Converged Access: Enabling Wireless

This chapter describes how to deploy a converged access switch, connect it as a mobility member in your converged topology, activate access point licenses, and have the access points ready for physical connection to the corresponding switch.

This chapter covers basic interface-level configuration on a switch, basic converged access wireless configuration, and mobility configuration that is specific to converged access technologies.

This chapter is primarily targeted at individuals who have previous experience with switching infrastructure or wireless technologies, or both, but who may not be familiar with converged access as a model of wireless deployment.

Concepts and Definitions

This section provides you with brief descriptions of the key phrases used in this chapter.

CAPWAP

Control and Provisioning of Wireless Access Points (CAPWAP) is a secured tunneling protocol over which access points connect to wireless controllers. Client traffic is sent from a wireless controller to an access point over a CAPWAP tunnel. Additionally, wireless controllers in a converged access architecture communicate with each other over a secured CAPWAP tunnel.

Switch Peer Group

A switch peer group is a collection of mobility agents that share a full–mesh CAPWAP tunnel topology and is defined on a Mobility Controller. Mobility Agents within the same switch peer group easily share client

context with each other and clients can quickly roam between the Mobility Agents in the same switch peer group.

Mobility Subdomain

A mobility subdomain is defined by a Mobility Controller on a one-to-one basis. A mobility subdomain can contain one or more switch peer groups. Client roaming between devices in different switch peer groups in the same mobility subdomain can be enabled by forwarding traffic through the mobility controller.

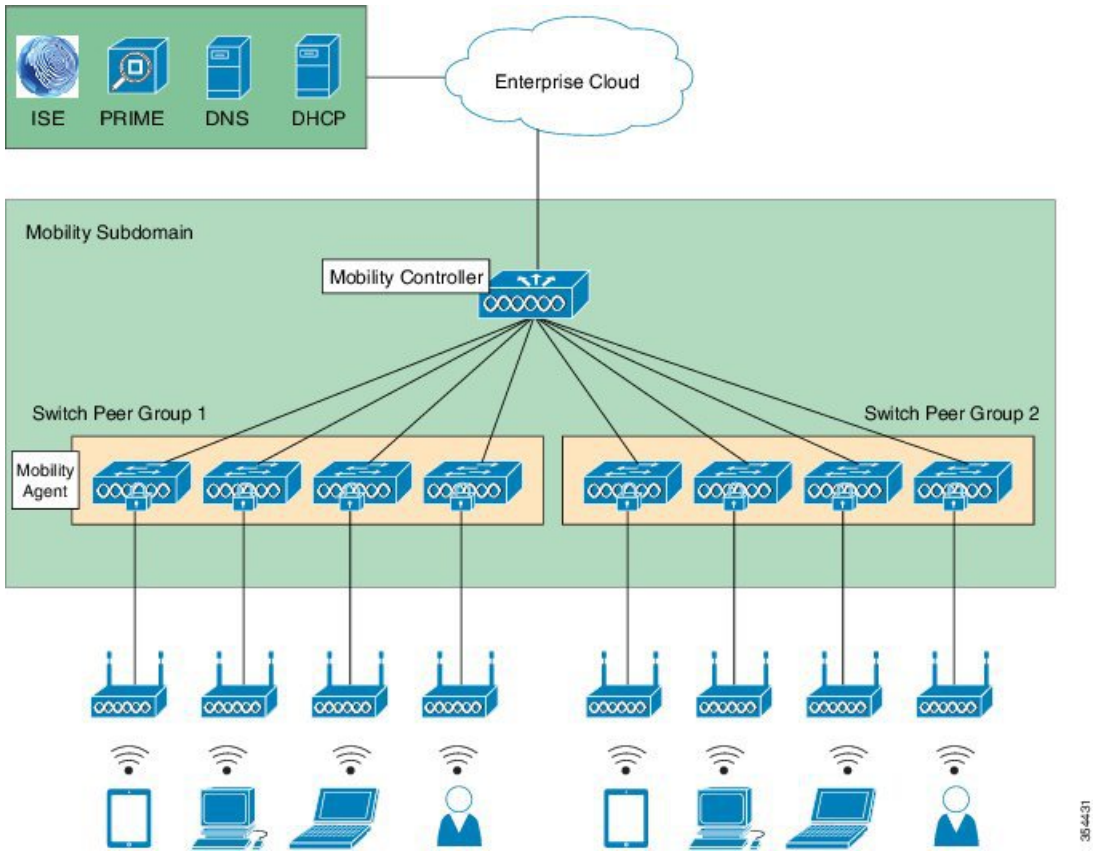
Mobility Domain

A mobility domain can be defined as a collection of mobility subdomains. Mobility domains are created by associating mobility controllers with one another to create a mesh of CAPWAP tunnels. Clients can roam between different mobility subdomains in the same domain by forwarding traffic through two mobility controllers, one in the original subdomain and one in the roamed-to subdomain. Clients cannot roam between different mobility domains.

Converged Access Topology Example

The following figure shows a converged access topology. The topology shows what a typical converged access mobility subdomain looks like. While your topology may differ, the mobility configuration on the individual mobility agents and the mobility controller will be the same as what is referenced in this chapter.

Figure 1: Converged Access Topology



Configuring Wireless Management Interface

To enable the wireless controller functionality on a device, use the **wireless management interface** command. The VLAN interface should be the same as the access point VLAN. After the command is enabled, the switch intercepts the CAPWAP discovery packets on the configured VLAN for the directly connected access points. This allows the access points to join the switch as controllers, and prevents them from joining another controller in the VLAN.

From Cisco IOS XE Release 3.8E, VSS wireless support was added to Cisco Catalyst 4500 Series, Cisco 3850 Series, and Cisco 3650 Series Switches.

Step 1 To configure the wireless management VLAN interface on each switch in your converged access deployment, use the following command:

```
Device(config)# wireless management interface vlan-interface
```

Step 2 To validate your configuration, use the following command. Make sure that the switch recognizes the VLAN interface you have selected, as the management interface.

```
Device# show wireless interface summary

Wireless Interface Summary

Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
-------------------------------------------------------------------------------
interface      Management     vlan    ip_address      netmask        mac_address
```

Configuring Mobility Architecture

Configuring a Mobility Controller

Each mobility subdomain needs a Mobility Controller. Note that a switch must operate either as a mobility agent or as a Mobility Controller. However, when operating as a Mobility Controller, the switch also performs all the standard functions of a Mobility Agent.

To configure a switch as a Mobility Controller and reload the switch for the configuration to take effect, use the following commands:

```
Device (config)# wireless mobility controller
Device (config)# exit
Device# write memory
Device# reload
```

After the device reloads, additional command options become available, because the switch is operating in Mobility Controller mode.

Note Cisco 5760 Wireless LAN Controllers cannot be configured as Mobility Agents, and are therefore, considered as Mobility Controllers always.

Configuring an Access Point Adder License

The distribution and tracking of access point licenses is handled on the Mobility Controller for a given mobility subdomain. When an access point first connects to a Mobility Agent, the Mobility Agent queries the Mobility Controller for a free access point license. If a free license exists, the access point is allowed to register.

Once purchased, adder licenses should be configured on the Mobility Controller. To configure an adder license, use the following command in privileged EXEC mode:

```
Device# license right-to-use activate apcount license-number
```

The number of unconfigured access point adder licenses can be viewed at any time by looking at the license summary. To view the license summary, use the following command:

```
Device# show license right-to-use summary
.
.
.
Total AP Count Licenses: license_number
AP Count Licenses In-use: used_licenses
AP Count Licenses Remaining: remaining_licenses
```

Note On Cisco Catalyst 4500 Series Switches, the stand-by mobility controller synchronizes the license count from the active mobility controller.

Configuring Multiple Subdomains

Note You can skip this section if you are not deploying multiple mobility subdomains.

Devices acting as Mobility Controllers can form CAPWAP tunnels with other Mobility Controllers, extending a mobility domain across one or more subdomains. This configuration is typical for large deployments or in scenarios where the required number of access points scale beyond what is supported on a single mobility subdomain. When a client roams between mobility subdomains, traffic traverses both mobility controllers through their established CAPWAP tunnels.

Step 1 To configure a Mobility Controller with its peer mobility controllers, use the following commands. This should be done on all the devices, creating a full–mesh mobility topology. Repeat this step for all the Mobility Controllers available in the mobility domain. For example, if you have three Mobility Controllers, repeat this step three times.

Mobility Controller 1:

```
Device(config)# wireless mobility group name group-name
Device(config)# wireless mobility group member ip mc2-ip
Device(config)# wireless mobility group member ip mc3-ip
```

Mobility Controller 2:

```
Device(config)# wireless mobility group name group-name
Device(config)# wireless mobility group member ip mc1-ip
```

```
Device(config)# wireless mobility group member ip mc3-ip
```

Mobility Controller 3:

```
Device(config)# wireless mobility group name group-name
Device(config)# wireless mobility group member ip mc2-ip
Device(config)# wireless mobility group member ip mc3-ip
```

Step 2 To verify the configuration, use the following command. Ensure that all the Mobility Controllers are able to establish bidirectional functionality with each other.

```
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : group_name
.
.
.
Controllers configured in the Mobility Domain:

IP              Public IP       Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
mc1_ip          -               group_name       0.0.0.0          UP   : UP
mc2_ip          mc2_ip          group_name       0.0.0.0          UP   : UP
mc3_ip          mc3_ip          group_name       0.0.0.0          UP   : UP
```

Configuring a Mobility Agent

Mobility agents must be configured with the wireless management interface IP address of the Mobility Controller for the subdomain they are to join.

Note Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches are configured as Mobility Agents in the factory. Therefore, no configuration is needed to enable Mobility Agent mode.

To configure a Mobility Agent with the IP address of its Mobility Controller, use the following command:

```
Device(config)# wireless mobility controller ip controller-ip
```

To verify if the Mobility Agent and the Mobility Controller are able to establish a bidirectional connection, use the following command:

```
Device#  show wireless mobility summary

Mobility Agent Summary:

Mobility Role                                   : Mobility Agent
.
.
```

```
.
Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

IP              Public IP            Link Status
------------------------------------------------
controller_ip   controller_ip        UP   : UP
```

Creating a Switch Peer Group

Before CAPWAP connections complete the mobility architecture, create one or more switch peer groups and specify which Mobility Agents should belong to which peer group. Mobility Agents within a switch peer group form a full–mesh CAPWAP topology, and roaming is fastest between them. When a client roams to another switch peer group in the same mobility subdomain, packets traverse the mobility controller. Splitting switch peer groups can help reduce roaming traffic since a Mobility Agent shares roaming information with the devices in its switch peer group and its Mobility Controller.

Note A switch peer group should include peer Mobility Agents, which provide wireless functionality, in an area that users access most frequently.

Define a switch peer group on a Mobility Controller. After the peer group is configured, add the peer group members to the switch peer group using the **wireless management interface** command. The IP addresses of the peer group member interfaces should be the same as the IP addresses configured.

```
Device(config)# wireless mobility controller peer-group peer-group
Device(config)# wireless mobility controller peer-group peer-group member ip member-ip-1
Device(config)# wireless mobility controller peer-group peer-group member ip member-ip-2
```

Mobility Agents in the switch peer group are associated with the peer group and establish a full–mesh mobility topology with other peers. You can verify the switch peer group from the Mobility Agent for a given switch peer group, or the Mobility Controller for all peer groups.

To verify the configuration on a Mobility Agent, use the following command:

```
Device# show wireless mobility summary

Mobility Agent Summary:

Mobility Role                                 : Mobility Agent
Mobility Protocol Port                        : 16666
Mobility Switch Peer Group Name               : peer_group
.
.
.
Switch Peer Group members:

IP              Public IP            Data Link Status
-----------------------------------------------------
member_ip_1     member_ip_1          UP
member_ip_2     member_ip_2          UP
```

To verify the configuration on a Mobility Controller, use the following command:

```
Device# show wireless mobility summary

Mobility Controller Summary:
```

```
Mobility Role                                  : Mobility Controller
.
.
.
Switch Peer Group Name            : peer_group
Switch Peer Group Member Count    : 2
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

IP               Public IP             Link Status
-------------------------------------------------
member_ip_1     member_ip_1            UP   : UP
member_ip_2     member_ip_2            UP   : UP
```

To verify the configuration on a Mobility Controller on Cisco Catalyst 3850 Series and Cisco Catalyst 4500 Series Switches, use the following command:

```
Device# show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                  : Mobility Controller
Wireless Management VLAN                       : 60
Wireless Management IP Address                 : 10.127.0.66
Mobility Group Name                            : ENG
Mobility Oracle Configured Mode                : Disabled
Mobility Oracle IP Address                     : 0.0.0.0
DTLS Mode                                      : Enabled
Mobility Keepalive Interval/Count              : 10/3
Mobility Control Message DSCP Value            : 48
Mobility Domain Member Limit/Count             : 8/2

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

HostName                IP               Public IP        Group Name       Multicast IP
  Link Status
-----------------------------------------------------------------------------------------------------
eng-bgl16-51a-sw1  10.127.0.66            N/A              ENG              0.0.0.0
    N/A
                   10.127.1.76            10.127.1.76      ENG              0.0.0.0
    UP   : UP

Sub-Domain Peer Group Summary
Switch Peer Group Limit/Count                  : 8/2
Switch Peer Group Member Limit/Count           : 32/3

Switch Peer Group Name            : 4th-floor-fd1
Switch Peer Group Member Count    : 1
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0

HostName          IP               Public IP        MTU     Link Status      Centralized
(Cfgd : Running)
-----------------------------------------------------------------------------------------------------

                10.127.1.130     10.127.1.130     0         DOWN : DOWN       Disabled
    Disabled

Switch Peer Group Name            : Mingla
Switch Peer Group Member Count    : 2
Bridge Domain ID                  : 0
Multicast IP Address              : 0.0.0.0
HostName          IP               Public IP        MTU     Link Status      Centralized
(Cfgd : Running)
-----------------------------------------------------------------------------------------------------
eng-bgl16-42a-sw1 10.127.1.157     10.127.1.157     1500      UP   : UP         Disabled
     Disabled
                10.127.1.209     10.127.1.209     1500      UP   : UP         Disabled
```

```
Disabled
```

Staging for Access Points

Configuring a Physical Port

Configure the downlink interfaces that connect to access points as Layer 2 switch ports. The access VLAN for the ports should be configured as the same VLAN used in the **wireless management interface** command. Enable the Spanning tree Portfast on access ports to flag these ports as edge ports to the spanning tree. This causes the port to immediately transition to the spanning tree forwarding state, allowing traffic to flow without progressing through the typical spanning tree process.

To configure the physical ports connected to the access points, use the following commands:

```
Device(config)# interface interface_number
Device(config-if)# description Access-point port
Device(config-if)# switchport access vlan wireless-mgmt-vlan
Device(config-if)# switchport mode access
Device(config-if)# spanning-tree portfast
Device(config-if)# spanning-tree bpduguard enable
```

Configuring an Access Point IP Address

After the wireless controller functionality is enabled and the mobility topology built, the device needs to be configured to support the directly connected access points. Typically, DHCP is used to provide IP addresses for access points. The DHCP addresses are provided by an external source or by the switch itself. Configure the addresses by external source or by switch, but not by both.

If an external source is used, the switch should be configured as a DHCP relay agent. To configure using external source, use the following commands:

```
Device(config)# interface vlan apvlan-interface
Device(config-if)# ip helper-address dhcp-server-ip
```

To use the switch as the DHCP server for access points, configure an appropriate DHCP pool on the switch. Configure the default router using the **default-router** command and specify the wireless management IP address. Use the **update arp** command to secure ARP table entries on the switch with the DHCP lease negotiated by the access point.

To configure the DHCP pool, use the following commands:

```
Device(config)# ip dhcp pool name
Device(dhcp-config)# network network-address network-mask
Device(dhcp-config)# default-router wireless-mgmt-vlan-ip
Device(dhcp-config)# update arp
```

After configuring the switch as the DHCP server, you can verify if the access points are obtaining addresses after they are connected. If you have configured an external DHCP server, check that server for bindings to validate this configuration.

To check the local Cisco IOS DHCP server bindings, use the following command:

```
Device# show ip dhcp pool

Pool name:
.
.
.
Leased addresses               : 3
```

Registering Access Points

At this point, access points are ready to be physically connected to the topology. After an access point is connected and has obtained an IP address, it will connect on the wireless management VLAN and broadcast a discovery request. The switch will intercept this request and communicate with the access point. No further intervention is required.

To verify that the access points have successfully registered with the switch, use the following command:

```
Device# show ap summary

Number of APs: 3
.
.
.
```