Réseaux fixes
I.4 Segmentation
Routage Inter-VLAN
Introduction IPv6

Luc Deneire

EII-5, Option Réseaux et Objets Connectés (ROC)

Module Objectives

Module Title: Inter-VLAN Routing

Module Objective: Troubleshoot inter-VLAN routing on Layer 3 devices

Topic Title	Topic Objective
Inter-VLAN Routing Operation	Describe options for configuring inter-VLAN routing.
Router-on-a-Stick Inter-VLAN Routing	Configure router-on-a-stick inter-VLAN routing.
Inter-VLAN Routing using Layer 3 Switches	Configure inter-VLAN routing using Layer 3 switching.
Troubleshoot Inter-VLAN Routing	Troubleshoot common inter-VLAN configuration issues.

What is Inter-VLAN Routing?

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

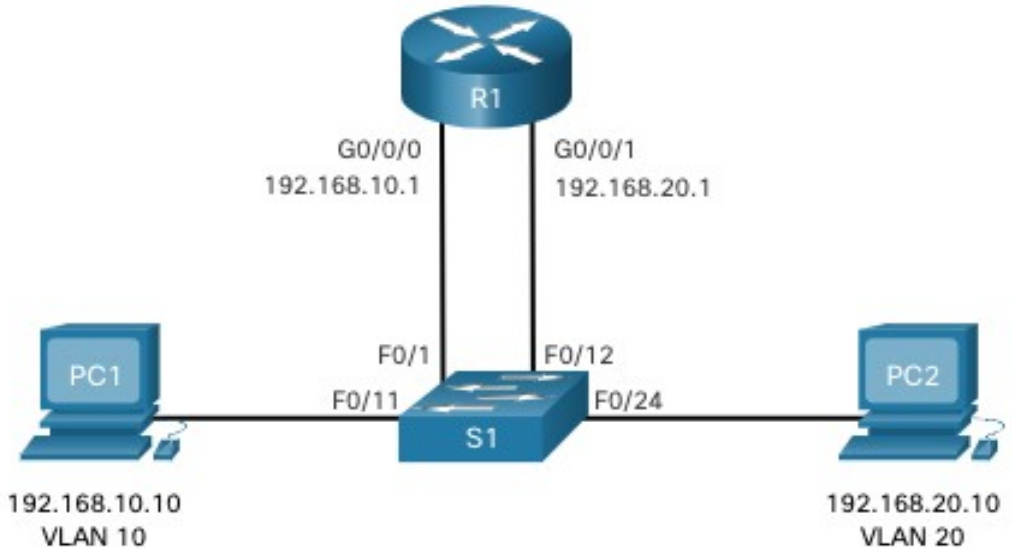
Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

- **Legacy Inter-VLAN routing** - This is a legacy solution. It does not scale well.
- **Router-on-a-Stick** - This is an acceptable solution for a small to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs)** - This is the most scalable solution for medium to large organizations.

Legacy Inter-VLAN Routing

- The first inter-VLAN routing solution relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.
- Legacy inter-VLAN routing using physical interfaces works, but it has a significant limitation. It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.
- **Note**: This method of inter-VLAN routing is no longer implemented in switched networks and is included for explanation purposes only.



Router-on-a-Stick Inter-VLAN Routing

The ‘router-on-a-stick’ inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It only requires one physical Ethernet interface to route traffic between multiple VLANs on a network.

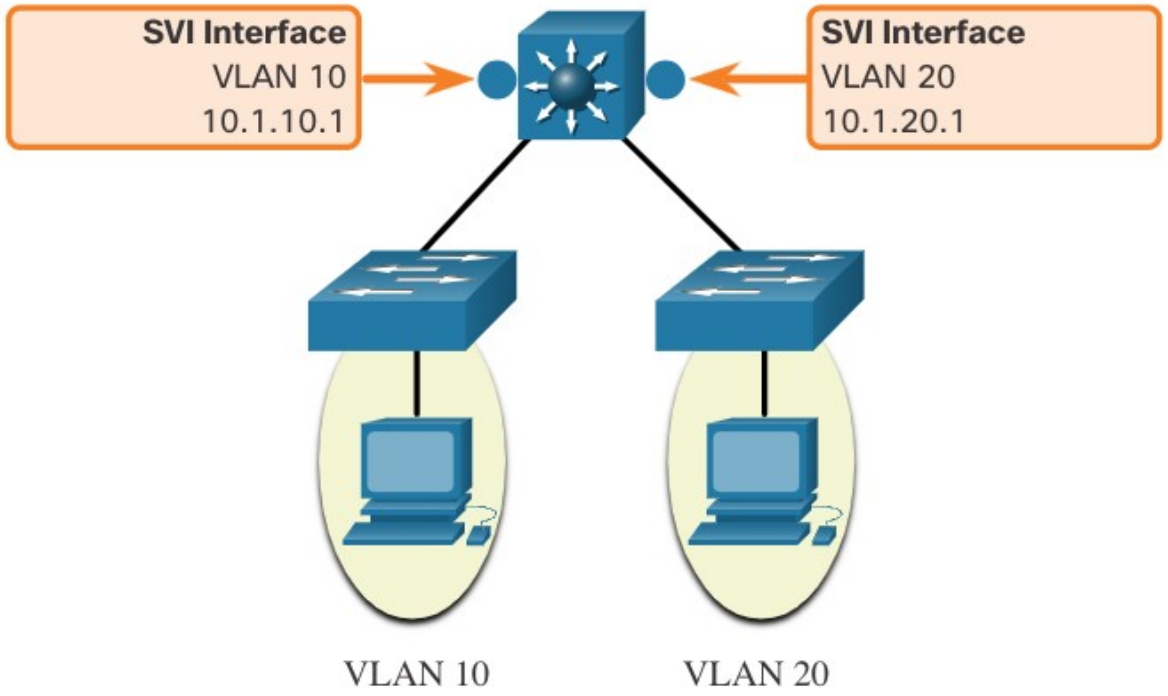
- A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using subinterfaces to identify routable VLANs.
- The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.
- When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.1q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface

Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

Inter-VLAN Routing on a Layer 3 Switch

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch, as shown in the figure.

Note: A Layer 3 switch is also called a multilayer switch as it operates at Layer 2 and Layer 3. However, in this course we use the term Layer 3 switch.



Inter-VLAN Routing on a Layer 3 Switch (Cont.)

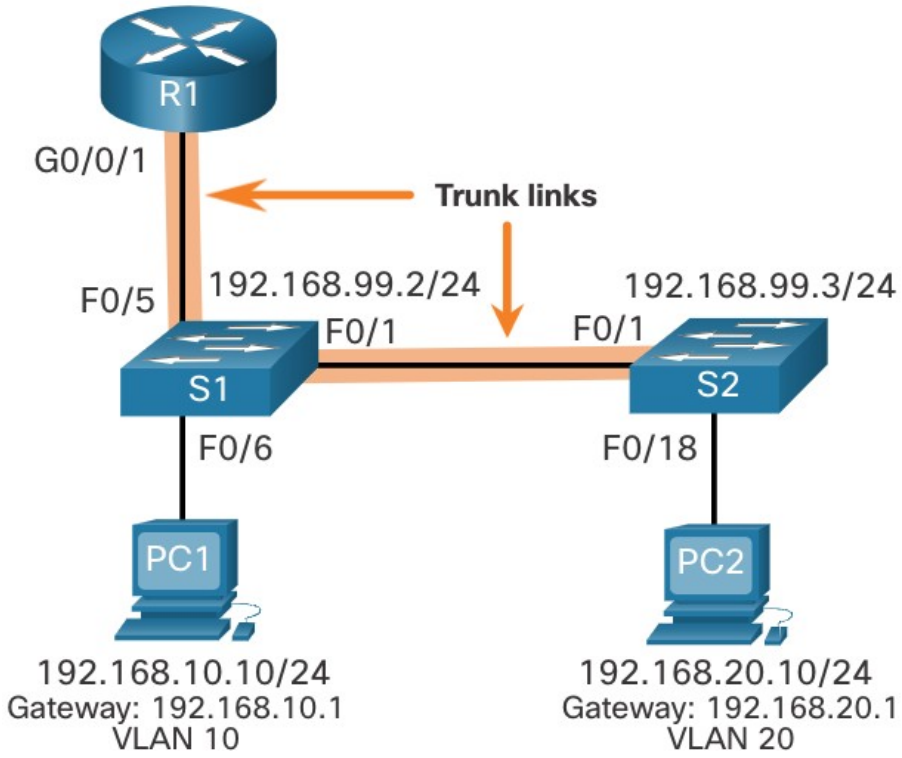
Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.
- They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
- Latency is much lower because data does not need to leave the switch in order to be routed to a different network.
- They are more commonly deployed in a campus LAN than routers.
- The only disadvantage is that Layer 3 switches are more expensive.

Router-on-a-Stick Scenario

- In the figure, the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.
- To route between VLANs, the R1 GigabitEthernet 0/0/1 interface is logically divided into three subinterfaces, as shown in the table. The table also shows the three VLANs that will be configured on the switches.
- Assume that R1, S1, and S2 have initial basic configurations. Currently, PC1 and PC2 cannot **ping** each other because they are on separate networks. Only S1 and S2 can **ping** each other, but they but are unreachable by PC1 or PC2 because they are also on different networks.
- To enable devices to ping each other, the switches must be configured with VLANs and trunking, and the router must be configured for inter-VLAN routing.



Subinterface	VLAN	IP Address
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

S1 VLAN and Trunking Configuration

Complete the following steps to configure S1 with VLANs and trunking:

- **Step 1**. Create and name the VLANs.
- **Step 2**. Create the management interface.
- **Step 3**. Configure access ports.
- **Step 4**. Configure trunking ports.

S2 VLAN and Trunking Configuration

The configuration for S2 is similar to S1.

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

R1 Subinterface Configuration

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed. A subinterface is created using the **interface** *interface_id subinterface_id* global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

- **encapsulation dot1q** *vlan_id* **[native]** - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified *vlan-id*. The **native** keyword option is only appended to set the native VLAN to something other than VLAN 1.
- **ip address** *ip-address subnet-mask* - This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, enable the physical interface using the **no shutdown** interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

R1 Subinterface Configuration (Cont.)

In the configuration, the R1 G0/0/1 subinterfaces are configured for VLANs 10, 20, and 99.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```

Verify Connectivity Between PC1 and PC2

The router-on-a-stick configuration is complete after the switch trunk and the router subinterfaces have been configured. The configuration can be verified from the hosts, router, and switch.

From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.

Next, use **ping** to verify connectivity with PC2 and S1, as shown in the figure. The **ping** output successfully confirms inter-VLAN routing is operating.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

Router-on-a-Stick Inter-VLAN Routing Verification

In addition to using **ping** between devices, the following **show** commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

Layer 3 Switch Inter-VLAN Routing

Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small to medium-sized organization. However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

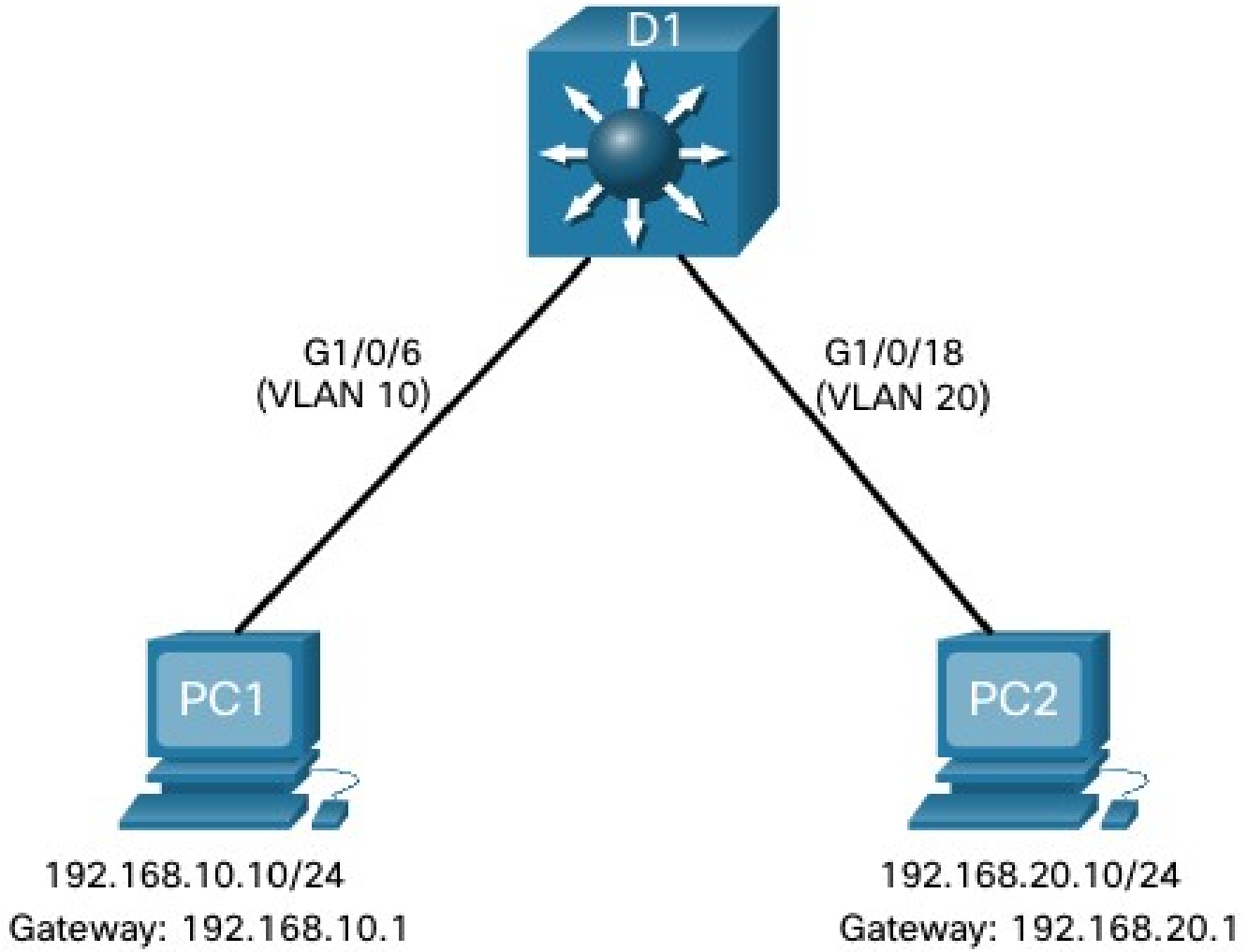
Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

- Route from one VLAN to another using multiple switched virtual interfaces (SVIs).
- Convert a Layer 2 switchport to a Layer 3 interface (i.e., a routed port). A routed port is similar to a physical interface on a Cisco IOS router.
- To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan** *vlan-id* command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.

Layer 3 Switch Scenario

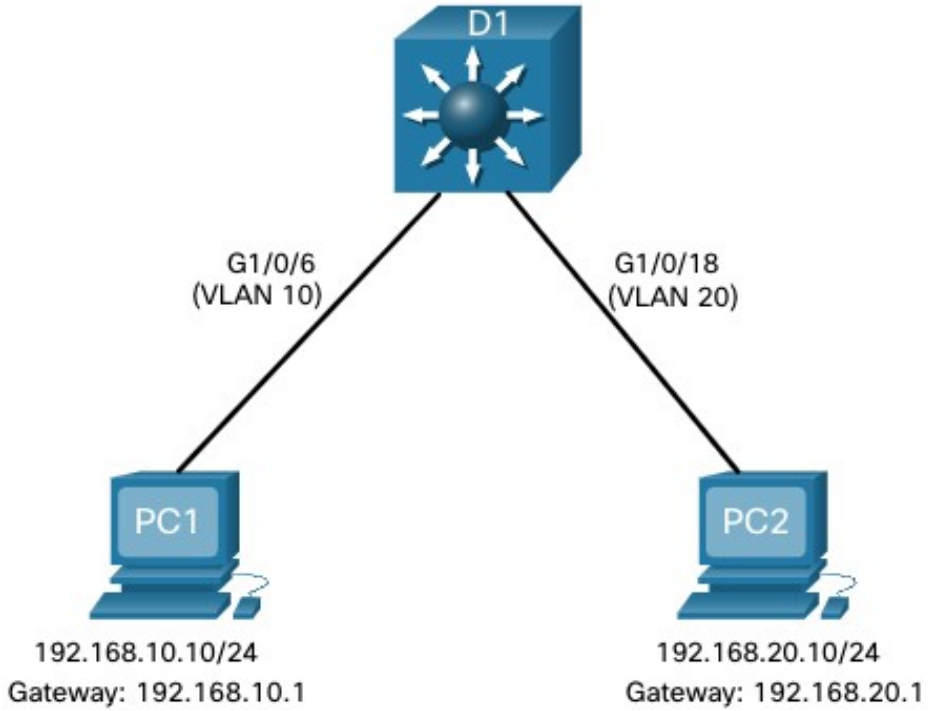
In the figure, the Layer 3 switch, D1, is connected to two hosts on different VLANs. PC1 is in VLAN 10 and PC2 is in VLAN 20, as shown. The Layer 3 switch will provide inter-VLAN routing services to the two hosts.



Layer 3 Switch Configuration

Complete the following steps to configure D1 with VLANs and trunking:

- **Step 1**. Create the VLANs. In the example, VLANs 10 and 20 are used.
- **Step 2**. Create the SVI VLAN interfaces. The IP address configured will serve as the default gateway for hosts in the respective VLAN.
- **Step 3**. Configure access ports. Assign the appropriate port to the required VLAN.
- **Step 4**. Enable IP routing. Issue the **ip routing** global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VAN routing on a Layer 3 switch for IPv4.



Layer 3 Switch Inter-VLAN Routing Verification

Inter-VLAN routing using a Layer 3 switch is simpler to configure than the router-on-a-stick method. After the configuration is complete, the configuration can be verified by testing connectivity between the hosts.

- From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.
- Next, verify connectivity with PC2 using the **ping** Windows host command. The successful **ping** output confirms inter-VLAN routing is operating.

Routing on a Layer 3 Switch

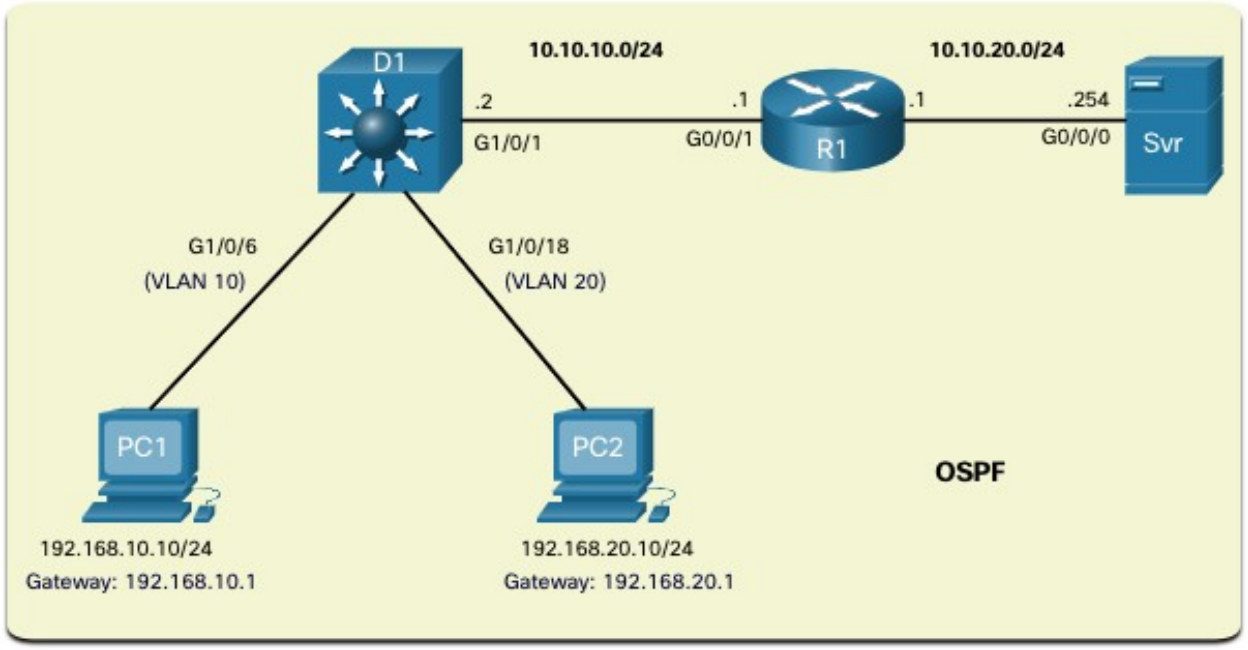
If VLANs are to be reachable by other Layer 3 devices, then they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the **no switchport** interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.

Routing Scenario on a Layer 3 Switch

In the figure, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.

Note: OSPF routing configuration is covered in another course. In this module, OSPF configuration commands will be given to you in all activities and assessments. It is not required that you understand the configuration in order to enable OSPF routing on the Layer 3 switch.



Routing Configuration on a Layer 3 Switch

Complete the following steps to configure D1 to route with R1:

Step 1. Configure the routed port. Use the **no switchport** command to convert the port to a routed port, then assign an IP address and subnet mask. Enable the port.

Step 2. Enable routing. Use the **ip routing** global configuration command to enable routing.

Step 3. Configure routing. Use an appropriate routing method. In this example, Single-Area OSPFv2 is configured

Step 4. Verify routing. Use the **show ip route** command.

Step 5. Verify connectivity. Use the **ping** command to verify reachability.

Common Inter-VLAN Issues

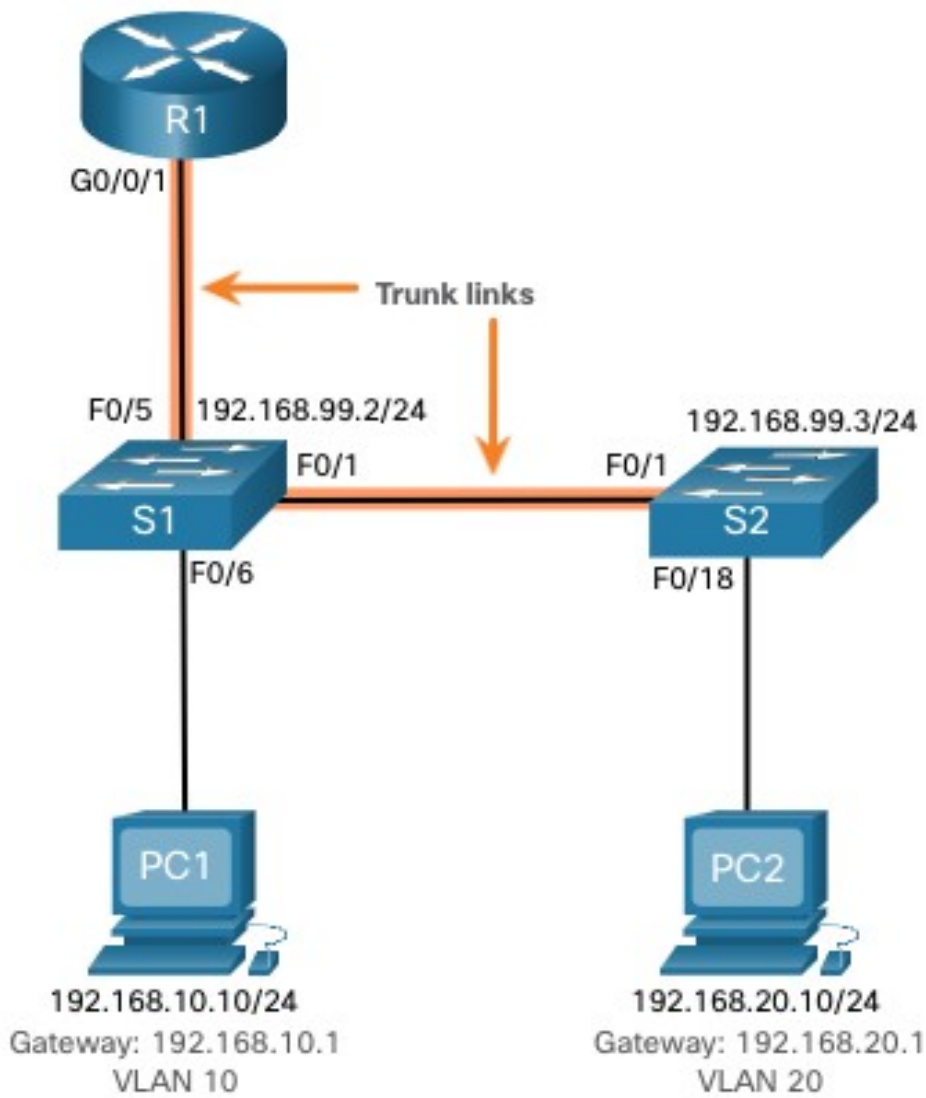
There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, then use the list in the table for other common reasons why inter-VLAN connectivity may fail.

Issue Type	How to Fix	How to Verify
Missing VLANs	•Create (or re-create) the VLAN if it does not exist. •Ensure host port is assigned to the correct VLAN.	**show vlan [brief]** **show interfaces switchport** **ping**
Switch Trunk Port Issues	•Ensure trunks are configured correctly. •Ensure port is a trunk port and enabled.	**show interface trunk** **show running-config**
Switch Access Port Issues	•Assign correct VLAN to access port. •Ensure port is an access port and enabled. •Host is incorrectly configured in the wrong subnet.	**show interfaces switchport** **show running-config interface** **ipconfig**
Router Configuration Issues	•Router subinterface IPv4 address is incorrectly configured. •Router subinterface is assigned to the VLAN ID.	**show ip interface brief** **show interfaces**

Troubleshoot Inter-VLAN Routing Scenario

Examples of some of these inter-VLAN routing problems will now be covered in more detail. This topology will be used for all of these issues.

Router R1 Subinterfaces		
Subinterface	**VLAN**	**IP Address**
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24



Missing VLANs

An inter-VLAN connectivity issue could be caused by a missing VLAN. The VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link.

When a VLAN is deleted, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN or recreate the missing VLAN. Recreating the missing VLAN would automatically reassign the hosts to it.

Use the **show interface** *interface-id* **switchport** command to verify the VLAN membership of the port.

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Switch Trunk Port Issues

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

- Verify that the port connecting to the router is correctly configured as a trunk link using the **show interface trunk** command.
- If that port is missing from the output, examine the configuration of the port with the **show running-config interface X** command to see how the port is configured.

```
S1# show interface trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```

Switch Access Port Issues

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

A common indicator of this issue is the PC having the correct address configuration (IP Address, Subnet Mask, Default Gateway), but being unable to ping its default gateway.

- Use the **show vlan brief**, **show interface X switchport** or **show running-config interface X** command to verify the interface VLAN assignment.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Router Configuration Issues

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations.

- Verify the subinterface status using the **show ip interface brief** command.
- Verify which VLANs each of the subinterfaces is on. To do so, the **show interfaces** command is useful but it generates a great deal of additional unrequired output. The command output can be reduced using IOS command filters. In this example, use the **include** keyword to identify that only lines containing the letters “Gig” or “802.1Q”

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

Réseaux fixes

Introduction IPv6

Luc Deneire

EII-5, Option Réseaux et Objets Connectés (ROC)

Coexistence de l'IPv4 et de l'IPv6

IPv4 et IPv6 coexisteront dans un proche avenir et la transition prendra plusieurs années.

L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être classées en trois catégories:

- **Double pile** -les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.
- **Tunneling** - méthode qui consiste à transporter un paquet IPv6 sur un réseau IPv4. Le paquet IPv6 est encapsulé dans un paquet IPv4.
- **Traduction** - La traduction d'adresse réseau 64 (NAT64) permet aux appareils compatibles IPv6 de communiquer avec les appareils compatibles IPv4 en utilisant une technique de traduction similaire à la NAT pour IPv4.

Remarque: Le tunneling et la traduction sont destinés à la transition vers IPv6 natif et ne doivent être utilisés qu'en cas de besoin. L'objectif doit être de communiquer de manière native via le protocole IPv6 depuis la source jusqu'à la destination.

Formats d'adressage IPv6

- Les adresses IPv6 ont une longueur de 128 bits et sont écrites en hexadécimal.
- Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.
- le format privilégié pour noter une adresseIPv6 est x:x:x:x:x:x:x:x, où chaque «x» est constitué de quatre valeurs hexadécimales.
- Pour les adresses IPv6, « hextet » est le terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales.
- Exemples d'adresses IPv6 au format privilégié.

  `2001:0db8:0000:1111:0000:0000:0000:0200` `2001:0db8:0000:00a3:abcd:0000:0000:1234`
- Règle 1 - Omettre le zéro de début (Leading Zero)

  `2001:db8:0:1111:0:0:0:200` `2001:0db8:0:a3:abcd:0:0:1234`

Règle 2 -Double Deux Points : Une suite de double deux-points (::) peut remplacer toute chaîne unique et continue d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros. Le double point (::) ne peut être utilisé qu'une seule fois dans une adresse, sinon il y aurait plusieurs adresses possibles.

`2001:db8:0:1111::200` `2001:db8:0:a3:abcd::1234`

Monodiffusion, Multidiffusion, Anycast

Il existe trois grandes catégories d'adresses IPv6 :

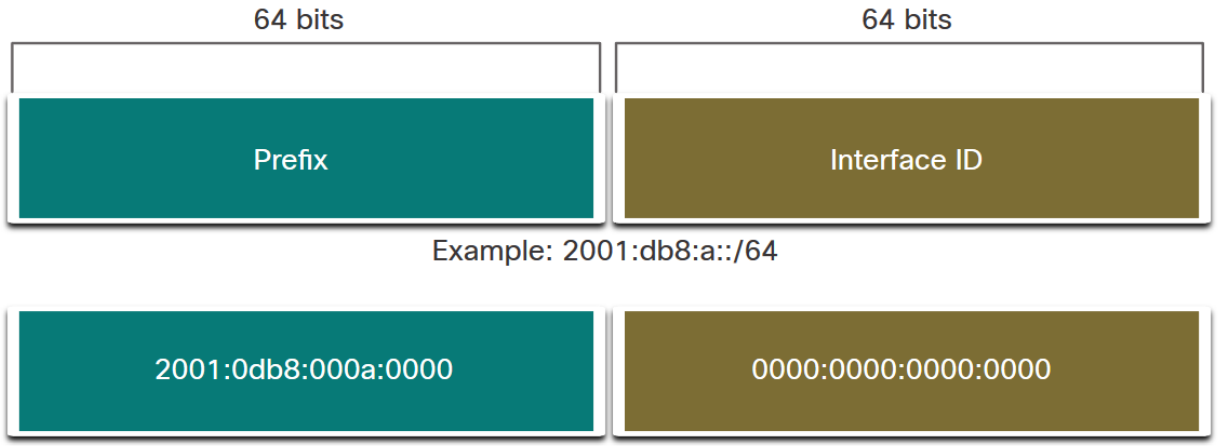
- **Monodiffusion** - La monodiffusion identifie de manière unique une interface sur un appareil compatible IPv6.
- **Multidiffusion** - La multidiffusion est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.
- **Anycast** - Il s'agit de toute adresse unicast IPv6 qui peut être attribuée à plusieurs appareils. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse.

Remarque: Contrairement à IPv4, IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion destinée à tous les nœuds IPv6 et qui offre globalement les mêmes résultats.

Longueur du préfixe IPv6

La longueur du préfixe IPv6 est utilisée pour indiquer la partie réseau de l'adresse IPv6:

La longueur de préfixe peut être comprise entre 0 et 128. La longueur du préfixe IPv6 recommandée pour les réseaux locaux et la plupart des autres types de réseaux est /64.

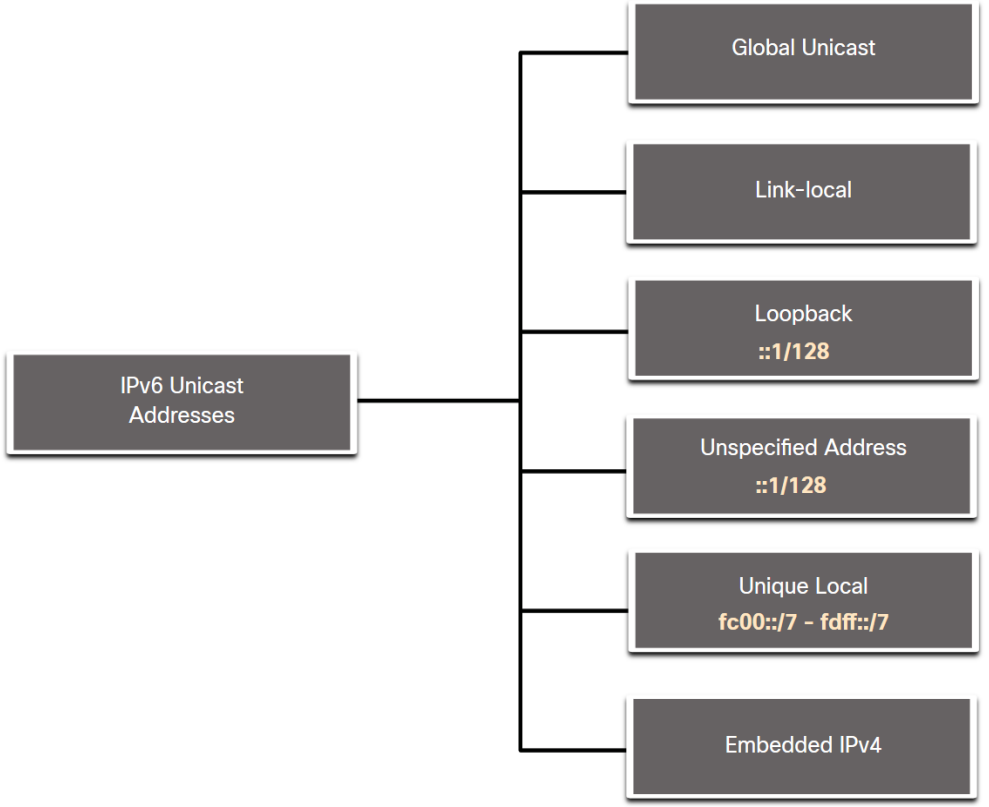


Remarque: Il est fortement recommandé d'utiliser un ID d'interface 64 bits pour la plupart des réseaux. En effet, la configuration automatique d'adresse sans état (SLAAC) utilise 64 bits pour l'ID d'interface. Il facilite également la création et la gestion des sous-réseaux.

Types d'adresses IPv6 Unicast

Contrairement aux périphériques IPv4 qui n'ont qu'une seule adresse, les adresses IPv6 ont généralement deux adresses monodiffusion :

- **Global Unicast Address (GUA)** –Cette adresse est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet.
- **Adresse locale de liaison (LLA)**- Requise pour chaque appareil compatible IPv6 et utilisée pour communiquer avec d'autres appareils sur la même liaison locale. Les LLA ne sont pas routables et se limitent à une seule liaison.



Une Remarque à propos de l'adresse locale unique

Les adresses locales uniques IPv6 (plage fc00::/7 à fdff::/7) présentent une certaine similitude avec les adresses privées RFC 1918 pour IPv4, mais il existe des différences significatives :

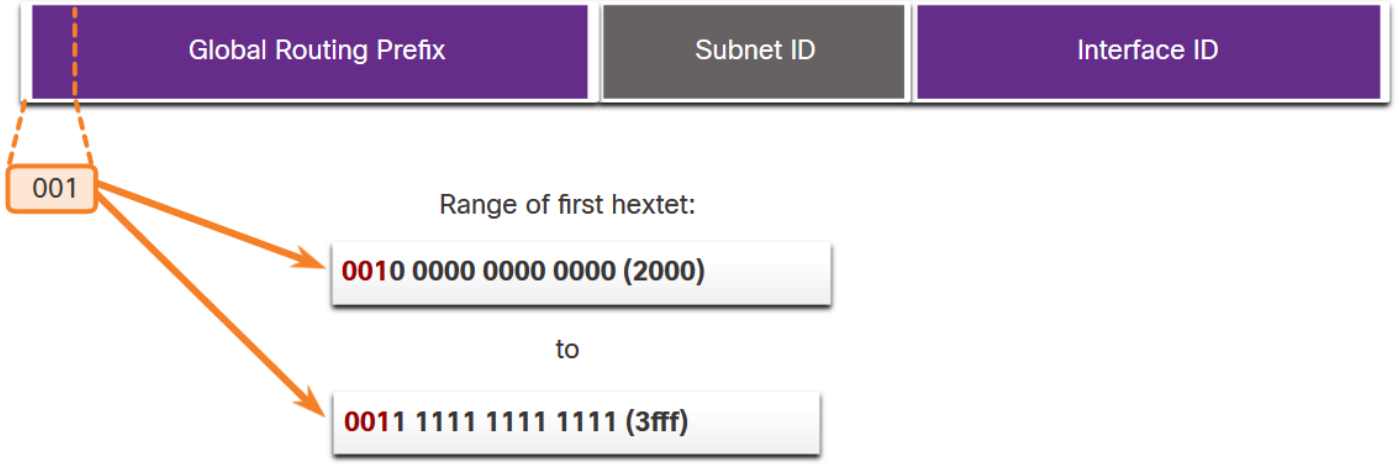
- Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites.
- Les adresses locales uniques peuvent être utilisées pour les périphériques qui n'auront jamais besoin d'être accessibles sur un autre réseau.
- Les adresses locales uniques ne sont pas routées globalement ou traduites en adresse IPv6 globale.

Remarque: de nombreux sites utilisent la nature privée des adresses RFC 1918 pour tenter de sécuriser ou de cacher leur réseau des risques potentiels de sécurité. Cela n'a jamais été l'utilisation prévue des ULA.

IPv6 GUA

Les adresses de diffusion globale (GUA) IPv6 sont uniques au monde et routables (Internet IPv6).

- Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::/3 sont attribuées
- Les GUA actuellement disponibles commencent par une décimale 2 ou 3 (Ceci représente seulement 1/8ème de l'espace d'adressage IPv6 total disponible).



IPv6 Structure GUA

Préfixe de routage global:

- Le préfixe de routage global est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un ISP) à un client ou à un site. Le préfixe de routage global varie en fonction des stratégies du fournisseur de services Internet.

ID de sous-réseau

- Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface. L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

ID d'interface

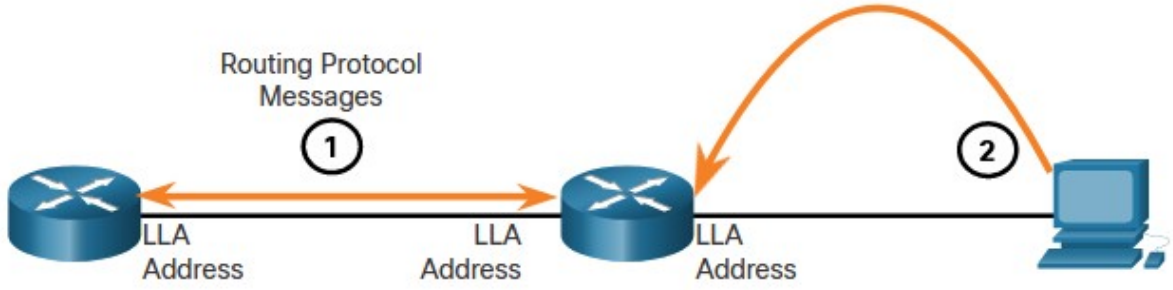
- L'ID d'interface IPv6 est l'équivalent de la partie hôte d'une adresse IPv4. Dans la plupart des cas, il est fortement recommandé d'utiliser des sous-réseaux /64, qui crée un ID d'interface de 64 bits.

Remarque: IPv6 permet d'attribuer des adresses d'hôte "tout 0" et "tout 1" à un appareil. L'adresse contenant uniquement des 0 peut également être utilisée, mais elle est réservée comme adresse anycast de routeur de sous-réseau, et elle ne doit être attribuée qu'aux routeurs.

IPv6 LLA

Une adresse link-local IPv6 (LLA) permet à un appareil de communiquer avec d'autres appareils IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau).

- Les paquets avec un LLA source ou de destination ne peuvent pas être routés.
- Chaque interface réseau compatible IPv6 doit avoir un LLA.
- Si un LLA n'est pas configuré manuellement sur une interface, le dispositif en créera un automatiquement.
- Les IPv6 LLAs sont dans la gamme fe80::/10.



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

Configuration statique GUA sur un routeur

La plupart des commandes de configuration et de vérification IPv6 de Cisco IOS sont semblables à celles utilisées pour l'IPv4. Dans de nombreux cas, la seule différence est l'utilisation d'**ipv6** au lieu d'**ip** dans les commandes.

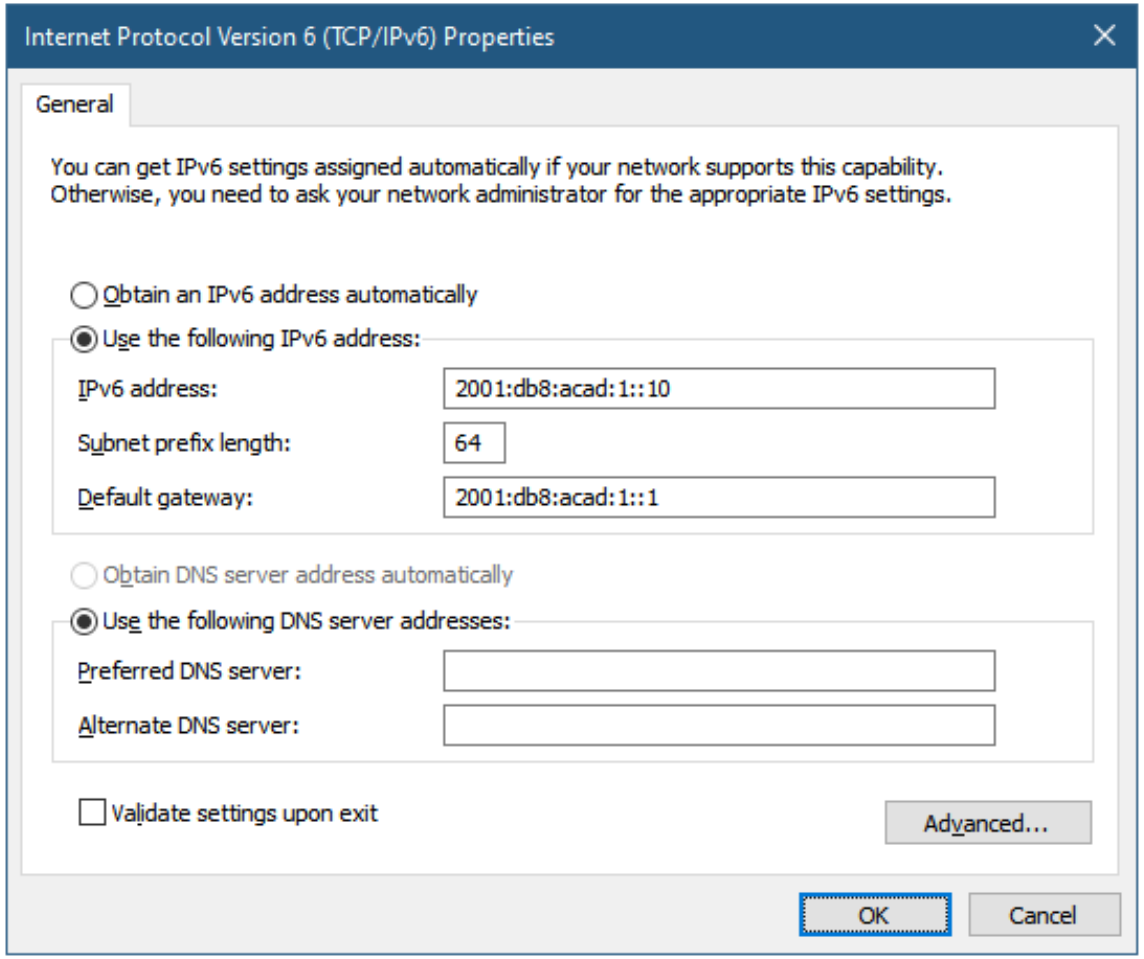
- La commande pour configurer une GUA IPv6 sur une interface est : **ipv6 adresse** *ipv6-adresse/prefix-length.*
- L'exemple montre les commandes pour configurer une GUA sur l'interface G0/0/0 sur R1 :

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

Configuration statique GUA sur un hôte Windows

- La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à celle d'une adresse IPv4.
- Le GUA ou LLA de l'interface du routeur peut être utilisé comme passerelle par défaut. La meilleure pratique consiste à utiliser le LLA.

Remarque: lorsque le DHCPv6 ou le SLAAC est utilisé, le LLA du routeur sera automatiquement spécifié comme adresse de passerelle par défaut.



Configuration statique d'une adresse monodiffusion Lien-Local

La configuration manuelle de l'adresse link-local permet de créer une adresse qui est reconnaissable et plus facile à mémoriser.

- Les LLA peuvent être configurés manuellement à l'aide de la commande **ipv6 address** *ipv6-link-local-address* **link-local** .
- L'exemple montre les commandes pour configurer un LLA sur l'interface G0/0/0 sur R1

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

Remarque: la même LLA peut être configurée sur chaque lien, à condition qu'elle soit unique sur ce lien. La pratique courante consiste à créer un LLA différent sur chaque interface du routeur pour faciliter l'identification du routeur et de l'interface spécifique.

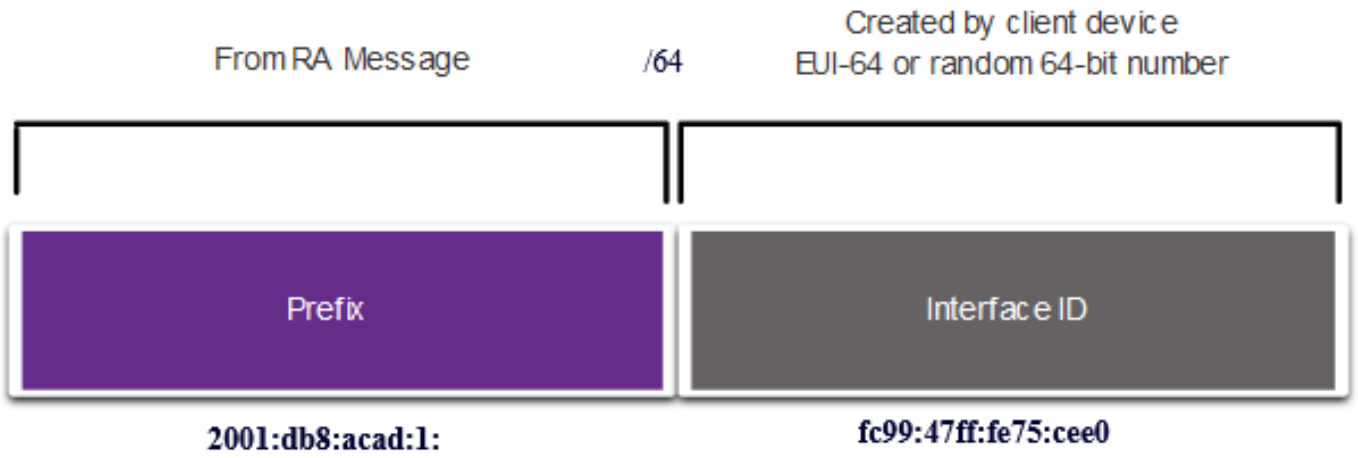
Messages RS et RA

Les périphériques obtiennent des adresses GUA dynamiquement via les messages ICMPv6 (Internet Control Message Protocol version 6).

- Les messages de sollicitation de routeur (RS) sont envoyés par les périphériques hôtes pour découvrir les routeurs IPv6
- Les messages de publicité de routeur (RA) sont envoyés par les routeurs pour informer les hôtes sur la façon d'obtenir une GUA IPv6 et fournir des informations réseau utiles telles que :
  - Préfixe réseau et longueur du préfixe
  - L'adresse de la passerelle par défaut
  - Adresses DNS et nom de domaine
- Le RA peut fournir trois méthodes pour configurer une IPv6 GUA :
  - SLAAC
  - SLAAC avec serveur DHCPv6 apatride
  - DHCPv6 avec état (pas de SLAAC)

Méthode 1: SLAAC

- SLAAC permet à un périphérique de configurer une GUA sans les services de DHCPv6.
- Les périphériques obtiennent les informations nécessaires pour configurer une GUA à partir des messages RA ICMPv6 du routeur local.
- Le préfixe est fourni par le RA et le périphérique utilise soit la méthode EUI-64, soit la méthode de génération aléatoire pour créer un ID d'interface.

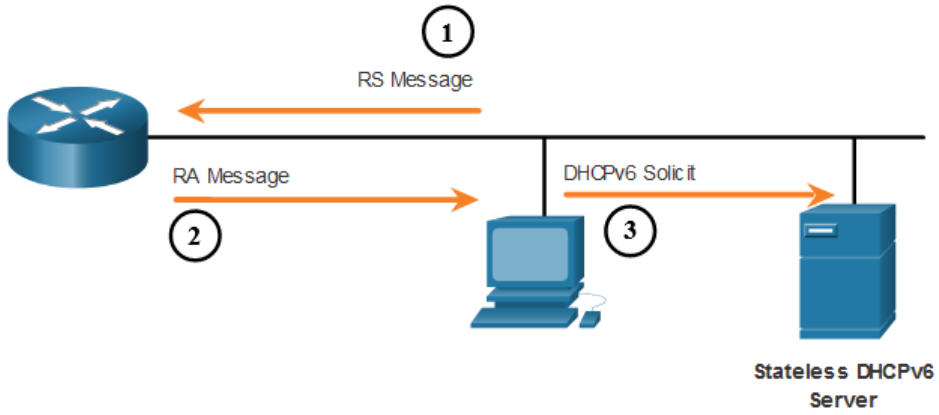


Méthode 2: SLAAC et DHCP sans état

Un RA peut demander à un périphérique d'utiliser à la fois SLAAC et DHCPv6 sans état.

Le message RA suggère que les appareils utilisent les éléments suivants :

- SLAAC pour créer sa propre IPv6 GUA
- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 sans état pour obtenir d'autres informations telles que l'adresse d'un serveur DNS et un nom de domaine.



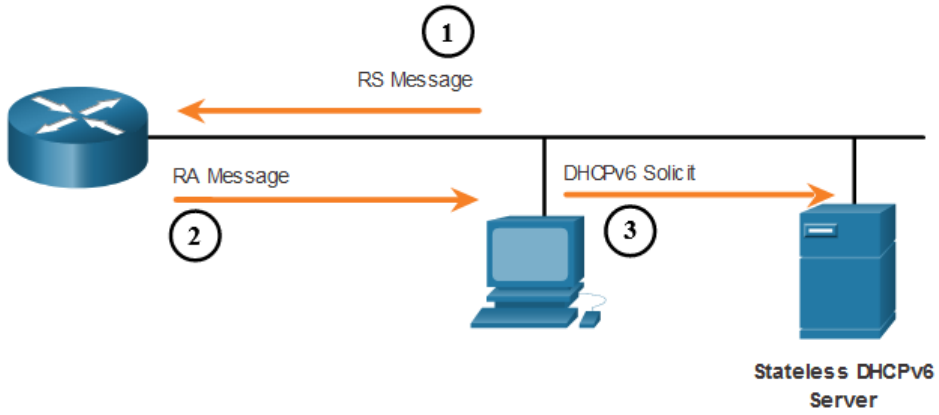
Méthode 3: DHCPv6 avec état

Un RA peut demander à un périphérique d'utiliser uniquement DHCPv6 avec état.

DHCPv6 avec état est similaire à DHCP pour IPv4. Un périphérique peut recevoir automatiquement une GUA, une longueur de préfixe et les adresses des serveurs DNS à partir d'un serveur DHCPv6 avec état.

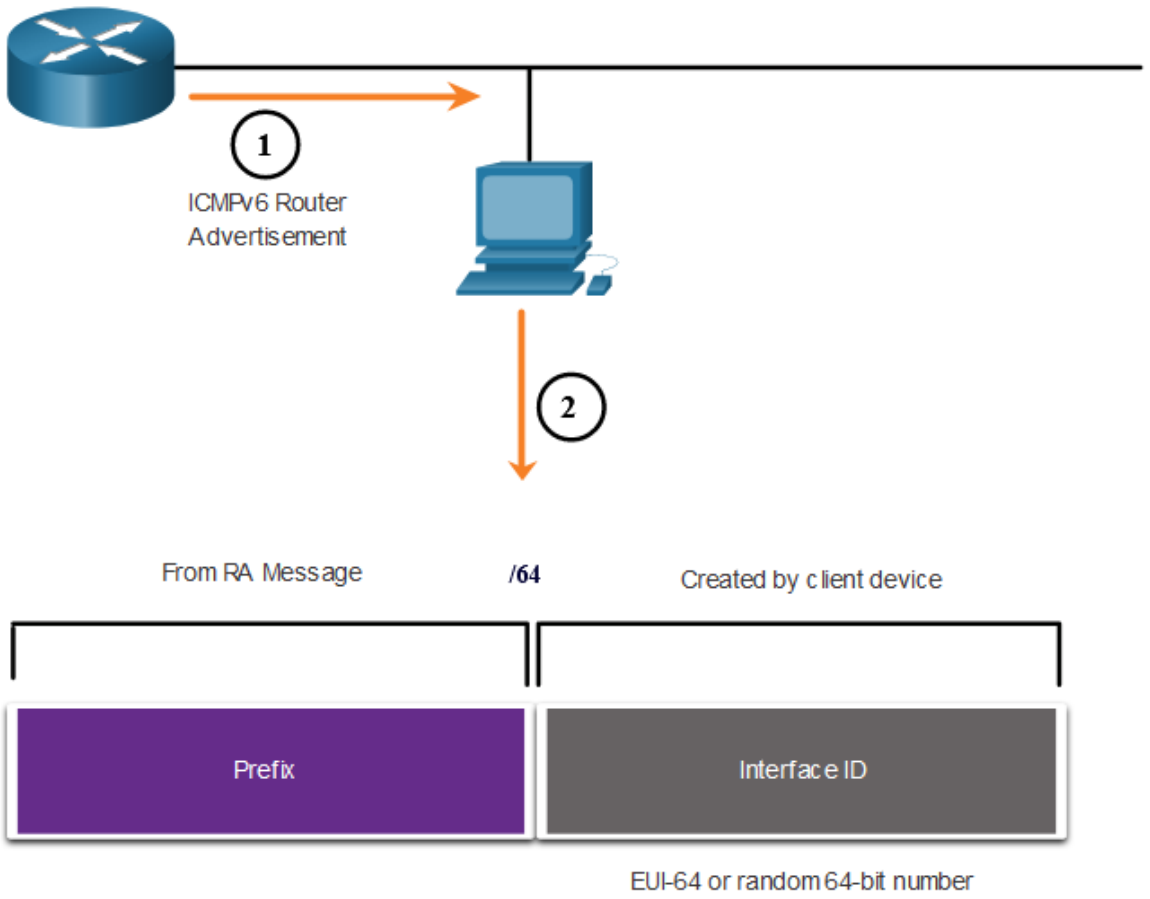
Le message RA suggère que les appareils utilisent les éléments suivants :

- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 avec état pour obtenir une adresse de diffusion globale, l'adresse d'un serveur DNS, un nom de domaine et toutes les autres informations.



Processus EUI-64 contre génération aléatoire

- Lorsque le message d'annonce de routeur est la SLAAC seule ou la SLAAC avec DHCPv6 sans état, le client doit générer lui-même son ID d'interface.
- L'interface ID peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement.



Processus EUI-64

L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié.

- Une valeur 16 bits de fffe (en hexadécimal) est insérée au milieu de l'adresse MAC Ethernet 48 bits du client.
- Le 7e bit de l'adresse MAC du client est inversé du binaire 0 à 1.
- Exemple :

MAC 48 bits	fc:99:47:75:ce:e0
ID d'interface EUI-64	fe:99:47:ff:fe:75:ce:e0

Identifiants d'interface générés de manière aléatoire

Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64.

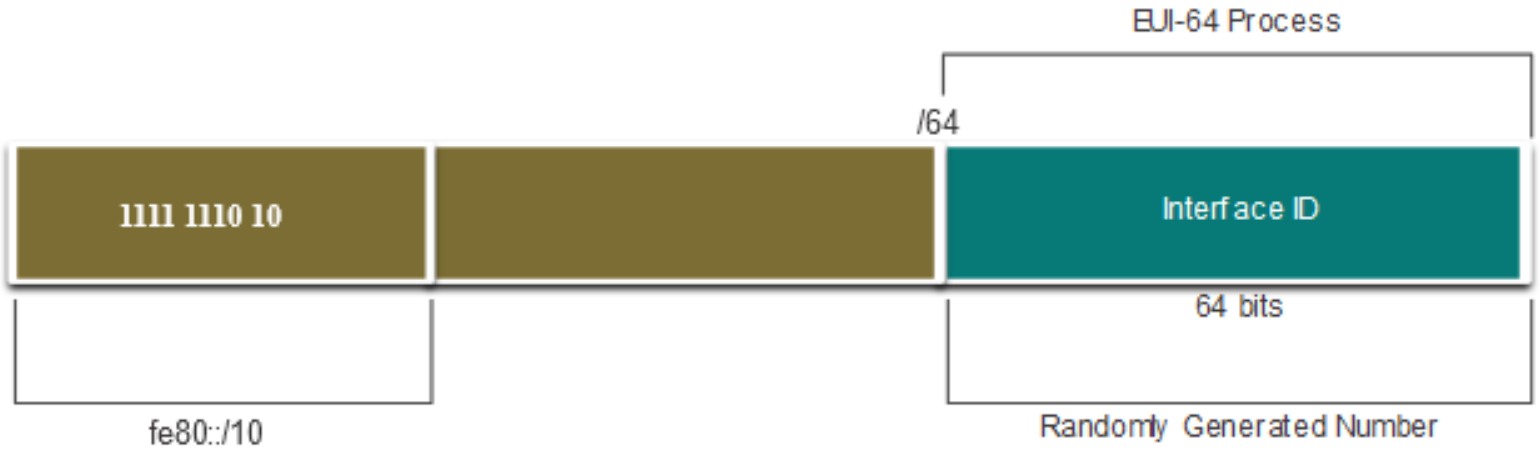
À partir de la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec le processus EUI-64.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Suffixe DNS propre à la connexion . :
IPv6 Address. . . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . .: fe80::1
C:\ >
```

Remarque: pour s'assurer que les adresses de monodiffusion IPv6 sont uniques, le client peut utiliser le processus de détection d'adresse dupliquée (DAD). Le principe est similaire à une requête ARP pour sa propre adresse. En l'absence de réponse, l'adresse est unique.

LLA dynamiques

- Toutes les interfaces IPv6 doivent avoir un IPv6 LLA.
- Comme les IPv6 GUA, les LLA peuvent être configurés dynamiquement.
- La figure montre que l'adresse link-local est créée dynamiquement à partir du préfixe FE80::/10 et de l'ID d'interface à l'aide de la méthode EUI-64 ou d'un nombre à 64 bits généré aléatoirement.



LLA dynamiques sur Windows

Les systèmes d'exploitation, tels que Windows, utiliseront généralement la même méthode pour une GUA créée par SLAAC et une LLA attribuée dynamiquement.

ID d'interface généré par la méthode EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . .: fe80::1
C:\ >
```

ID d'interface généré aléatoirement sur 64 bits :

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . .: fe80::1
C:\ >
```

Vérifier la configuration de l'adresse IPv6

Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface. Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6.

Voici un exemple d'un LLA configuré dynamiquement sur l'interface G0/0/0 de R1 :

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640  (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Adresses de multidiffusion IPv6 attribuées

Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8. Il existe deux types d'adresses de multidiffusion IPv6 :

- Les adresses de multidiffusion bien connues
- Adresses de multidiffusion de nœud sollicité

Remarque: les adresses de multidiffusion ne peuvent être que des adresses de destination et non des adresses source.

Adresses de multidiffusion IPv6 bien connues

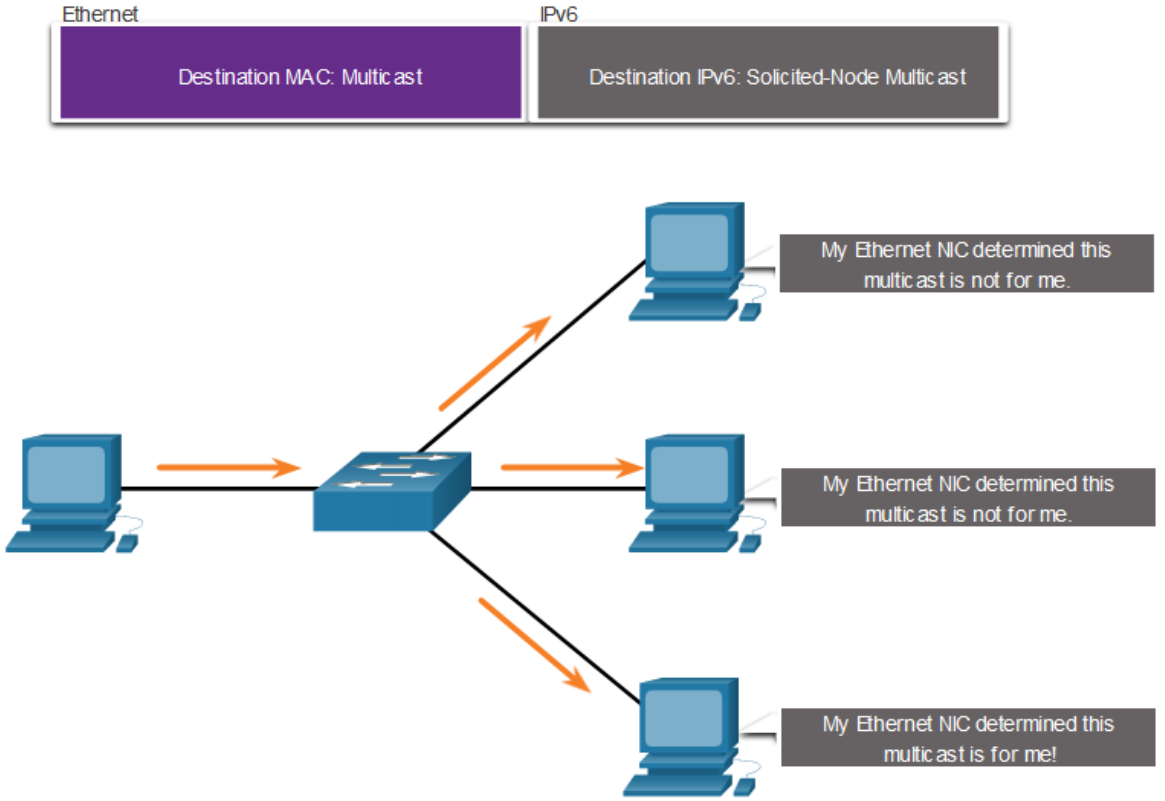
Des adresses de multidiffusion IPv6 bien connues sont attribuées et sont réservées à des groupes d'appareils prédéfinis.

Il existe deux groupes communs de multidiffusion assignés par IPv6 :

- **ff02::1 All-nodes multicast group** - Il s'agit d'un groupe de multidiffusion que tous les appareils compatibles IPv6 rejoignent. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau.
- **ff02::2 All-routers multicast group** - Il s'agit d'un groupe multicast que tous les routeurs IPv6 rejoignent. Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec la commande de configuration globale **ipv6 unicast-routing** .

Noeud sollicité IPv6 Multicast

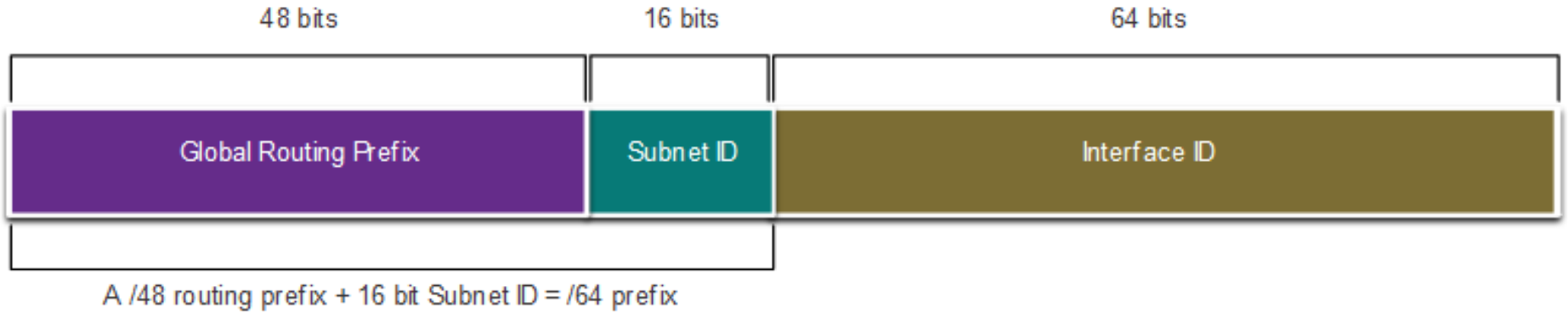
- Une adresse de multidiffusion de nœud sollicité est comparable à une adresse de multidiffusion à tous les nœuds.
- Une adresse de multidiffusion à noeud sollicité est mise en correspondance avec une adresse de multidiffusion Ethernet spéciale.
- Cela permet à la carte réseau Ethernet de filtrer la trame en examinant l'adresse MAC de destination sans l'envoyer au processus IPv6 pour voir si le périphérique est la cible prévue du paquet IPV6.



Sous-réseautage utilisant l'ID de sous-réseau

IPv6 a été conçu en pensant au sous-réseau.

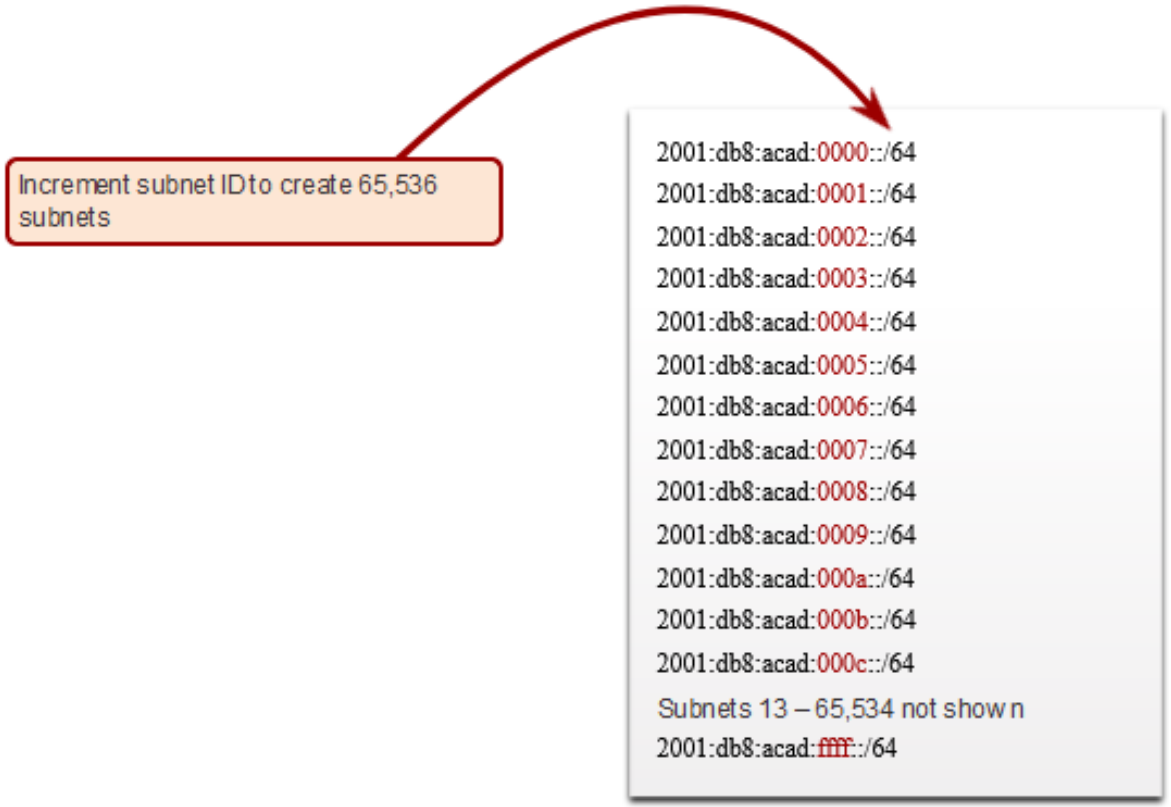
- Un champ d'ID de sous-réseau distinct dans la GUA IPv6 est utilisé pour créer des sous-réseaux.
- Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface.



Exemple de sous-réseautage IPv6

Étant donné le préfixe de routage global 2001:db8:acad::/48 avec un ID de sous-réseau de bits.

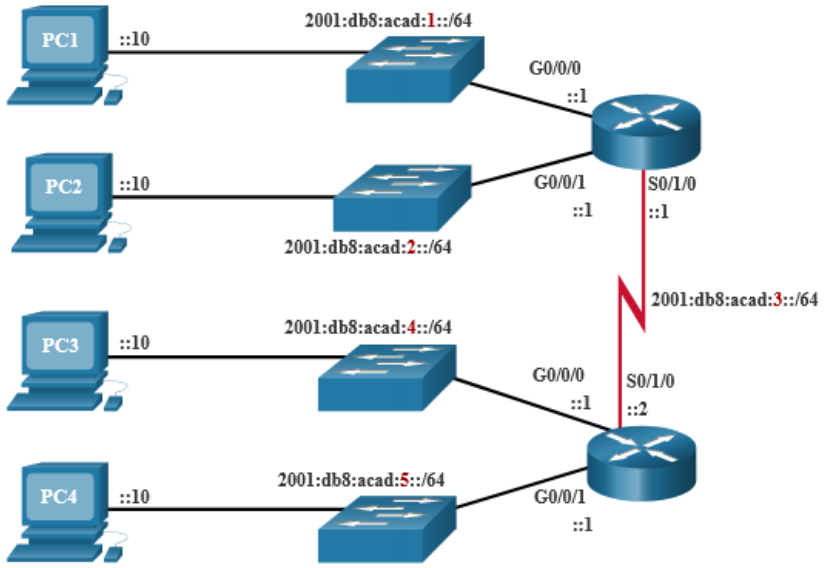
- Permet 65 536 /64 sous-réseaux
- Le préfixe de routage global est le même pour tous les sous-réseaux.
- Seul l'hexagone d'identification du sous-réseau est incrémenté en hexadécimal pour chaque sous-réseau

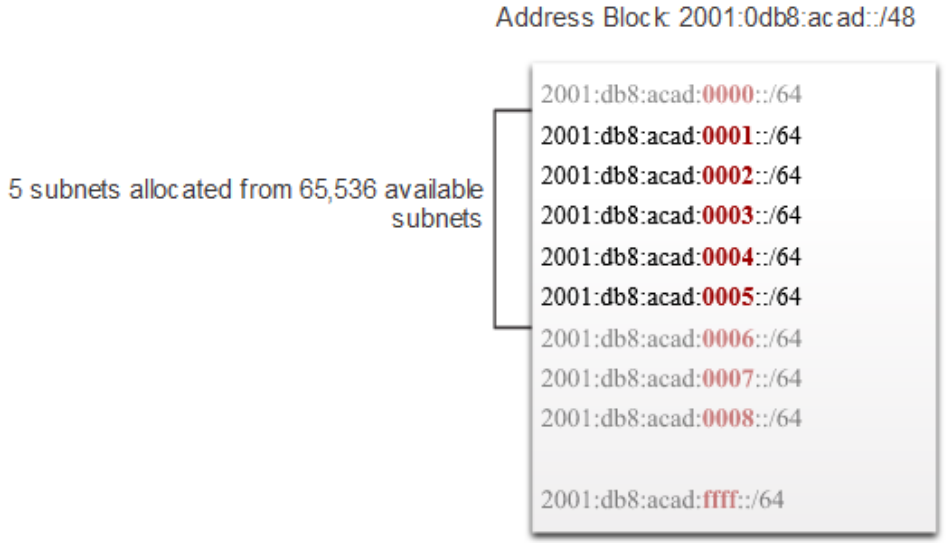


Allocation de sous-réseau IPv6

La topologie de l'exemple nécessite cinq sous-réseaux, un pour chaque réseau local ainsi que pour la liaison série entre R1 et R2.

Les cinq sous-réseaux IPv6 ont été alloués, avec les champs d'ID de sous-réseau 0001 à 0005. Chaque sous-réseau /64 propose plus d'adresses qu'il ne sera jamais nécessaire.





Routeur configuré avec des sous-réseaux IPv6

Comme pour la configuration IPv4, l'exemple indique que chacune des interfaces du routeur a été configurée pour utiliser un sous-réseau IPv6 différent.

Note, la commande “ ipv6 unicast-routing” active le routage ipv6, qui est désactivé par défaut

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```