Converged Access: Basic Configuration

This chapter provides information about the basic configuration of the wired features on a device. For information about the deployment of the wired features, refer to the *Cisco Wired LAN Technology Design Guide*.

Concepts and Definitions

The following concepts and terms are used throughout this guide:

NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between devices in a network. NTP is implemented using User Datagram Protocol (UDP), which in turn runs over an IP. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices within a millisecond of one another.

SSH

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command line login, remote command execution, and other secure-network services between two networked computers. It connects an SSH server and SSH client through a secure channel over a network that is not secure. SSH is typically used to log in to remote machines and execute commands.

Remote shell protocols send information, such as password, in plaintext making the networks susceptible to interception and disclosure. SSH is designed as a replacement for Telnet and other remote shell protocols that are not secure.

VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, irrespective of the physical location of users. A VLAN has the same attributes as the physical LAN. However, you can group the end stations in a VLAN even if they are not physically located on the same LAN segment. A switch module port can belong to a VLAN, but the unicast, broadcast, and multicast packets are forwarded only to the end stations in the VLAN. A VLAN is often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN.

Interface VLAN membership on a switch module is assigned manually on an interface-by-interface basis and is known as interface-based or static VLAN membership. Traffic between the VLANs must be routed. VLANs are identified with a number ranging from 1 to 4094.

Port Channel

A port channel bundles up to eight individual interfaces into a group to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic that is carried over a failed link switches to one of the remaining member ports within the port channel. This traffic switch facilitates the load and balances the traffic across the physical interfaces. A port channel is operational as long as at least one physical interface within the port channel is operational.

You can create a port channel by bundling compatible interfaces. You can configure and run either static port channels or the port channels that run the Link Aggregation Control Protocol (LACP). Any configuration change that you apply to a port channel is applied to each member interface of that port channel.

Use a static port channel with no associated protocol for a simplified configuration. To use a port channel efficiently, you can use LACP, which is defined in IEEE 802.3ad.

ARP

Address Resolution Protocol (ARP) provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. It can be used in the following scenario:

Host B wants to send information to Host A, but does not have the MAC address of Host A in the ARP cache. Host B generates a broadcast message for all the hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All the hosts within the broadcast domain receive the ARP request and Host A responds with its MAC address.

DHCP Snooping and Trust

Dynamic Host Configuration Protocol (DHCP) snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature validates DHCP messages that are received from the untrusted sources and filters the invalid messages. It limits the rate of DHCP traffic that is sent or received from trusted and untrusted sources. It builds and maintains the DHCP snooping binding database which contains information about untrusted hosts with leased IP addresses. It utilizes the DHCP snooping binding database to validate subsequent requests from the untrusted hosts. DHCP snooping is enabled on a per VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or on a range of VLANs.

DNS

Domain Name System (DNS) is a hierarchical distributed naming system that maps hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with the IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations. IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as delimiting characters. For example, Cisco Systems is a commercial organization that the IP identifies by a com domain name. Therefore, its domain name is cisco.com. To keep track of domain names, IP has defined the concept of a domain name server that holds a cache (or database) of names mapped to IP addresses. If you need to map the domain name to the IP addresses, you must identify the hostname, specify the server name that is present on your network, and then enable the DNS.

To map a domain name to an IP address, use the following command on your network and enable the DNS:

serverservpresent

Configuring Converged Access

Configuring a Switch Hostname

You can configure a hostname on a switch to uniquely identify the switch. By default, the system name and the system prompt are **Switch**.

Tip Configure your switch hostname such that you can easily identify the switch in your network. Set the hostname for the switch product family, the role of the switch in your network, and the switch location. For example, 3850-access-Bld1Flr1

To configure a host name, use the **hostname** command in the global configuration mode.

```
Device(config)# hostname 3850-access-Bld1Flr1
```

Viewing System Level Licensing

The switch is preinstalled with the ordered license. If a license is not pre-ordered, the switch is booted with the LAN-base license, by default. Right-to-use (RTU) licensing allows the activation of a specific license type and level, and the management of license usage on the switch.

The following are the available RTU licenses:

- LAN Base — Layer 2 features
- IP Base — Layer 2 and Layer 3 features
- IP Services — Layer 2, Layer 3, and IPv6 features

Tip Wireless functionality is supported only on IP Base licenses or on IP Services licenses.

In case of a switch stack, the switch that is activated with an RTU license is the active switch. The license level for the standby or member switches in the stack can be activated at the same time from the active switch console.

Activating an RTU License

Step 1 To activate an RTU License, use the following command in privileged EXEC mode:

```
Device# license right-to-use activate {ipbase |ipservices | lanbase}{all | evaluation all}[slot
slot-number][acceptEULA]
```

Step 2 To reload the switch stack and complete the activation process for RTU license, use the following command in privileged EXEC mode:

```
Device# reload
```

Step 3 After you configure a specific license type and level, you can manage your license by monitoring the license state. To monitor the license state, use the following command:

```
Device# show license right-to-use usage [slot 9]
```

Working with NTP System Clock and Console Timestamps

If you use any of the following features, it is mandatory to use NTP to synchronize controllers:

- SNMPv3
- Access point authentication
- Management frame protection

Cisco Catalyst 3850 and Cisco Catalyst Series switches also supports synchronization with NTP using authentication.

Note Configure a service timestamp for console messages, logs, and debug outputs to allow accurate and easy cross-referencing of events in a network.

Configuring an NTP Server

Step 1 To configure an NTP server, use the following commands in the global configuration mode:

```
Device(config)#ntp server ip-address
Device(config)# clock timezone zone hours-offset
Device(config)# clock summer-time zone recurring
```

Step 2 To configure service time stamps, use the following commands in global configuration mode:

```
Device(config)# service timestamps debug datetime msec localtime
Device(config)# service timestamps log datetime msec localtime
```

Step 3 To verify whether the system clock is synchronized with the NTP server, use the following command in privileged EXEC mode:

```
Device# show ntp status
```

Defining DNS

To configure name and address resolution, define a domain name, and specify the IP address for one or more servers, use the following commands in global configuration mode:

```
Device(config)# ip domain-name name
Device(config)# ip name-server server-address1[server-address2 ... server-address6]
```

Note The default domain name is the value set by the **ip domain-name** command.

Generating Cryptographic Keys

When SSH or HTTPS is configured on a switch, a default cryptographic key is generated. For enhanced security, we recommend that you increase the key length beyond the default size. The recommended key size is 2048.

To generate a cryptographic key, use the following command:

```
Device(config)# crypto key generate rsa modulus 2048
```

Note For more information about additional cryptographic configuration options and examples, refer to the "Configuring SPAN and RSPAN" chapter in the Consolidated Platform Configuration Guide, Cisco IOS XE 3.3SE.

Configuring SSH for User Login

Note Disable the Telnet access to the device.

Step 1 To configure SSH, use the following command in global configuration mode:

```
Device(config)# ip ssh version 2
```

```
Device(config)# ip ssh authentication-retries 3
Device(config)# ip ssh time-out 120
Device(config)# line vty 0 15
Device(config-line)# transport input ssh
```

Step 2 To configure local login and password for access, use the following commands in the global configuration mode.

```
Device(config)# username admin privilege 15 secret my-password
Device(config)# enable secret my-secret-password
Device(config)# service password-encryption
Device(config)# exit
```

Note The local login account and password provides basic device access authentication to view platform operations.

Step 3 To verify whether SSH is enabled, use the following command in privileged EXEC mode:

```
Device# show ip ssh
```

Configuring Management Interface Setup

The GigabitEthernet 0/0 interface on the Cisco Catalyst 3850 Series Switches is used for out-of-band management and is located next to the console port on the back panel of the switch. Out-of-band management manages Cisco Catalyst 3850 Series Switches and all other networking devices through a physical network that is separate from the network that carries end-user traffic. The GigabitEthernet 0/0 interface is located on the back panel of the switch, which is next to the console port.

Note On Cisco Catalyst 4500 Series Switches, FastEthernet 0 is used as the management interface

Note

- Management traffic originating from a switch must be associated with GigabitEthernet 0/0 Virtual Routing and Forwarding (VRF).
- The management VRF, *mgmt-vrf* is a built-in VRF. A default route is required for the management VRF.

  Note On Cisco Catalyst 4500 Series Switches, the management VRF is *mgmtvrf*

- The GigabitEthernet 0/0 interface cannot be used as the source interface for sending SNMP traps.
- The GigabitEthernet 0/0 interface is a Layer 3 interface.

Step 1 To configure the interface on Cisco Catalyst 3850 Series Switches, use the following commands:

```
Device(config)# interface GigabitEthernet 0/0 or interface FastEthernet0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
```

Step 2 To verify the reachability to the default gateway use the following ping utility:

```
Device# ping vrf Mgmt-vrf gateway-ip-address
```

Configuring a VLAN

To configure a VLAN, use the following commands:

```
Device# configure terminal
Device(config)# vlan data-vlan
Device(config)# name data-name

Device(config)# vlan voice-vlan
Device(config)# name voice-name

Device(config)# vlan wireless-management-vlan
Device(config)# name management-name
Device(config)# exit
```

Configuring a Default Route

To configure a default route, use the following command in global configuration mode:

```
Device(config)# ip route 0.0.0.0 0.0.0.0
```

Configuring an Uplink Interface

This section describes how to configure Ethernet interfaces that connect a switch stack to distribution switches or routers. Typically, EtherChannels are used for uplink connectivity because they offer additional resiliency.

Note When you stack two or more physical switches into one logical switch, we recommend that you spread the uplink interfaces across the physical members, preventing a complete member failure.

This section provides the options available for configuring uplink interfaces:

- L3 connectivity using port channel

  To configure L3 connectivity using a port channel, use the following commands:

```
Device(config)# interface intf-id1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 10 <<<<<allowed-vlan-list
Device(config-if)# channel-group 1 mode active  <<<<< Different channel-group modes
can be selected based on the remote interface configuration.
Device(config-if)# no shutdown

Device(config)# interface <intf-id2>
Device(config-if)# switchport mode trunk
Device(config-if)# switchport trunk allowed vlan 15 <<<<<allowed vlan list
Device(config-if)# channel-group 1 mode active <<<< generic
Device(config-if)# no shutdown


Device(config)# interface Port-channel 10
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown
```

  Note To create a port channel, **intf-id1** and **intf-id2** are available.
  For further information on L2 and L3 etherchannel, refer to the Configuring EtherChannelschapter in the Layer 2/3 Configuration Guide.

- L3 connectivity using Switch Virtual Interface (SVI):

  To configure SVI interface, use the following commands:

```
Device(config)# interface vlan X
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no shutdown

Device(config)# interface type/number
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device (config-if)# no shutdown
```

Configuring DHCP Snooping and Trust

Step 1 To configure DHCP snooping, use the following commands:

```
Device(config)# ip dhcp snooping

Device(config)# ip dhcp snooping vlan-number
```

Step 2 To trust the incoming DHCP packets on the uplink to the network, use the following command:

```
Device(config-if)# ip dhcp snooping trust
```

Enabling IP ARP Inspection

To enable IP ARP inspection, use the following command:

```
Device(config)# ip arp inspection vlan data-vlan voice-vlan
```

Configuring a Downstream Wired Client Interface

To configure a downstream wired client interface, use the following commands:

```
Device(config)# interface range gigabitethernet1/0/1 - 4
Device(config-if)# switchport access vlan
Device(config-if)# switchport voice vlan 100
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# spanning-tree portfast
Device(config-if)# no shutdown
Device(config-if)# exit
```

Configuring an Access Point Interface

To configure an access point interface, use the following commands:

```
Device(config)# interface range gigabitethernet1/0/1 - 4
Device(config-if)# switchport access vlan management-vlan
Device(config-if)# spanning-tree portfast
Device(config-if)# no shutdown
Device(config-if)# exit
```

Stacking for High Availability

When Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches are connected using a stack cable, the high availability feature is enabled by default.

Note For more information on stacking, refer to Stack Manager and High Availability Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

Prerequisites for Switch Stack Configuration

The following are the prerequisites for switch stack configuration on Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches :

- All the switches in the switch stack should run the same license level as the active switch.
- All the switches in the switch stack should run compatible software versions.
- A switch stack can have a maximum of nine stacking-capable switches.
- You cannot have a switch stack containing a mix of Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches.
- During a stateful switchover event, all the clients are deauthenticated and must rejoin the new active switch.

Viewing Stack Details

Use the following command to display the summary information about a stack:

```
Device# show switch
Switch/Stack Mac Address : c800.846a.2080 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Standby  c800.840f.7480     1      V05     Ready
*2       Active   c800.846a.2080     1      V05     Ready
 3       Member   c800.846a.3180     0      0      Ready
```