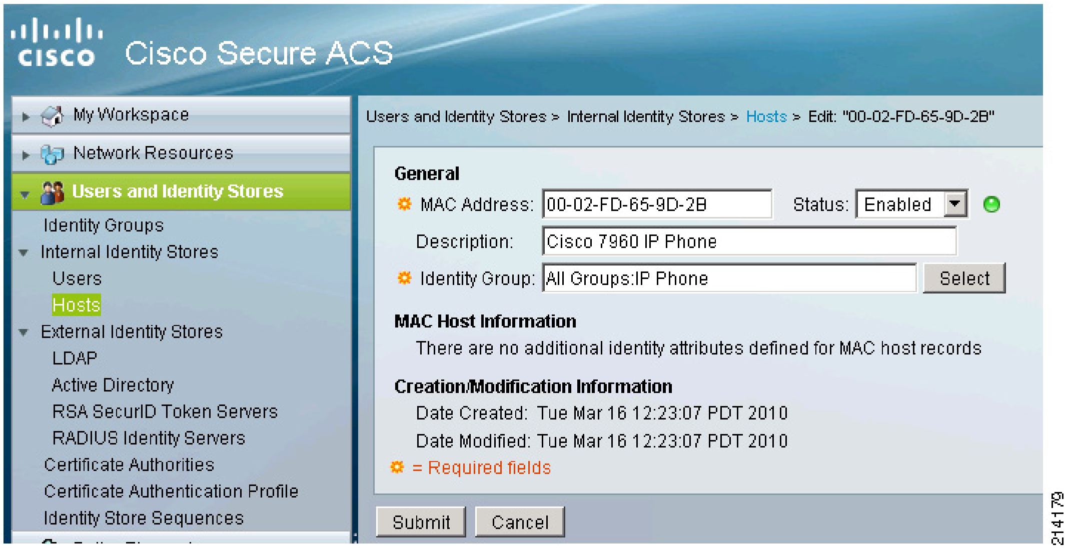
Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, under Users and Identity Stores, expand **Internal Identity Stores** and select **Hosts**.

Step 3 Click **Create**.

The window shown in Figure 28 appears.

Figure 28 Hosts



Users and Identity Stores > Internal Identity Stores > Hosts > Edit: "00-02-FD-65-9D-2B"

General

MAC Address: 00-02-FD-65-9D-2B Status: Enabled

Description: Cisco 7960 IP Phone

Identity Group: All Groups:IP Phone

MAC Host Information

There are no additional identity attributes defined for MAC host records

Creation/Modification Information

Date Created: Tue Mar 16 12:23:07 PDT 2010

Date Modified: Tue Mar 16 12:23:07 PDT 2010

= Required fields

Step 4 Enter the MAC address of the phone and assign it to an Identity Group that identifies this device as a phone.

Step 5 Click **Submit**.

Configuring an MAB Access Service

In this section, MAB access service is created in Cisco Secure ACS. This access service is 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.

Creating the MAB Access Service and Protocol Filter

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

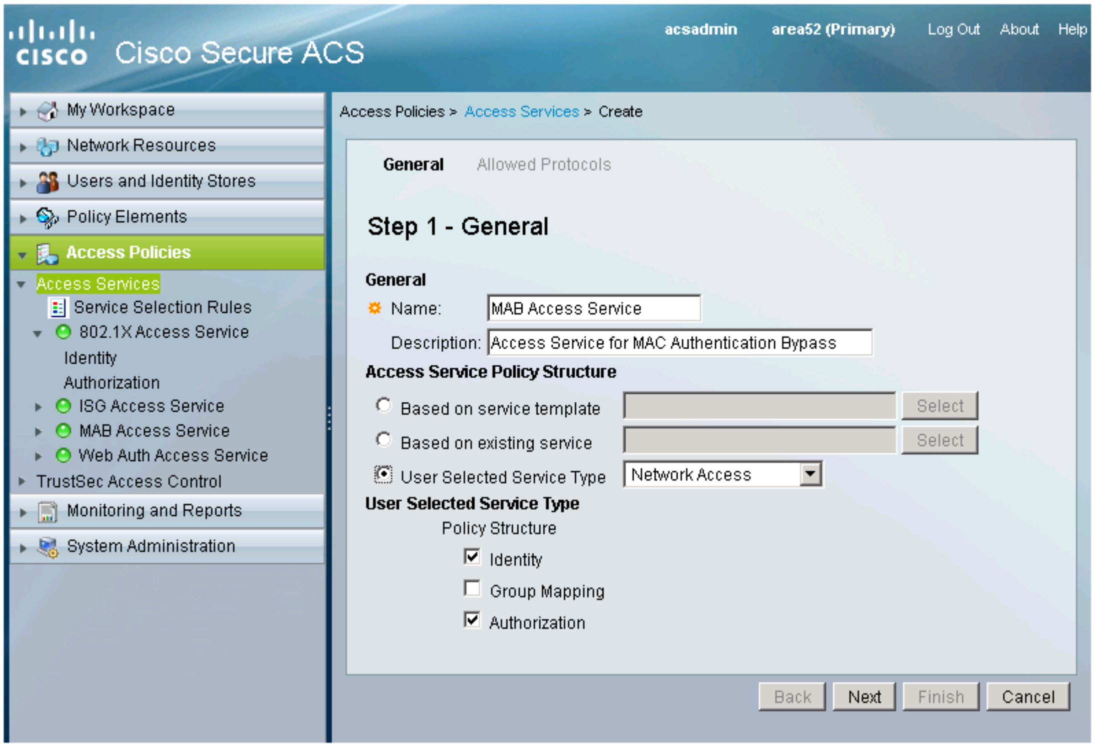
Step 2 In the left navigation column, under Access Policies, click **Access Services**.

The list of existing access services appears.

Step 3 At the bottom of the right windowpane, click **Create**.

The window shown in Figure 29 appears.

Figure 29 Access Services—General



Step 1 - General

General

Name: MAB Access Service

Description: Access Service for MAC Authentication Bypass

Access Service Policy Structure

○ Based on service template

○ Based on existing service

● User Selected Service Type: Network Access

User Selected Service Type

Policy Structure

☑ Identity

□ Group Mapping

☑ Authorization

Step 4 On the General screen, do the following:

a. Under General, specify a name for this service and optionally, a description.

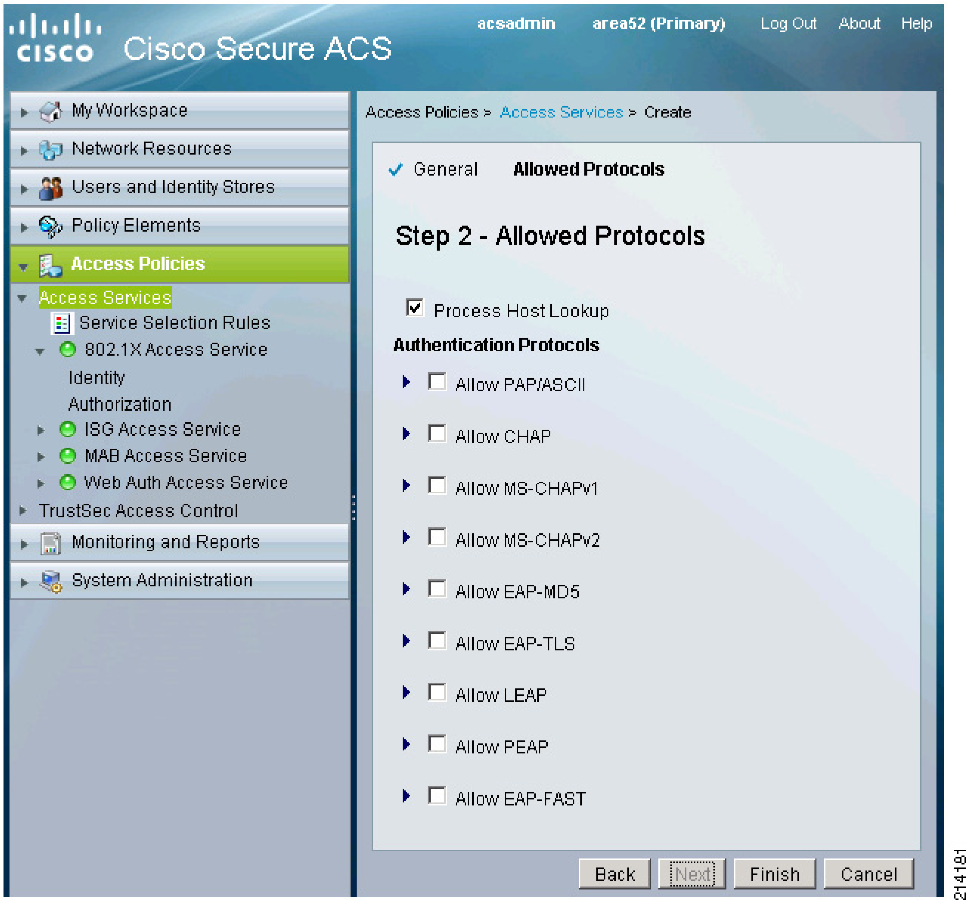
b. Under Access Service Policy Structure, select **User Selected Service Type** and in the drop-down menu, choose **Network Access**.

c. Under User Selected Service Type/Policy Structure, select **Identity** and **Authorization.**

d. Click **Next**.

The window shown in Figure 30 appears.

Figure 30 Access Services—Allowed Protocols



Step 2 - Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

- ☐ Allow PAP/ASCII
- ☐ Allow CHAP
- ☐ Allow MS-CHAPv1
- ☐ Allow MS-CHAPv2
- ☐ Allow EAP-MD5
- ☐ Allow EAP-TLS
- ☐ Allow LEAP
- ☐ Allow PEAP
- ☐ Allow EAP-FAST

Step 5 On the Allowed Protocols screen, select **Process Host Lookup** and click **Finish.**

Step 6 When you are prompted to modify the service selection policy, click **No**.

Configuring the MAB Identity Policy

Complete the following steps.

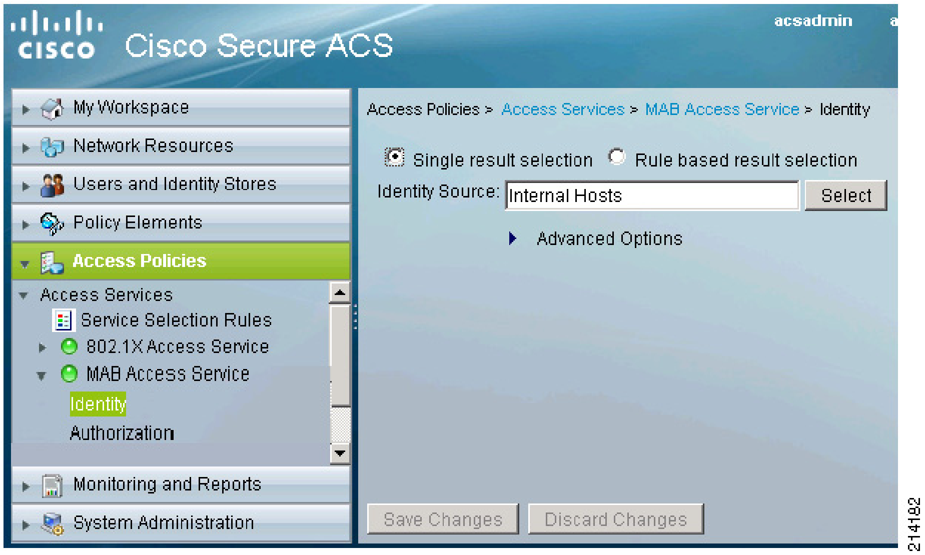
Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, expand **Access Policies** > **MAB Access Service** and click **Identity**.

The window shown in Figure 31 appears.

Figure 31 MAB Access Service—Identity



Access Policies > Access Services > MAB Access Service > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Hosts

Step 3 In the 802.1X Access Service Identity policy window, do the following:

a. Select **Select one result**.

b. For Identity Source, choose **Internal Hosts**.

c. Click **Save Changes**.

Creating the 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.

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

Step 2 In the left navigation column, do the following:

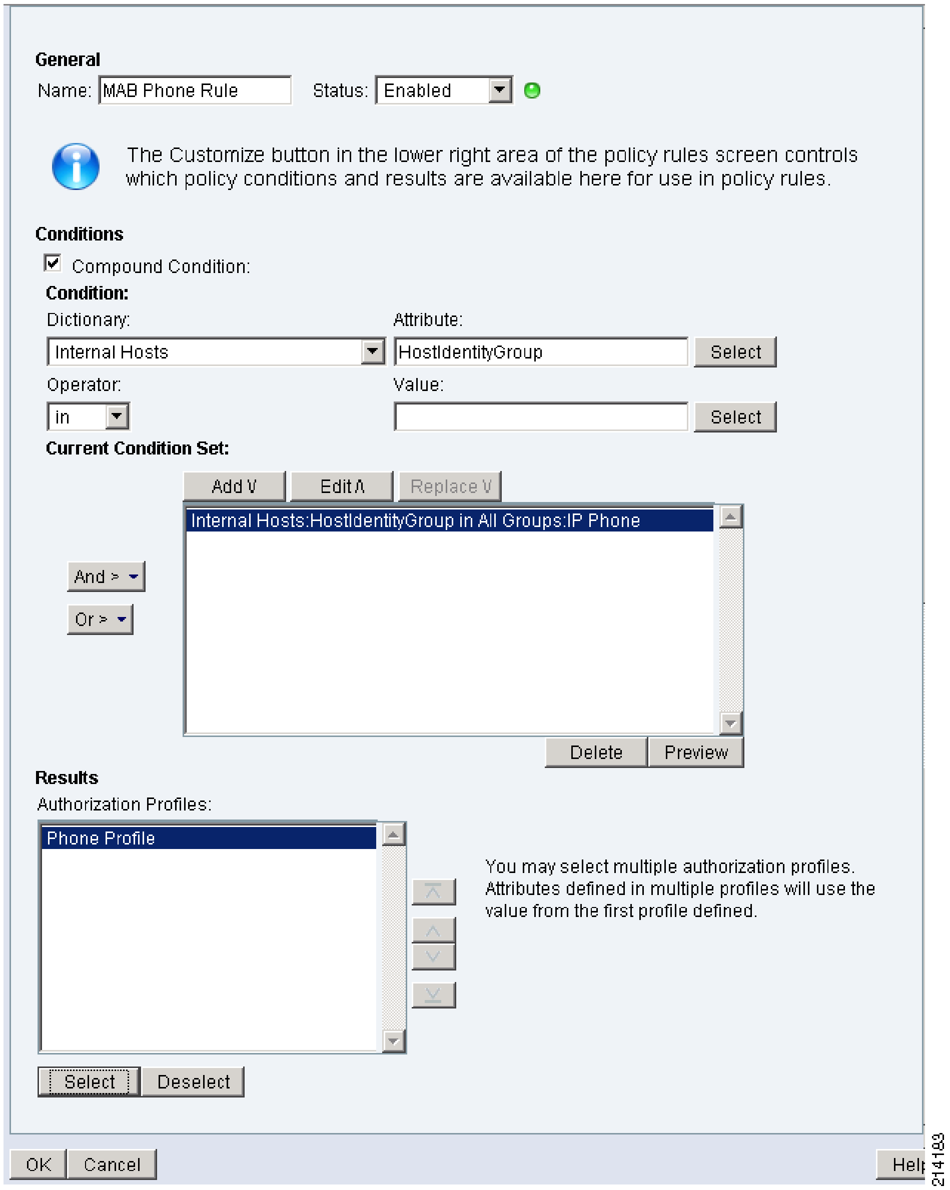
a. Expand **Access Policies** to list the access services.

b. Expand **MAB** and click **Authorization**.

c. Click **Create**.

The window shown in Figure 32 appears.

Figure 32 Creating the Phone MAB Authorization Rule



General

Name: MAB Phone Rule Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Compound Condition:

Condition:

Dictionary: Internal Hosts

Attribute: HostIdentityGroup

Operator: in

Value:

Current Condition Set:

Internal Hosts:HostIdentityGroup in All Groups:IP Phone

Results

Authorization Profiles:

Phone Profile

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.

Step 3 In the configuration, do the following:

a. Specify a name for the MAB authorization rule; *MAB Phone Rule* is used here.

b. Select **Compound Condition**.

c. Under Dictionary, select Internal Hosts.

d. Under Attribute, select **HostIdentityGroup**.

e. Under Operation, select **in.**

f. Under Value, enter the phone group name that was assigned to the phone MAC in the Internal Host database in the "Configuring Phones for MAB (Phones without 802.1X Support)" section on page 52.

The group used in this document is *All Groups:IP Phone*.

g. Click **Add V** to add this condition to the Current Condition Set.

   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.

h. Click **And >** to the left of the Current Condition Set.

i. Under Results, click **Select**.

   A list of all available authorization profiles is displayed.

j. Select the Phone Profile that was created in the "Creating a Phone Authorization Profile in Cisco Secure ACS" section on page 36 and click **OK**.

k. Click **OK** to finish the MAB authorization rule.

Step 4 Click **Save Changes**.

Validating the MAB Phone Authorization Policy for ACS

Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

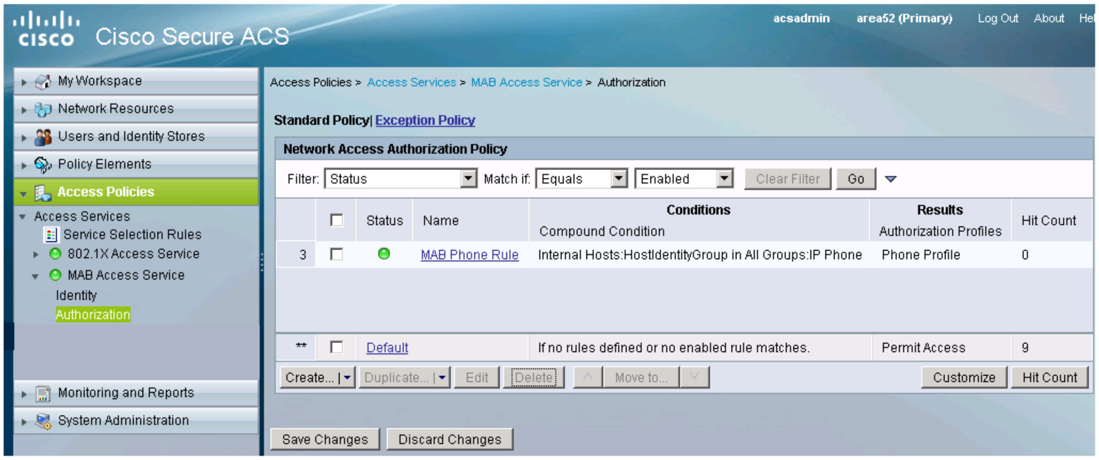
Step 2 In the left navigation column, do the following:

a. Expand **Access Policies** to list the access services.

b. Expand **MAB Access Service** and click **Authorization**.

   The window shown in Figure 33 appears with a summary of the configured authorization rules.

Figure 33 Access Policies—Authorization



Access Policies > Access Services > MAB Access Service > Authorization

Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	□	Status	Name	Conditions Compound Condition	Results Authorization Profiles	Hit Count
3	□	●	MAB Phone Rule	Internal Hosts:HostIdentityGroup in All Groups:IP Phone	Phone Profile	0
**	□		Default	If no rules defined or no enabled rule matches.	Permit Access	9

Step 3 Verify that MAB Phone Rule that you created have a Result of **Phone Profile**.

Step 4 Verify that the Default rule at the bottom of the table has a Result of **Permit Access**.

This is the rule that is matched for data devices that authenticate using MAB.

Creating 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. Complete the following steps.

Procedure

Step 1 Open the Cisco Secure ACS Management interface.

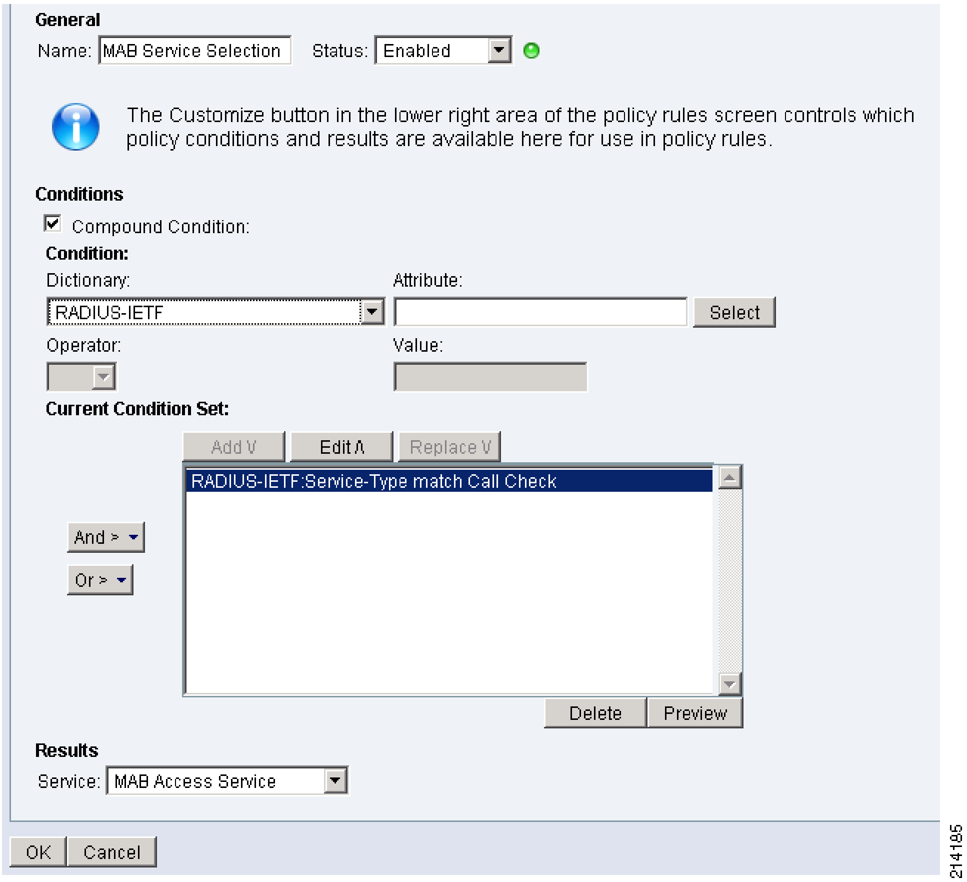
Step 2 In the left navigation column, under Access Policies, click **Service Selection**.

The list of existing service selection rules appears.

Step 3 At the bottom of the right windowpane, click **Create**.

The Service Selection rule dialog box appears, as shown in Figure 34, and should be filled out as described in the following steps.

Figure 34 Service Selection Rule Dialog Box



General

Name: MAB Service Selection Status: Enabled ●

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Compound Condition:

Condition:

Dictionary: RADIUS-IETF

Attribute:

Operator:

Value:

Current Condition Set:

RADIUS-IETF:Service-Type match Call Check

Results

Service: MAB Access Service

Step 4 In the configuration window, do the following:

a. Specify a name for the rule (MAB Service Selection is used here).

b. Under Conditions, select **Compound Condition**.

c. Under Dictionary, choose **RADIUS-IETF**.

d. Under Attribute, select **Service-Type**.

e. Under Operator, choose **match**.

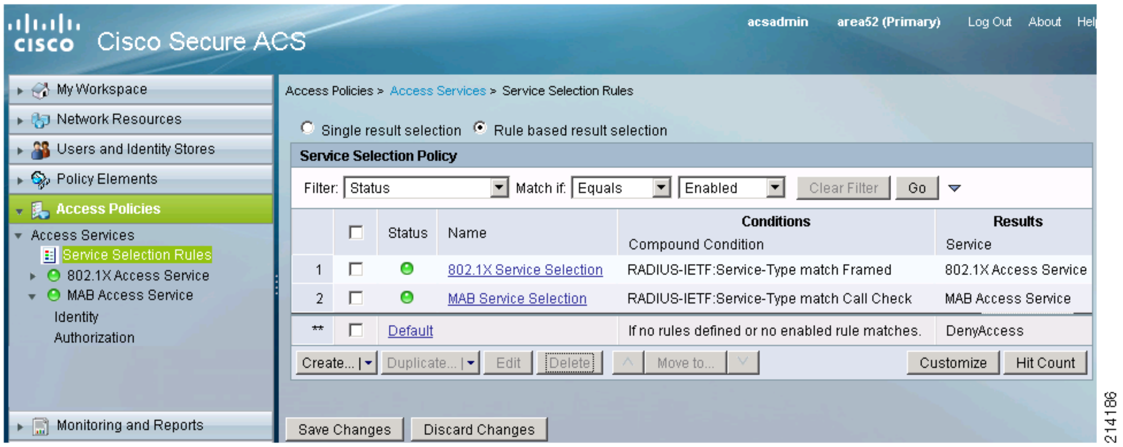
f. Under Value, select **Call Check**.

g. Under Current Condition Set, click **Add**.

h. Under Results, select the access service that was created in the previous step (*MAB Access Service*)., and click **OK**.

The Service Selection rule summary appears with the new rule, as shown in Figure 35.

Figure 35 Service Selection Rules



		Status	Name	Conditions Compound Condition	Results Service
1	□	●	802.1X Service Selection	RADIUS-IETF:Service-Type match Framed	802.1X Access Service
2	□	●	MAB Service Selection	RADIUS-IETF:Service-Type match Call Check	MAB Access Service
**	□		Default	If no rules defined or no enabled rule matches.	DenyAccess

Step 5 Click **Save Changes**.

Configuring the Switch (All Phone Authentication Types)

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

Verifying 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 BPDU Guard, may also be enabled. The following is a working example:

```
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 802.1X.

Configuring 802.1X and MAB for IP Telephony

A basic configuration of 802.1X and MAB includes global AAA settings, global RADIUS settings, global 802.1X settings, and interface 802.1X settings. Table 8 summarizes these settings. An example of a working configuration appears at the end of this section.

Table 8 Cisco IOS Software 802.1X Configuration

Cisco IOS Software AAA Settings for 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 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 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 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 the "Configuring Phones That Support 802.1X" section on page 38.
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 the "Configuring Phones That Support 802.1X" section on page 38.
Cisco IOS Software 802.1X Global Settings	
dot1x system-auth-control	Globally enables 802.1X port-based access control
Cisco IOS Software 802.1X Interface Settings	

Table 8 Cisco IOS Software 802.1X Configuration

`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 MAB as a fallback to 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 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 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 802.1X supplicant present, use the following formula: tx-period * (max-reauth-req +1).

The following example shows a basic 802.1X configuration that supports IP telephony using MDA. To give MAB devices faster network access, the 802.1X timeout using the configuration below is 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 802.1X on Cisco IOS Software, see the Identity-Based Networking Services (IBNS) configuration guide at http://www.cisco.com/go/trustsec.

Monitoring IP Telephony in an 802.1X Environment

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

Monitoring Sessions from the CLI

The most comprehensive CLI command for monitoring IP phones in an IEEE-802.1X enabled network is the **show authentication sessions** command. Following are examples:

Example 1 802.1X-Authenticated Phone

In the following output, you see one authenticated session for an 802.1X-authenticated Cisco IP phone. In this case, there is no data device plugged in behind the phone. Key fields are highlighted in bold. Note that you can determine that this phone used an LSC to authenticate because 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 2 802.1X-Authenticated Data Device Plugged in to MAB-Authenticated Phone

In the following output, you see two sessions on interface fastEthernet 2/47: an 802.1X-authenticated data device in the DATA domain, with the key fields highlighted in bold in the top half of the output; and a MAB-authenticated phone in the VOICE domain, with the key fields highlighted in bold in the lower half of the output.

```
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 command for monitoring the link state of the second port of the phone is **show cdp neighbors detail**. Note that even though the Cisco 7961 is 802.1X-capable and the Cisco 7960 is not, both phones can use CDP to accurately report the status of the second port. Following are examples:

Example 3 Reported Link State with No Device Connected Behind the IP Phone

As is shown in the bolded 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 the IP Phone.

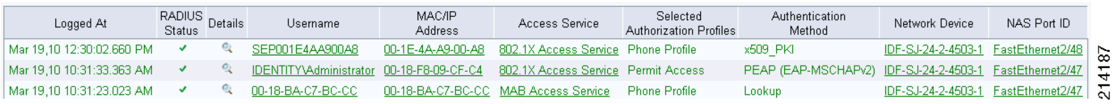
As is shown in the bolded section below, the phone is reporting that its second port is up; the data device is connected.

```
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):
```

Monitoring Sessions from ACS

Use the reporting capabilities on Cisco Secure ACS to verify the session details. The output shown in Figure 36 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.

Figure 36 ACS Report



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

Troubleshooting IP Telephony in an 802.1X-Enabled Environment

Table 9 summarizes some common problems encountered when configuring IP telephony in an 802.1X-enabled environment.

Table 9 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.

Table 9 IP Telephony Troubleshooting (continued)

Port err-disables when PC is connected behind phone	• Phone did not pass 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 • Session from previously connected data device was not properly cleared (that is, the link state issue)	• 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. • Implement a link state solution; for example, CDP Enhancement for Second Port Disconnect, inactivity timer.
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.
802.1X-capable Cisco IP phones are authenticated by MAB	The phone is not enabled for 802.1X by default	Use Unified CM to enable the phone for 802.1X.
Cisco IP phone fails 802.1X	ACS requested EAP-MD5 instead of EAP-TLS and the phone has no password by default	Configure Cisco ACS to request EAP-TLS when authenticating IP phones.

References

TrustSec 1.99 Documents

- Wired 802.1X Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Dot1X_Deployment/Dot1x_Dep_Guide.html
- IP Telephony for 802.1X Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/IP_Tele/IP_Telephony_DIG.html
- MAC Authentication Bypass Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/MAB/MAB_Dep_Guide.html
- TrustSec Phased Deployment Configuration Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Phased_Deploy/Phased_Dep_Guide.html
- Local WebAuth Deployment Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/WebAuth/WebAuth_Dep_Guide.html
- Scenario-Based TrustSec Deployments Application Note—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Scenario_based_AppNote/Scenario_based_AN.html

- TrustSec 1.99 Deployment Note: FlexAuth Order, Priority, and Failed Authentication— http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/FlexAuthNote/flexauth-note.html
- TrustSec Planning and Deployment Checklist— http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/TrustSec_Checklist/trustsec-199_checklist.html

Related Documents

- Configuring WebAuth on the Cisco Catalyst 3750 Series Switches— http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750/software/release/12.2_55_se/configuration/guide/sw8021x.html
- Configuring WebAuth on the Cisco Catalyst 4500 Series Switches— http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst4500/12.2/53SG/configuration/webauth.html
- Configuring WebAuth on the Cisco Catalyst 6500 Series Switches— http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html
- Cisco IOS Firewall authentication proxy— http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0.shtml
- WebAuth with Cisco Wireless LAN Controllers— http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml#external-process