Configure Inter-VLAN Routing with Catalyst Switches

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Related Products

Background Information

Configure

- Network Diagram
- Configurations
  - Recommendations

Verify

- Catalyst 3850
- Catalyst 4500-A
- Catalyst 4500-B

Troubleshoot

Related Information

Introduction

This document describes how to configure Inter-VLAN routing with Cisco Catalyst series switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to create VLANs
- Knowledge of how to create Trunk links

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 3850 that runs Cisco IOS® XE Software Release 16.12.7
- Catalyst 4500 that runs Cisco IOS® Software Release 03.09.00E

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Related Products

This configuration can also be used with these hardware and software versions:

- Any Catalyst 3k/9k switch and later
- Any Catalyst switch model, used as the access layer switch

Background Information

By implementing Inter-VLAN routing, organizations can maintain the benefits of VLAN segmentation while still allowing necessary communication between different parts of the network.

This is particularly useful in complex network environments where different departments or services need to interact securely and efficiently.

A sample configuration for Inter-VLAN routing is set up on a Catalyst 3850 series switch, with a pair of Catalyst 4500 series switches acting as Layer 2 (L2) switches that connect directly to the Catalyst 3850.

The Catalyst 3850 switch has a default route for all traffic destined for the Internet. The next hop is a Cisco router, but this can also be any Internet Gateway, such as a firewall.

In a LAN, VLANs divide devices into distinct collision domains and Layer 3 (L3) subnets.

Devices within the same VLAN can communicate directly without requiring routing.

However, communication between devices in different VLANs necessitates a routing device.

Layer 2 (L2) switches need an L3 routing device to facilitate communication between VLANs.

This routing device can be external to the switch or integrated into another module within the same chassis.

Modern switches, such as the Catalyst 3K/9K, incorporate routing capabilities directly within the switch.

These switches can receive a packet, identify that it belongs to a different VLAN, and forward it to the appropriate port on the destination VLAN.

A typical LAN design segments the network based on the group or function of the devices.

For instance, the engineering VLAN contains only devices related to the engineering department, while the finance VLAN includes only finance-related devices.

Enabling routing allows devices in different VLANs to communicate without being in the same broadcast domain. T

his VLAN design also offers an additional advantage: administrators can use access lists to restrict communication between VLANs.

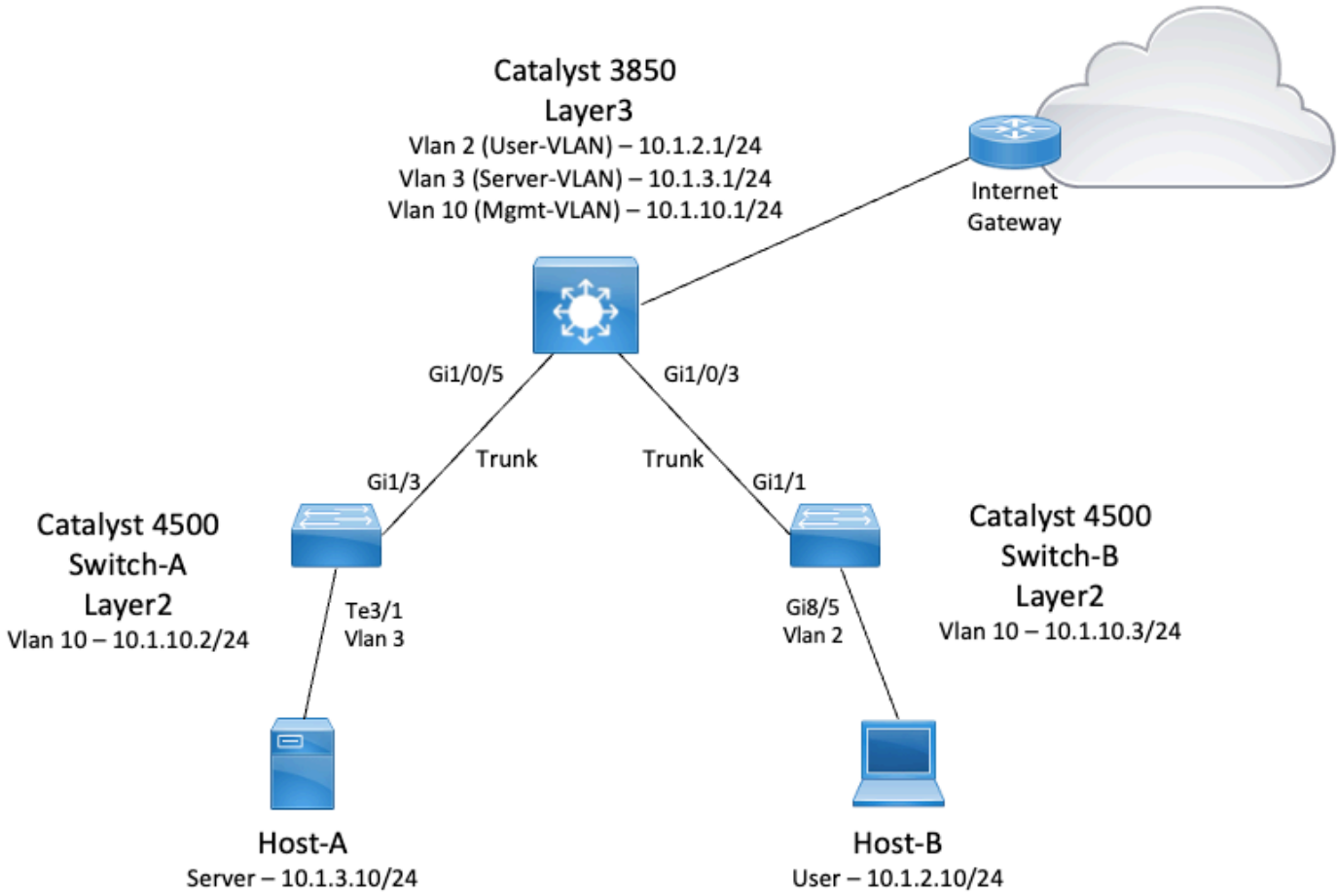
For example, access lists can be used to prevent devices in the engineering VLAN from accessing devices in the finance VLAN.

Configure

This section provides the information needed to configure Inter-VLAN routing as described in this document.

Note: Use the Cisco Support Tools to find more information on the commands used here. Only registered Cisco users have access to tools like this and other internal information.

Network Diagram



In this diagram, the Catalyst 3850 switch provides the Inter-VLAN routing function between the different VLANs. The Catalyst 3850 switch can act as an L2 device with the disablement of IP routing.

In order to make the switch function as an L3 device and provide Inter-VLAN routing, make sure that **ip routing** is enabled globally.

Configurations

These next three VLANs were defined for this setup:

- VLAN 2 — User-VLAN

- VLAN 3 — Server-VLAN
- VLAN 10 — Mgmt-VLAN

Each server and host device must have its default gateway configured to the corresponding VLAN interface IP address on the Catalyst 3850.

For instance, the default gateway for servers is 10.1.3.1. The access layer switches, which are the Catalyst 4500, are connected to the Catalyst 3850 via trunk links.

For Internet traffic, the Catalyst 3850 has a default route pointing to a Cisco router, which acts as the Internet Gateway.

Consequently, any traffic for which the Catalyst 3850 does not have a route in its routing table is forwarded to the Cisco router for further processing.

Recommendations

- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLANs differ, traffic on the native VLANs cannot be transmitted correctly, potentially causing connectivity issues in your network.
- Separate the management VLAN from the the other VLANs, as illustrated in this diagram. This separation ensures that any broadcast or packet storm in the user or server VLAN does not affect switch management.
- Do not use VLAN 1 for management. All ports on Catalyst switches default to VLAN 1, and any unconfigured ports are placed in VLAN 1. Using VLAN 1 for management can cause potential issues.
- Use a Layer 3 (routed) port to connect to the default gateway port. In this example, a Cisco router can be replaced with a firewall that connects to the Internet gateway router.
- This example configures a static default route on the Catalyst 3850 towards the Cisco router to reach the Internet. This setup is ideal if there is only one route to the Internet.
- Configure static routes, preferably summarized, on the gateway router for subnets reachable by the Catalyst 3850. This step is important because this configuration does not use routing protocols.
- If you have two L3 switches in your network, you can connect the access layer switches to both 3850 switches and run Hot Standby Router Protocol (HSRP) between them to provide network redundancy.
- If additional bandwidth is needed for the uplink ports, you can configure EtherChannels, which also provide link redundancy in case of a link failure.

The running configurations of the switches used in the topology are shown next:

Note: The configuration of the Internet Gateway router is not relevant, so it is not covered in this document.

- Catalyst 3850
- Catalyst 4500-A
- Catalyst 4500-B

Catalyst 3850
<#root> SW_3850#

```
show running-config

Building configuration...

Current configuration : 11543 bytes
!
! Last configuration change at 12:16:54 UTC Tue Nov 15 2022
!
version 16.12
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
no platform punt-keepalive disable-kernel-core
!

hostname SW_3850

!
!--- IP routing enabled for Inter-VLAN routing.



ip routing

!
!
no ip domain lookup
!
!
login on-success log
!
!
!

vtp mode off


!
!--- Output suppressed.

!--- Configure IEEE 802.1q trunks.
!--- Issue the switchport mode trunk command to force the switch port to trunk mode.

!
interface GigabitEthernet1/0/1
 shutdown
!
interface GigabitEthernet1/0/2
 shutdown
!

interface GigabitEthernet1/0/3
 description To_Switch-B
 switchport mode trunk

!
interface GigabitEthernet1/0/4
 no switchport
 no ip address
 shutdown
!
```

```
interface GigabitEthernet1/0/5

 description To_Switch-A

 switchport mode trunk

!
interface GigabitEthernet1/0/6
no switchport
no ip address
shutdown
!
interface Vlan1
 no ip address
 shutdown
!

!--- This Switch Virtual Interface (SVI) is the default gateway for Users.
!
interface Vlan2

 description User-SVI

 ip address 10.1.2.1 255.255.255.0

!

!--- This SVI is the default gateway for Servers VLAN.
!
interface Vlan3

 description Server-SVI

 ip address 10.1.3.1 255.255.255.0

!

!--- This SVI is the default gateway for other L2 switches management interface.
!
interface Vlan10

 description Management-SVI

 ip address 10.1.10.1 255.255.255.0
```

```
!
!--- This route statement allows the 3850 to send Internet traffic to the Cisco router.

ip route 0.0.0.0 0.0.0.0 10.1.1.2

ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
line con 0
line vty 5 15
!
end
```

Note: For this example, VLAN Trunk Protocol (VTP) was set to **off** on all the switches, with the use of **vtp mode off** command.

```
<#root>

SW_3850(config)#

vtp mode off

Setting device to VTP Off mode for VLANS.
SW_3850(config)#

vlan 2

SW_3850(config-vlan)#

name User_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 3

SW_3850(config-vlan)#

name Server_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 10

SW_3850(config-vlan)#

name Mgmt_VLAN
```

```
SW_3850(config-vlan)#
exit
SW_3850(config)#
end
```

Catalyst 4500-A

<#root>

Switch-A#

show running-config

```
Building configuration...

Current configuration : 15360 bytes
!
! Last configuration change at 01:06:17 UTC Wed Nov 16 2022
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
!
```

hostname Switch-A

```
!
no ip domain-lookup
no ip dhcp snooping information option
!
!
login block-for 60 attempts 3 within 60
login delay 1
login quiet-mode access-class testblock
login on-failure log
login on-success log
```

vtp mode off

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
```

vlan 3
name Server-VLAN
!
vlan 10
name Mgmt-VLAN

```
!
```

```
!--- Output suppressed

!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 switchport mode trunk

!

!--- Configure Server (Host-A) to be the on the access VLAN 3.

!

interface TenGigabitEthernet3/1
 switchport access vlan 3
 switchport mode access

!
interface TenGigabitEthernet3/2
 shutdown
!
interface TenGigabitEthernet3/3
!
interface TenGigabitEthernet3/4
!

!--- Output suppressed.
!--- IP address on VLAN 10 manages this switch.

!
interface Vlan1
 no ip address
!
interface Vlan10
 ip address 10.1.10.2 255.255.255.0

!
ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!

!--- Configure the default gateway so that the switch is reachable from other
!--- VLANs/subnets. The gateway points to the VLAN 10 interface on the 3850.

ip default-gateway 10.1.10.1
ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!
!
line con 0
```

```
 stopbits 1
line vty 0 4
 logging synchronous
 transport input all
line vty 5 15
 logging synchronous
 transport input all
!
end
```

Catalyst 4500-B

```
<#root>

Switch-B#

show running-config


Building configuration...

Current configuration : 6841 bytes
!
! Last configuration change at 10:44:33 UTC Tue Nov 15 2022
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!

hostname Switch-B

!
boot-start-marker
boot system bootflash:cat4500es8-universal.SPA.03.11.06.E.152-7.E6.bin
boot-end-marker
!
!
vrf definition mgmtVrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no aaa new-model
hw-module module 7 mode 1
!

vtp mode off


!
spanning-tree mode pvst
spanning-tree extend system-id
!

vlan 2
```

```
name User-VLAN
!
vlan 10 name
Mgmt-VLAN


!
!

interface GigabitEthernet1/1
 switchport mode trunk

!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!

!--- Output suppressed.
!--- Configure User (Host-B) in VLAN 2.

!

interface GigabitEthernet8/5
 switchport access vlan 2
 switchport mode access

!

!--- Configure the management IP address in VLAN 10.

!
interface Vlan1
 no ip address
!

interface Vlan10
 ip address 10.1.10.3 255.255.255.0

!

!--- Define the default route so that the switch is reachable.

!


ip default-gateway 10.1.10.1


ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!
!
line con 0
 stopbits 1
line vty 0 4
 login
```

```
 transport input none
!
!
end
```

Verify

Next, you can find a list of essential commands that can be utilized to check the status of the devices and to confirm your configuration works properly:

show vtp status - This command displays the status of the VLAN Trunking Protocol (VTP) on the switch. It provides information about the VTP version, domain name, mode (server, client, or transparent), and the number of existing VLANs. This is useful for verifying VTP configuration and ensuring consistent VLAN information across the network.

show interfaces trunk - This command shows the status of trunk ports on the switch. It provides details about which interfaces are configured as trunks, the encapsulation type (for example 802.1Q), and the VLANs allowed on each trunk. This is essential for troubleshooting VLAN connectivity issues and ensuring proper trunk configuration.

show ip route - This command displays the IP routing table of the switch. It lists all known routes, including directly connected networks, static routes, and routes learned through dynamic routing protocols. This is crucial for verifying the routing paths and ensuring that the switch can reach all necessary networks.

show ip cef - This command shows the Cisco Express Forwarding (CEF) output. It provides information about the CEF entries, including the next-hop addresses and the associated interfaces. This is useful for troubleshooting forwarding issues and ensuring efficient packet processing.

Note: The Cisco CLI Analyzer Tool can help troubleshoot and check the overall health of your Cisco-supported software with this smart SSH client that uses integrated TAC tools and knowledge.

Note: For details on CLI commands, see the Command Reference Guides for specific switching platform.

Note: Only registered Cisco users have access to tools like this and other internal information.

Catalyst 3850

<#root>

SW_3850#

show vtp status

```
VTP Version capable             : 1 to 3
VTP version running             : 1
```

```
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : bc67.1c5d.3800
Configuration last modified by 10.0.0.10 at 0-0-00 00:00:00

Feature VLAN:
--------------

VTP Operating Mode               : Off

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 0
MD5 digest                        : 0x7E 0xC3 0x8D 0x91 0xC8 0x53 0x42 0x14
                                    0x79 0xA2 0xDF 0xE9 0xC0 0x06 0x1D 0x7D
```

<#root>

SW_3850#

show interfaces trunk

```
Port        Mode             Encapsulation  Status        Native vlan

Gi1/0/3     on               802.1q         trunking      1
Gi1/0/5     on               802.1q         trunking      1


Port        Vlans allowed on trunk

Gi1/0/3     1-4094
Gi1/0/5     1-4094


Port        Vlans allowed and active in management domain

Gi1/0/3     1-3,10
Gi1/0/5     1-3,10

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/3     1-3,10
Gi1/0/5     1,3,10
```

<#root>

SW_3850#

show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
```

```
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.100.100.2 to network 0.0.0.0


S*    0.0.0.0/0 [1/0] via 10.100.100.2

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.1.2.0/24 is directly connected, Vlan2
L        10.1.2.1/32 is directly connected, Vlan2
C        10.1.3.0/24 is directly connected, Vlan3
L        10.1.3.1/32 is directly connected, Vlan3
C        10.1.10.0/24 is directly connected, Vlan10
L        10.1.10.1/32 is directly connected, Vlan10
C        10.100.100.0/24 is directly connected, GigabitEthernet1/0/2
L        10.100.100.1/32 is directly connected, GigabitEthernet1/0/2
```

Catalyst 4500-A

```
<#root>

Switch-A#

show vtp status


VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : cisco.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 6400.f13e.dc40
Configuration last modified by 10.1.10.2 at 0-0-00 00:00:00

Feature VLAN:
--------------

VTP Operating Mode                : Off

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 32
Configuration Revision            : 0
MD5 digest                        : 0x0B 0x61 0x4F 0x9B 0xCD 0x1B 0x37 0x55
                                    0xAB 0x0C 0xC1 0x4B 0xF8 0xDE 0x33 0xB3



<#root>

Switch-A#

show interfaces trunk


Port        Mode             Encapsulation  Status        Native vlan

Gi1/3       on               802.1q         trunking      1
```

```
Port        Vlans allowed on trunk
Gi1/3       1-4094

Port        Vlans allowed and active in management domain
Gi1/3       1,3,10

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/3       1,3,10
```

Catalyst 4500-B

```
<#root>

Switch-B#

show vtp status


VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 6c20.5606.3540
Configuration last modified by 10.1.10.3 at 11-15-22 10:42:29

Feature VLAN:
--------------

VTP Operating Mode                : Off

Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 0
MD5 digest                        : 0xEC 0xB4 0x8D 0x46 0x94 0x95 0xE0 0x8F
                                    0xEE 0x1E 0xC7 0x9F 0x26 0x88 0x49 0x9F



<#root>

Switch-B#

show interfaces trunk


Port        Mode             Encapsulation  Status        Native vlan

Gi1/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk

Gi1/1       1-4094
```

```
Port        Vlans allowed and active in management domain

Gi1/1       1-2,10


Port        Vlans in spanning tree forwarding state and not pruned
Gi1/1       1-2,10
```

Troubleshoot

1. Ping Issues Within the Same VLAN

- If you cannot ping devices within the same VLAN, check the VLAN assignment of the source and destination ports to ensure they are in the same VLAN.
- To check the VLAN assignment, use the **show interface status** command.
- Use the **show mac address-table** command to verify that the L2 switch is learning the MAC address of each device in the appropriate VLAN.

2. Ping Issues Across Different Switches

- If the source and destination are on different switches, ensure that the trunks are configured properly. Use the **show interfaces trunk** command to verify the configuration.
- Check that the native VLAN matches on both sides of the trunk link and that the subnet mask matches between the source and destination devices.

3. Ping Issues Between Different VLANs

- If you cannot ping devices in different VLANs, ensure you can ping the respective default gateway (see Step 1).
- Verify that the default gateway of the device points to the correct VLAN interface IP address and that the subnet mask matches.

4. Internet Connectivity Issues

- If you cannot reach the Internet, ensure that the default route on the Catalyst 3850 points to the correct IP address and that the subnet address matches the Internet Gateway router.
- Make sure that the L3 switch (3850 in this scenario) is able to ping the Internet Gateway.
- To check, use the **show ip cef <prefix>** command to identify if it point to the correct interface.
- Ensure that the Internet Gateway router has routes to both the Internet and the internal networks.

Related Information

- Configure Inter VLAN Routing with the Use of an External Router
- Create Ethernet VLANs on Catalyst Switches
- Cisco Technical Support & Downloads