CHAPTER 11

BYOD Wired Infrastructure Design

Revised: August 7, 2013

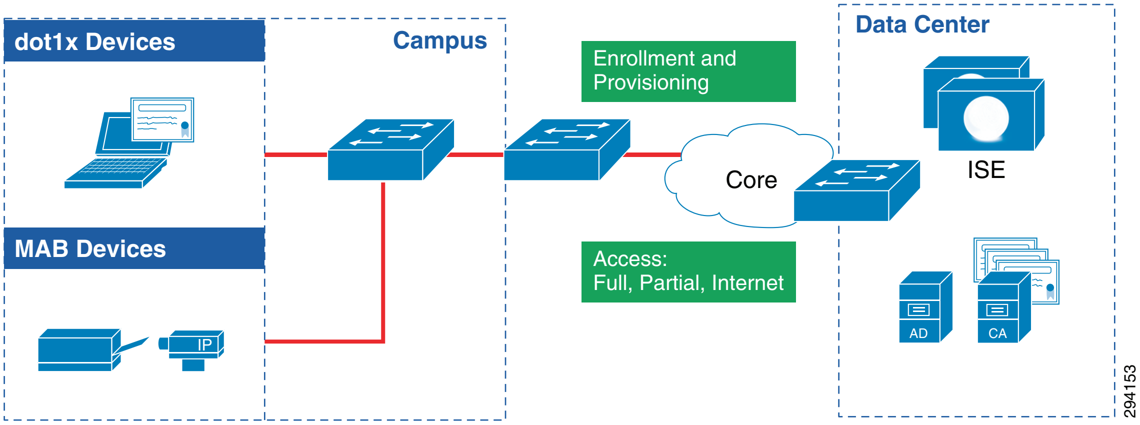
The previous sections discussed how BYOD devices can be on-boarded to the network and also how different policies can be enforced for mobile devices using wireless medium. This section discusses how to design and configure on-boarding and enforcing network access policies for wired devices. These devices can be located at Campus or at Branch location. Moreover, wired devices can connect using either converged access layer switches or by using non-converged access layer switches. This section discusses the design and configuration details for following network architectures:

- Campus (Both Converged Access and non-Converged Access)
- Branch (Both Converged Access and non-Converged Access)

Campus Wired Design

At the campus location there are 802.1X-capable clients that go through the provisioning/enrollment process and there are other types of devices like printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also will need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. Figure 11-1 shows an end-to-end network architecture diagram that includes wired device access from campus:

Figure 11-1 Network Diagram for Wired Devices at Campus Location



VLAN Design for Wired Switches at Campus

In the campus BYOD wired designs presented in this document, the VLAN assignment is same for all types of access—Full, Partial, or Internet. This means that the VLAN assignment to the port does not change when the device accessing the port changes. For example, the corporate-owned asset and the personal device would still use the same VLAN number. The policy enforcement is done by a DACL which is pushed from the ISE for non-Converged Access switches. On the other hand, policy enforcement in Converged Access switches is done using a named ACL instead of a DACL. To obtain more information about the different types of DACLs or named ACLs, refer to Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices." The following is an example configuration of Layer 2 interface of the access layer switch and is the same either on centralized campus or a converged access campus switch:

```
interface GigabitEthernet1/0/2
 switchport access vlan 42   ! VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

IP Address Design for Campus Wired Infrastructure

In the campus wired network designs discussed in this design guide, the access layer switch performs Layer 2 functions only. The aggregation switch performs Layer 3 routing. The following is an example of part of the configuration of the Layer 3 aggregation switch:

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end

ua31-6500-1#
```

As seen above, the Layer 3 interfaces are configured with the ip-helper address command, which helps clients obtain an IP address. For the purposes of this design guide, the DHCP server is located in the data center.

Policy Enforcement in the Campus for Wired Devices

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the campus. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

The policy enforcement method at campus non-Converged Access switches is done by defining DACLs in the ISE based on the authZ policy and pushing that DACL to the port on the access layer switch. In Converged Access switches, policy enforcement is done through a named ACL sent by the ISE based on the authZ policy. The named ACL must be previously configured on the Converged Access Catalyst 3850 switch. To obtain more information on the authZ profiles used in this design guide, refer to either Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

ACL Design for Campus Access Layer Switches

This section discusses the set of ACLs that are used for provisioning devices onto the network, protecting against unauthorized access, and blacklisting the device. The ACLs discussed in this section apply to both Converged access layer switches and non-converged access layer switches. Table 11-1 summarizes these ACLs and their purpose.

Table 11-1 Campus ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL-DEFAULT	Access Layer Switch	To protect against unauthorized access through the switch port
ACL_Provisioning	ISE	To allow an endpoint access to complete on-boarding process
ACL_Provisioning_Redirect	Access Layer Switch	Redirect web traffic initiated by new devices accessing the network. This ACL is a named ACL that is present on the access layer switch.
ACL_BLACKHOLE_Redirect	Access Layer Switch	Redirect web traffic initiated by black listed devices

ACL-DEFAULT—This ACL is configured on the access layer switch and used as a default ACL on the port. Its purpose is to prevent un-authorized access. In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no DACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the DACL sent by ISE, ACL-DEFAULT protects the port in the above mentioned scenarios. In the converged access design, the ACL is a named ACL and is configured on the Catalyst 3850 switch. The ISE sends the name of the ACL to be applied at the port. Again, if the switch rejects the named ACL sent by ISE, ACL-DEFAULT protects the port.

An example of a default ACL on a campus access layer switch is shown below:

```
Extended IP access list ACL-DEFAULT
    10 permit udp any eq bootpc any eq bootps log (2604 matches)
    20 permit udp any host 10.230.1.45 eq domain
    30 permit icmp any any
    40 permit udp any any eq tftp
    50 deny ip any any log (40 matches)
```

As seen from the output above, ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

ACL_Provisioning_Redirect—This ACL is used during on-boarding of wired devices. The ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However, this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

An example of ACL_Provisioning_Redirect ACL on a campus switch is shown below:

```
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (43 matches)
    30 deny ip any host 10.225.42.15 (27 matches)
    40 permit tcp any any eq www (30 matches)
    50 permit tcp any any eq 443 (240 matches)
```

ACL_BLACKHOLE_Redirect—This ACL is used to redirect devices that have been blacklisted to the ISE portal to let the user know that the device in use has been blacklisted. This ACL is similar to the ACL_Provisioning_Redirect ACL.

An example of ACL_BLACKHOLE_Redirect on a campus switch is shown below:

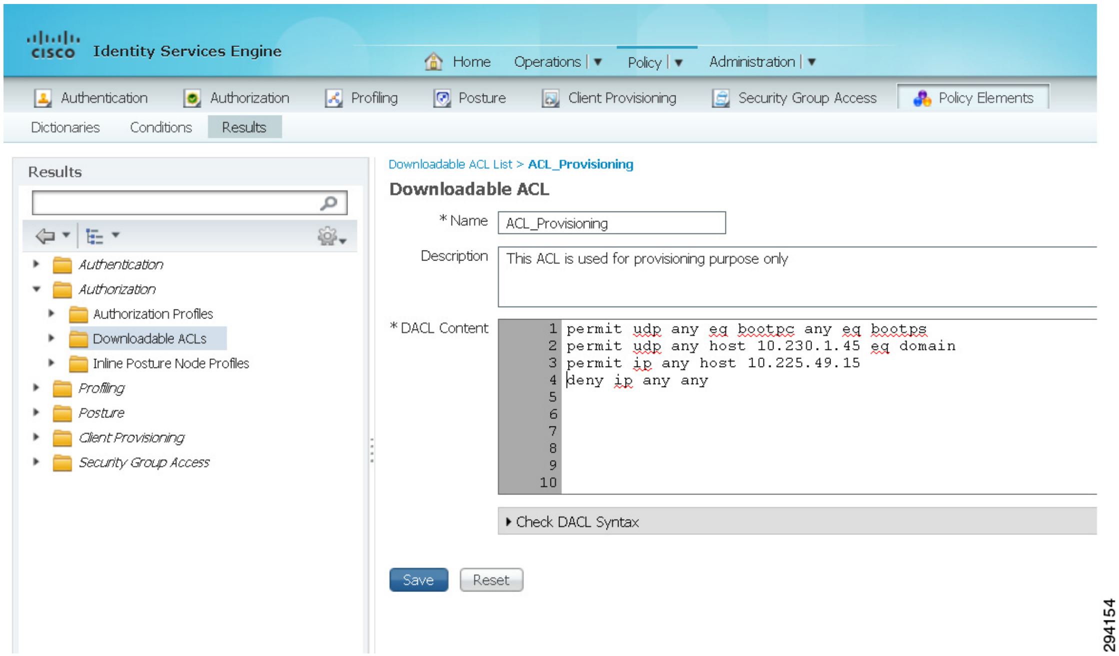
```
Extended IP access list ACL_BLACKHOLE_Redirect
    10 deny udp any eq bootpc any eq bootps
    20 deny udp any host 10.230.1.45 eq domain
    35 deny ip any host 10.225.49.15
    40 permit ip any any
```

Note The converged access layer switches use the same ACL_BLACKHOLE_Redirect for redirecting black listed wired devices.

Provisioning ACL

This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-2.

Figure 11-2 ACL_Provisioning



Downloadable ACL

* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content:

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

Note The ACL_Provisioning ACL is also used for Converged access layer switches.

802.1X and AAA Configuration for Campus Switches

A Cisco Catalyst Switch is used to provide end user Ethernet connectivity into the network in this design guide. The access layer switch enables 802.1X authentication for the client devices and interacts with the Identity Services Engine using the RADIUS protocol. Based on the results from the authentication process, a user may be allowed restricted or full access into the network using a VLAN assignment and a downloadable Access Control List (DACL). The flex-authentication configuration described below allows for using both 802.1X and MAC Authentication Bypass (MAB) as a fallback mechanism. Flex-auth is useful for devices that do not have 802.1X support such as printers.

This section discusses on the configuration details of enabling AAA on the campus access layer switches, and these switches can be either converged access layer switches non-converged access layer switches.

The following steps are required to configure the access switch for AAA on the Campus Switch:

Step 1 Enable Authentication, Authorization, and Accounting (AAA):

```
ACL(config)# aaa new-model
```

Step 2 Create an authentication method for 802.1X (default use all RADIUS servers for authentication):

```
ACL(config)# aaa authentication dot1x default group radius
```

Step 3 Create an authorization method for 802.1X (enables RADIUS for policy enforcement):

```
ACL(config)# aaa authorization network default group radius
```

Step 4 Create an accounting method for 802.1X (provides additional information about sessions to ISE):

```
ACL(config)# aaa accounting dot1x default start-stop group radius
```

The following steps are required to configure the access switch for RADIUS:

Step 1 Add ISE server to the RADIUS group:

```
ACL(config)# radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key
shared-secret
```

Step 2 Configure ISE server dead time (15 seconds total-3 retries of 5 second timeout):

```
ACL(config)# radius-server dead-criteria time 5 tries 3
```

Step 3 Configure the switch to send Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server vsa send accounting
ACL(config)# radius-server vsa send authentication
```

Step 4 Configure the Cisco Vendor-Specific attributes:

```
ACL(config)# radius-server attribute 6 on-for-login-auth
ACL(config)# radius-server attribute 8 include-in-access-req
ACL(config)# radius-server attribute 25 access-request include
```

Step 5 Configure IP address to be used to source RADIUS messages:

```
ACL(config)# ip radius source-interface interface-name Vlan4093
```

The following steps are required to configure the access switch for 802.1X:

Step 1 Enable 802.1X globally (command by itself does not enable authentication on the switchports):

```
ACL(config)# dot1x system-auth-control
```

Step 2 Enable IP device tracking:

```
ACL(config)# ip device tracking
```

The following interface level commands enable 802.1X for Flex-Auth:

Step 1 Configure the authentication method priority (dot1x has higher priority over MAB):

```
ACL(config-if)# authentication priority dot1x mab
```

Step 2 Configure the authentication method order (dot1x first):

```
ACL(config-if)# authentication order dot1x mab
```

Step 3 Enable Flex-Auth:

```
ACL(config-if)# authentication event fail action next-method
```

Step 4 Enable support for more than one MAC address on the physical port:

```
ACL(config-if)# authentication host-mode multi-auth
```

Step 5 Configure the violation action (restrict access for additional devices that may fail authentication):

```
ACL(config-if)# authentication violation restrict
```

Step 6 Enable port for 802.1X:

```
ACL(config-if)# dot1x pae authenticator
```

Step 7 Enable port for MAB:

```
ACL(config-if)# mab
```

Step 8 Configure timers (30 seconds (10x3) until falling back to MAB):

```
ACL(config-if)# dot1x timeout tx-period 3
```

Step 9 Turn authentication on:

```
ACL(config-if)# authentication port-control auto
```

Step 10 Enable the ACL-DEFAULT to the port

```
ACL(config-if)# ip access-group ACL-DEFAULT in
```

Step 11 Enable http and https server:

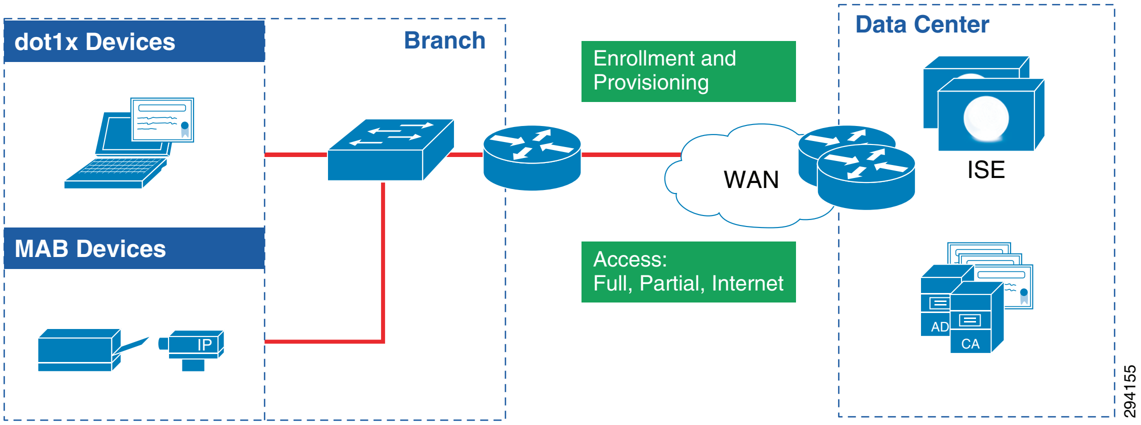
```
ACL (config)# ip http-server
ACL (config)# ip http secure-server
```

Branch Wired Design—Non-Converged Access

At a branch location, there are 802.1X capable clients that go through the provisioning/enrollment process and there are also other types of devices such as printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. This section discusses wired designs for branches which do not deploy Converged Access (Catalyst 3850) switches. The branch wired design discussed in this section is meant to accompany FlexConnect-based wireless branch designs. The Converged Access branch wired design is discussed in Branch Wired Design—Converged Access.

Figure 11-3 shows an end-to-end network architecture diagram that includes wired device access from the branch.

Figure 11-3 Network Diagram for Wired Access at Branch Location



VLAN Design at Branch Locations

Four VLANs are implemented for wired devices at the non-Converged Access branch location. Table 11-2 illustrates the names of these VLANs and their purpose.

Table 11-2 VLANs and their Purpose

VLAN Name	VLAN Number	Description
Wired_Full	13	Devices placed in this VLAN get full access to corporate resources and branch local servers.
Wired_Partial	14	Devices placed in this VLAN get restricted access to resources.
Wired_Internet	15	Devices placed in this VLAN get only Internet access only.
Branch_Server	16	Local Servers at branch location are placed in this VLAN.

IP Address Allocation at Branch Location

In the non-converged access branch network design discussed in this design guide, the switch performs Layer 2 functions only and the branch router performs Layer 3 routing. Hence, all the Layer 3 interfaces for the VLANs mentioned above are implemented at the branch router. The following is an example configuration of the branch router:

```
interface GigabitEthernet0/1.13
 encapsulation dot1Q 13
 ip address 10.200.13.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 13 ip 10.200.13.1
 standby 13 priority 110
 standby 13 preempt
!
interface GigabitEthernet0/1.14
 encapsulation dot1Q 14
 ip address 10.200.14.2 255.255.255.0
 ip access-group Branch1_ACL_Partial_Access in
 ip helper-address 10.230.1.61
 standby 14 ip 10.200.14.1
 standby 14 priority 110
 standby 14 preempt
!
interface GigabitEthernet0/1.15
 encapsulation dot1Q 15
 ip address 10.200.15.2 255.255.255.0
 ip access-group ACL_Internet_Only in
 ip helper-address 10.230.1.61
 standby 15 ip 10.200.15.1
 standby 15 priority 110
 standby 15 preempt
!
interface GigabitEthernet0/1.16
 encapsulation dot1Q 16
 ip address 10.200.16.2 255.255.255.0
 ip helper-address 10.230.1.61
 standby 16 ip 10.200.16.1
 standby 16 priority 110
 standby 16 preempt
!
```

As seen above, the Layer 3 interfaces are configured with the **ip-helper address** command, which helps branch clients obtain an IP address. For the purposes of this design guide, the DHCP server is in a data center location.

Policy Enforcement in the Branch for Wired Devices

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the branch. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

When designing the ACLs for branch the following should be considered:

- Configuring static ACLs at every branch router in the network.
- Configuring the ISE to push downloadable ACLs to access layer switches at every branch location.

Table 11-3 gives the advantages and disadvantages of each approach.

Table 11-3 ACL Policy Enforcement

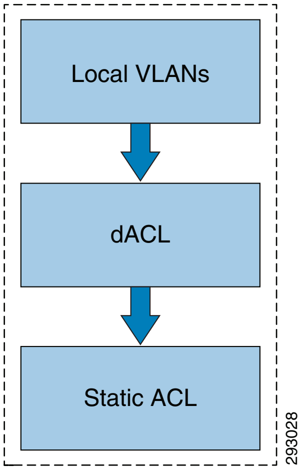
Method	Advantages	Disadvantages
Static ACLs	Modify the ACL based on the branch's needs	Hard to manage each branch policy individually
Downloadable ACLs	Centralized access control	Creating an individual policy at ISE for every branch location would make the policy very large from an administrative perspective. For example, to manage 500 unique branches, 500 ACLs, 500 authZ profiles, and 500 authZ policy rules would need to be defined on the ISE.

Each of the above methods has advantages and disadvantages. This design guide focuses on a combination that includes both methods. The static ACLs are the primary method by which access is restricted. However, the static ACLs are applied at the router only; to override the ACL called

"DEFAULT-ACL" which is present on every port of the access layer switch, a DACL (permit all traffic) is downloaded from ISE. This DACL from the ISE allows the traffic to flow upstream from the access layer switch to the Branch router. The Branch router is pre-configured with the different ACLs that restrict access. These ACLs either provide full, partial, or Internet access to the users.

Figure 11-4 shows how the authorization policy pushes the VLAN information and the DACL (permit all traffic) to the port on the access layer switch, thereby allowing the traffic to reach from the access layer switch up to the router where the traffic will be filtered.

Figure 11-4 Enforcing Permissions



ACL Design at Branch Location

ACLs are very important at the branch location, since they are the main method used to enforce policies. Some ACLs are defined on the Layer 2 switch for provisioning purposes, while others are defined on the branch router. In addition, some ACLs may be downloaded from the ISE.

Table 11-4 summarizes the various ACLs at branch locations and their purpose.

Table 11-4 Branch ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL_DEFAULT	Switch	To protect against unauthorized access through the switch port
ACL_Provisioning_Redirect	Switch	Redirect web traffic initiated by new devices accessing the network.
ACL_Blackhole	Switch	Redirect web traffic initiated by black listed devices
ACL_Internet_Only	Branch Router	Allow only Internet traffic
ACL_Provisioning	ISE	Used during provisioning process
ACL_Partial_Access	Branch Router	Allow partial access to certain resources

ACL_DEFAULT—This ACL is used as a default ACL on the port and its purpose is to prevent un-authorized access. In an 802.1X authentication/authorization scenario, after the device is authenticated and authorized, if there is no DACL applied to the port or if there is a mistake in the syntax of the downloadable ACL and the switch rejects the DACL sent by ISE, ACL_DEFAULT protects the port in the above mentioned scenarios. An example of a default ACL is shown below:

```
bn22-3750x-1#show ip access-lists
Load for five secs: 13%/0%; one minute: 16%; five minutes: 16%
Time source is NTP, 16:24:50.872 EDT Wed Sep 19 2012

Extended IP access list ACL-DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any log
```

As seen from the output above, ACL_DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

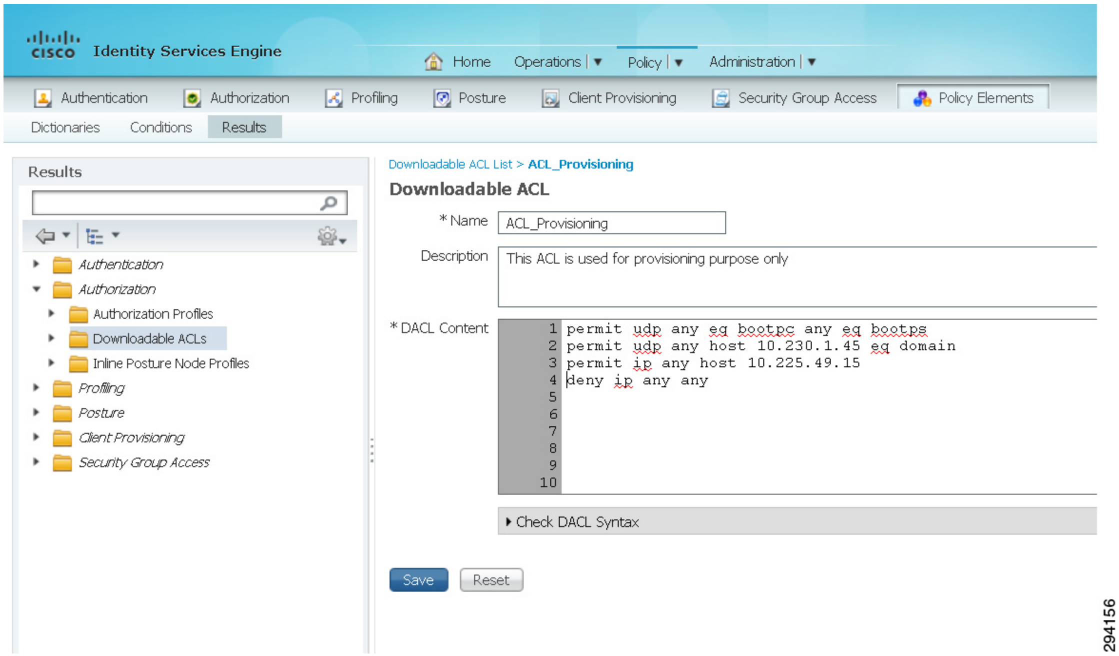
ACL_Provisioning_Redirect—This ACL is used during the on-boarding of wired devices. This ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

```
uasl-3750x-1#show ip access-lists | begin ACL_Provisioning_Redirect
Extended IP access list ACL_Provisioning_Redirect
    10 deny udp any eq bootpc any eq bootps log
    20 deny udp any host 10.230.1.45 eq domain (1865 matches)
    30 deny ip any host 10.225.42.15 (839 matches)
    40 deny ip any host 10.225.49.15 (1853 matches)
    50 permit tcp any any eq www (3728 matches)
    60 permit tcp any any eq 443 (4140 matches)
uasl-3750x-1#
```

Provisioning ACL

This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-5.

Figure 11-5 ACL_Provisioning



Downloadable ACL

* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content:

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

802.1X and AAA Configuration for Branch Switches

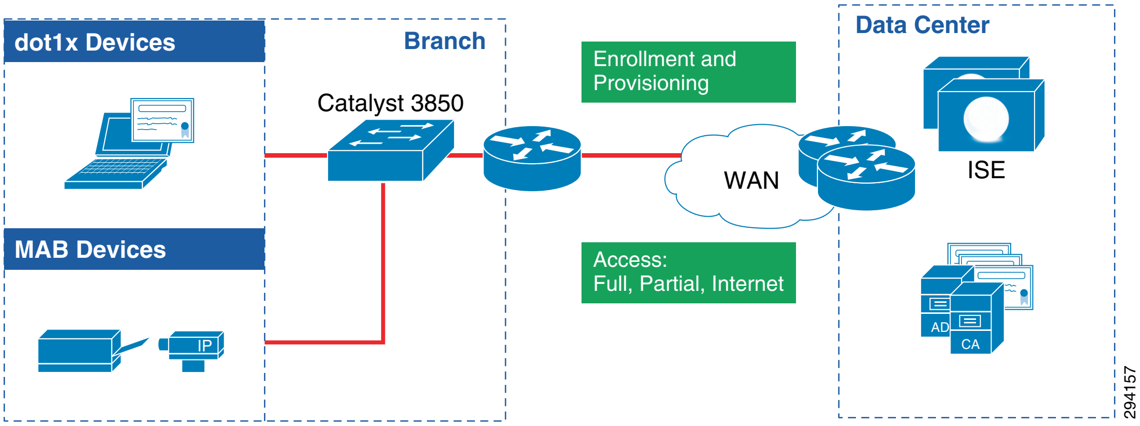
The configuration of 802.1X and AAA for branch non-Converged Access switches is exactly identical to the campus switches. Refer to 802.1X and AAA Configuration for Campus Switches for details.

Branch Wired Design—Converged Access

At a branch location, there are 802.1X capable clients that go through the provisioning/enrollment process and there are other types of devices like printers, cameras, etc. which do not have 802.1X capabilities and can only provide their MAC address as their source of authentication. These devices also need to access the network and this design allows them to authenticate/authorize and obtain their authorization policy from ISE. This section discusses wired designs for branches that deploy Converged Access (Catalyst 3850) switches.

Figure 11-6 shows an end-to-end network architecture diagram that includes wired device access from the branch.

Figure 11-6 Network Diagram for Wired Devices at Branch Location Using Converged Access Switches



VLAN Design at Branch Locations

In the Branch BYOD wired designs presented in this document, the VLAN assignment is same for all types of access—Full, Partial, or Internet. This means that the VLAN assignment to the port does not change when the device accessing the port changes. For example, the corporate-owned asset and the personal device would still use the same VLAN number. The policy enforcement in Converged Access switches is done using a named ACL instead of a DACL. Different named ACLs are applied to each device granting different access to the network. Since the named ACL is configured on the Catalyst 3850 switch specific to the particular branch, a single Cisco ISE policy can be implemented across multiple branches. However the Access Control Entries (ACEs) within the ACL for each branch can be unique to the IP addressing of the branch. This reduces the administrative complexity of the Cisco ISE policy, albeit at the expense of increased complexity of having to configure and maintain ACLs at each branch Catalyst 3850 Series switch.

Three VLANs are implemented for wired devices at the Converged Access branch location. Table 11-5 illustrates the names of these VLANs and their purpose.

Table 11-5 VLANs and their Purpose—Converged Access

VLAN Name	VLAN Number	Description
BYOD_Employee	10	Devices in this VLAN get access to either full, partial or limited access based on named ACL.
BYOD_Provisioning	11	Provisioning VLAN
Branch_Server	16	Local Servers at branch location are placed in this VLAN.

IP Address Allocation at Branch Location

In the converged access branch network design discussed in this design guide, the Catalyst 3850 switch performs Layer 2 functions only. There is no branch router, unlike Branch Wired design for non-Converged Access. The following is an example configuration of a Layer 2 interface of the access layer switch and is the same on either a centralized campus or a converged access campus switch:

```
interface GigabitEthernet1/0/2
 switchport access vlan 42   ! VLAN used in this design is 42
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

Layer 3 connectivity within the branch is provided by the ISR routers that also serve as the WAN connectivity point for the branch. The following is an example of part of the configuration of the Layer 3 router:

```
ua31-6500-1#show running-config interface vlan 42
Building configuration...

Current configuration : 91 bytes
!
interface Vlan42
 ip address 10.207.42.1 255.255.255.0
 ip helper-address 10.230.1.61
end
```

As seen above, the Layer 3 interfaces are configured with the **ip-helper address** command, which helps branch clients obtain an IP address.

Policy Enforcement at the Branch Using Converged Access Switches

ACLs are the primary method through which policy enforcement is done at access layer switches for wired devices within the branch. There are two distinct sets of ACLs used:

- ACLs for managing the device—These ACLs are used for provisioning the device or managing the device like Blacklisting.
- ACLs that are mainly for enforcing the policies.

In Converged Access switches, policy enforcement is done through a named ACL sent by the ISE based on the authZ policy. The named ACL must be previously configured on the Converged Access Catalyst 3850 switch. To obtain more information on the authZ profiles used in this design guide, refer to either Chapter 16, "BYOD Limited Use Case—Corporate Devices" or Chapter 15, "BYOD Enhanced Use Case—Personal and Corporate Devices."

ACL Design at Branch Location for Converged Access Switches

This section discusses both sets of ACLs that are important for a converged access layer switch at a branch location:

- ACL that are used for provisioning.
- ACLs that are used for policy enforcement.

Table 11-6 summarizes the various ACLs in the Converged Access branch wired branch design and their purpose.

Table 11-6 Branch ACLs and Purpose

ACL Name	Where it Applies	Purpose
ACL_DEFAULT	Switch	To protect the switch port
ACL_Blackhole	Switch	Redirect web traffic initiated by black listed devices
ACL_Internet_Only	Switch	Allow only Internet traffic
ACL_Provisioning	ISE	Used during provisioning process
ACL_Partial_Access	Switch	Allow partial access to certain resources
ACL_Full_Access	Switch	Allow full access to all resources

ACL_Default—This ACL is used as a default ACL on the port and its purpose is to prevent un-authorized access. In the Converged Access Design this is done through a named ACL approach. The ACL_DEFAULT resides on the Catalyst 3850 switch.

```
Extended IP access list ACL_DEFAULT
  10 permit udp any eq bootpc any eq bootps
  20 permit udp any any eq domain
  30 permit icmp any any
  40 permit udp any any eq tftp
  50 deny ip any any
```

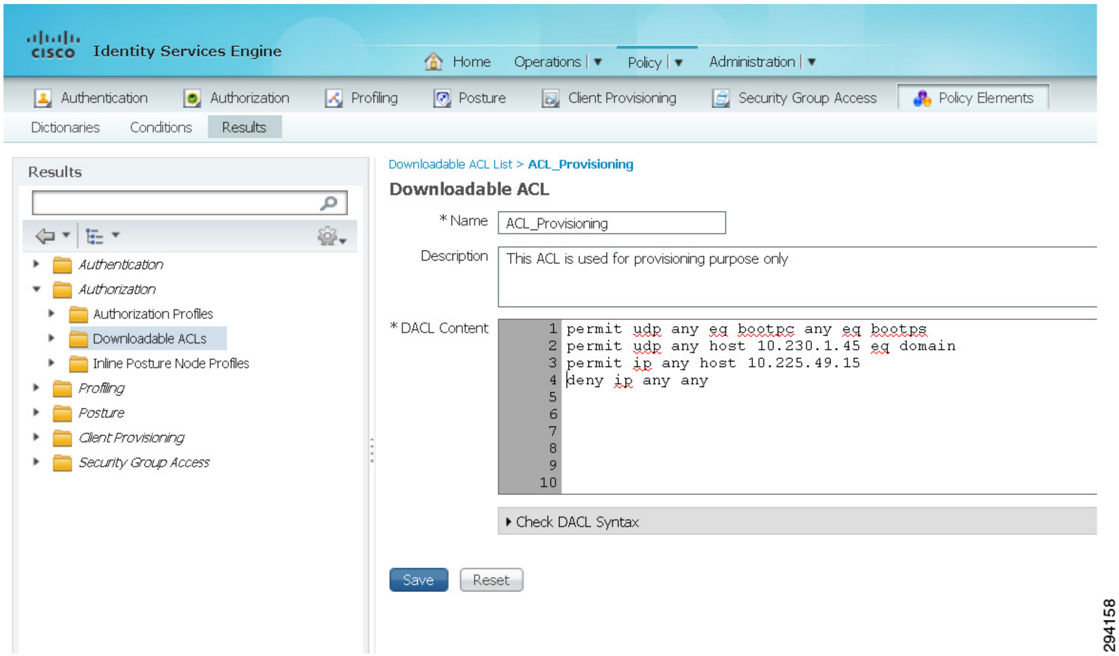
As seen from the output above, ACL_DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

ACL_Provisioning_Redirect—This ACL is used during the on-boarding of wired devices. This ACL triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere, which means that when the user opens a web browser and attempts to access any website, that traffic is re-directed. The example shown below redirects any web traffic initiated by the user. However, this ACL can be modified to allow only certain traffic to be redirected to ISE portal. The underlying assumption in this design is that all the devices must be registered with ISE, therefore when an un-registered device accesses the network, it is redirected to ISE.

```
Extended IP access list ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit tcp any any eq www
 permit tcp any any eq 443
```

ACL_Provisioning—This ACL is also used during the on-boarding of wired devices. This DACL is downloaded from the ISE and restricts access to only the ISE, DNS, and DHCP server. This ACL is defined on the ISE, as shown in Figure 11-7.

Figure 11-7 ACL_Provisioning



* Name: ACL_Provisioning

Description: This ACL is used for provisioning purpose only

* DACL Content:

```
permit udp any eq bootpc any eq bootps
permit udp any host 10.230.1.45 eq domain
permit ip any host 10.225.49.15
deny ip any any
```

802.1X and AAA Configuration for Branch Switches

The configuration of 802.1X and AAA for branch switches is exactly identical to the campus switches. Refer to 802.1X and AAA Configuration for Campus Switches.

MAB Devices at Branch or at Campus Location

This section discusses how to design access for MAB devices using either converged access switches or traditional access layer switches. MAB devices can be present at either branch or campus locations.

MAB devices are generally those devices that cannot run 802.1X and can only present their mac-address for authentication. It is important to note that BYOD devices also use the MAB protocol during the provisioning process. During the provisioning process, BYOD devices are re-directed to the ISE guest portal to complete the registration process. MAB devices do not need to be registered and therefore do not need to be re-directed. The requirement for MAB devices is to authenticate the device and apply an authorization policy. Here are the high level steps that need to be performed for MAB devices:

1. Configure the access layer switch port or WLC to support the MAB protocol.
2. Import a MAC-address list of all MAB devices as an Identity group in ISE.
3. Configure an authentication policy for Wired and Wireless MAB devices. This same policy will be used to authenticate BYOD devices during provisioning.
4. Configure authorization policy rules in ISE for wired and wireless devices.

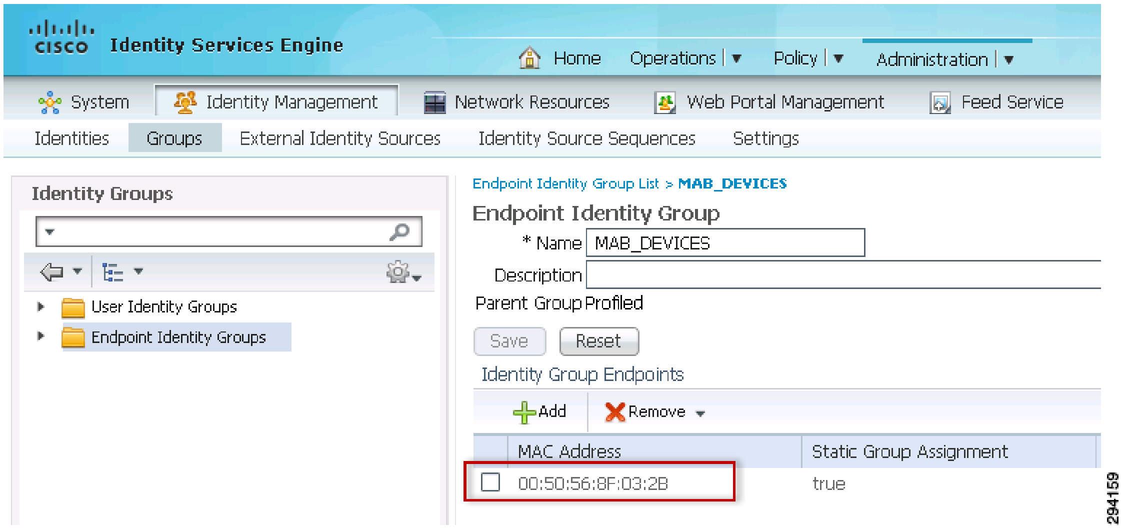
When a MAB device connects, the access layer switch sends the authentication request to the ISE using the MAC-address of the device as the source of authentication. An example is shown below.

```
Sep 25 11:09:50.741: %DOT1X-5-FAIL: Authentication failed for client (0050.568f.
1bb2) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
```

```
Sep 25 11:09:50.741: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
 'dot1x' for client (0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC813
0400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
0050.568f.032b) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
Sep 25 11:09:50.749: %AUTHMGR-5-START: Starting 'mab' for client (0050.568f.032b
) on Interface Gi1/0/10 AuditSessionID 0AC8130400000221292C2D59
```

In this design, all the MAC addresses of MAB devices are placed in an internal identity group called MAB_DEVICES so ISE will know this device in advance. To add new MAC addresses to the MAB_DEVICES identity group, click **Administration > Groups > Endpoint Identity Groups**, as shown in Figure 11-8.

Figure 11-8 MAB_DEVICES Identity Group



Endpoint Identity Group

* Name MAB_DEVICES

Description

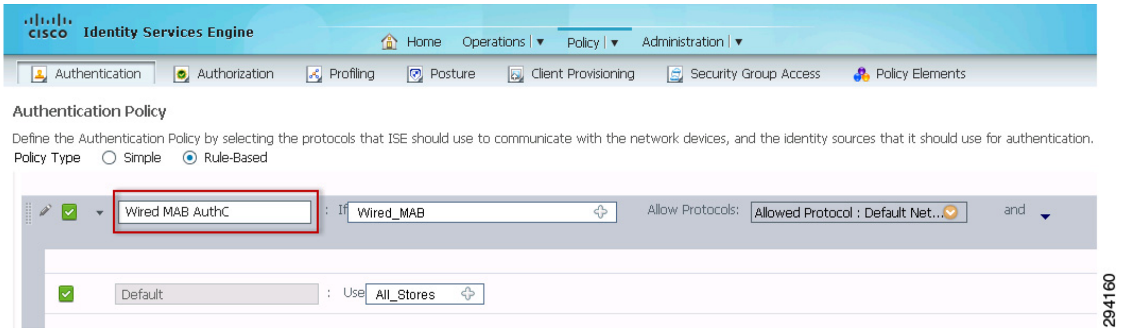
Parent Group Profiled

Identity Group Endpoints

MAC Address	Static Group Assignment
□ 00:50:56:8F:03:2B	true

Figure 11-9 shows the authentication policy defined on the ISE for wired MAB devices.

Figure 11-9 WIRED MAB AuthC



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

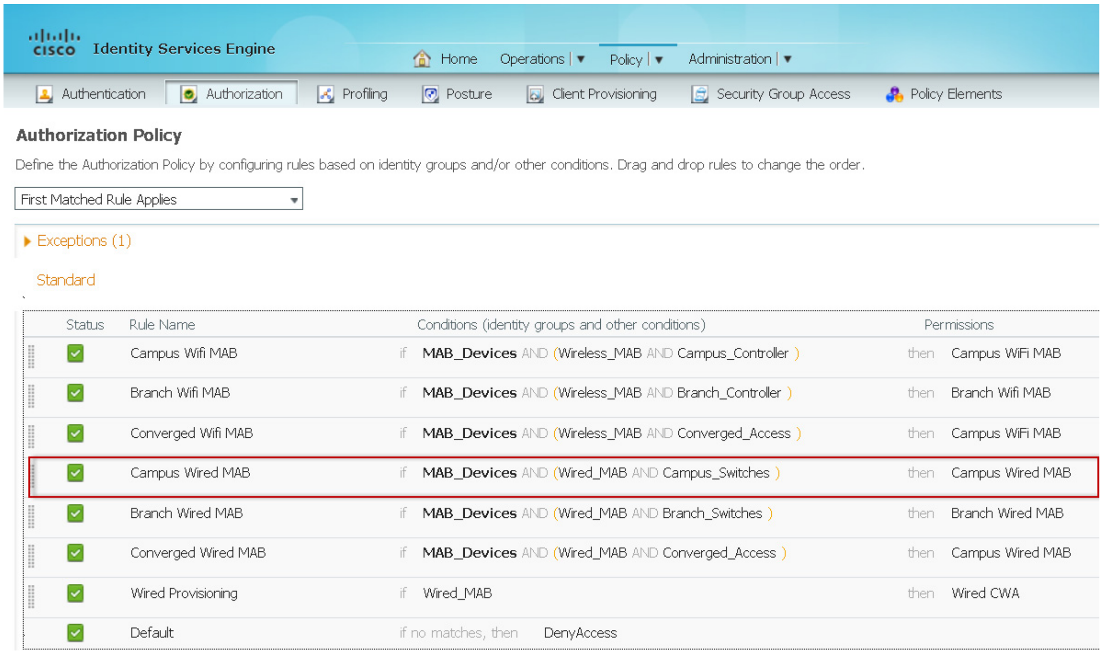
Policy Type ○ Simple ● Rule-Based

☑ Wired MAB AuthC : If Wired_MAB Allow Protocols: Allowed Protocol : Default Net... and

☑ Default : Use All_Stores

The authorization policy is different for MAB devices originating in the branch design with FlexConnect versus in the campus location. In the branch design in a FlexConnect model, every device is placed in different VLANs, but this is not done in the campus or a branch design with converged access. Hence there are different rules that are defined in the authZ policy to take care of location of the device-branch versus campus. Figure 11-10 shows how the policy rules are defined for campus devices.

Figure 11-10 Authorization Policy for MAB devices



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies ▾

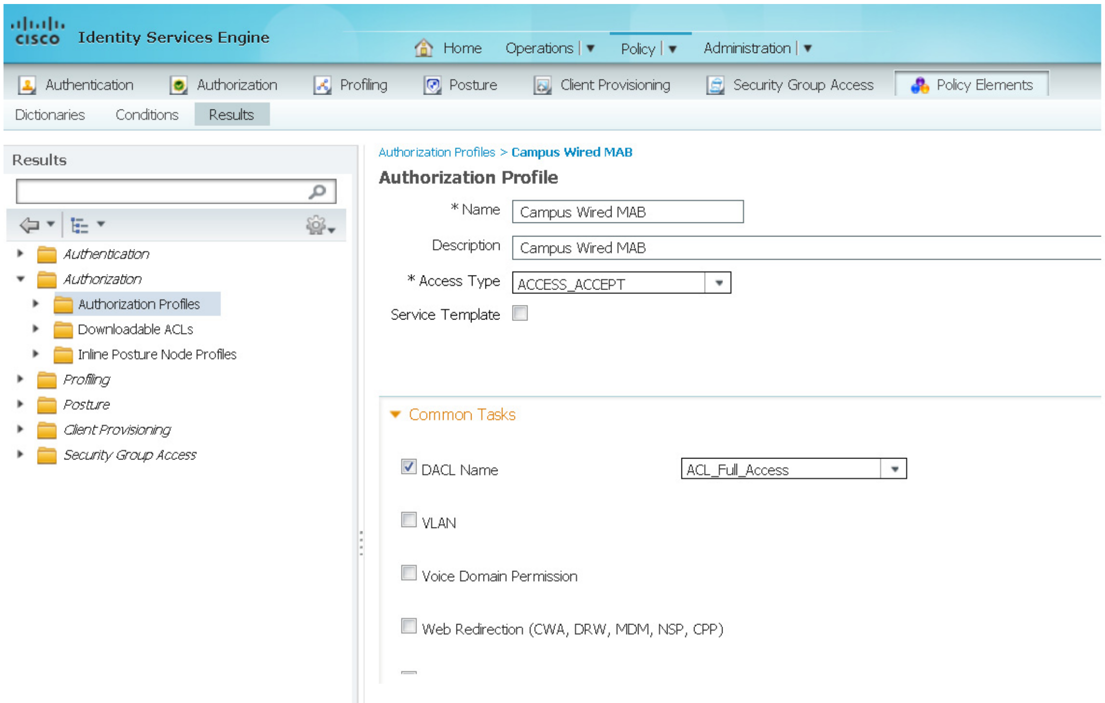
▸ Exceptions (1)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Campus Wifi MAB	if	MAB_Devices AND (Wireless_MAB AND Campus_Controller)	then	Campus WiFi MAB
☑	Branch Wifi MAB	if	MAB_Devices AND (Wireless_MAB AND Branch_Controller)	then	Branch Wifi MAB
☑	Converged Wifi MAB	if	MAB_Devices AND (Wireless_MAB AND Converged_Access)	then	Campus WiFi MAB
☑	Campus Wired MAB	if	MAB_Devices AND (Wired_MAB AND Campus_Switches)	then	Campus Wired MAB
☑	Branch Wired MAB	if	MAB_Devices AND (Wired_MAB AND Branch_Switches)	then	Branch Wired MAB
☑	Converged Wired MAB	if	MAB_Devices AND (Wired_MAB AND Converged_Access)	then	Campus Wired MAB
☑	Wired Provisioning	if	Wired_MAB	then	Wired CWA
☑	Default	if no matches, then	DenyAccess		

Campus Wired MAB is an authorization profile that pushes the appropriate settings to the access layer switch. Figure 11-11 shows the authorization profile details.

Figure 11-11 Campus Wired MAB Authorization Profile



Authorization Profiles > **Campus Wired MAB**

Authorization Profile

* Name: Campus Wired MAB

Description: Campus Wired MAB

* Access Type: ACCESS_ACCEPT ▾

Service Template □

▾ Common Tasks

☑ DACL Name: ACL_Full_Access ▾

□ VLAN

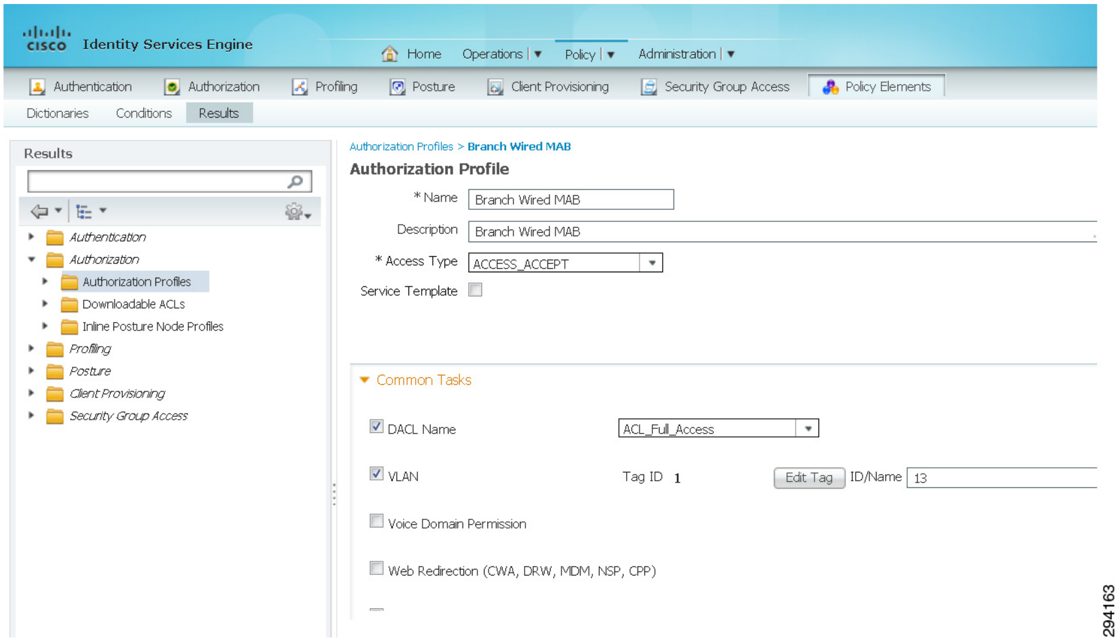
□ Voice Domain Permission

□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

The Campus Wired MAB authorization profile does not push VLAN information, but rather applies a DACL to the port. The Converged Access design uses the same authorization profile as shown in the Figure 11-11. Also note that in the Converged Access design, for the authorization profile, a DACLs is used for both Campus and Branch designs.

Conversely, Branch_Wired_MAB authorization profile pushes the VLAN information to the access port on the wired switch for designs with branch with FlexConnect. Figure 11-12 shows the Branch_Wired_MAB profile configuration.

Figure 11-12 Branch_Wired_MAB Authorization Profile



Authorization Profile

* Name: Branch Wired MAB

Description: Branch Wired MAB

* Access Type: ACCESS_ACCEPT

Service Template ☐

☑ DACL Name: ACL_Full_Access

☑ VLAN: Tag ID 1 ID/Name 13

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

The Converged Access Branch Design also uses same authorization profile for MAB devices as shown in the Figure 11-12.