

Lecture 7

IPv6 Addressing. ICMP

Objectives

**Implement an IPv6
Addressing scheme**

**IPv6 Address
Types**

IPv6 subnetting



IPv4 Issues

IPv4 Issues

Need for IPv6

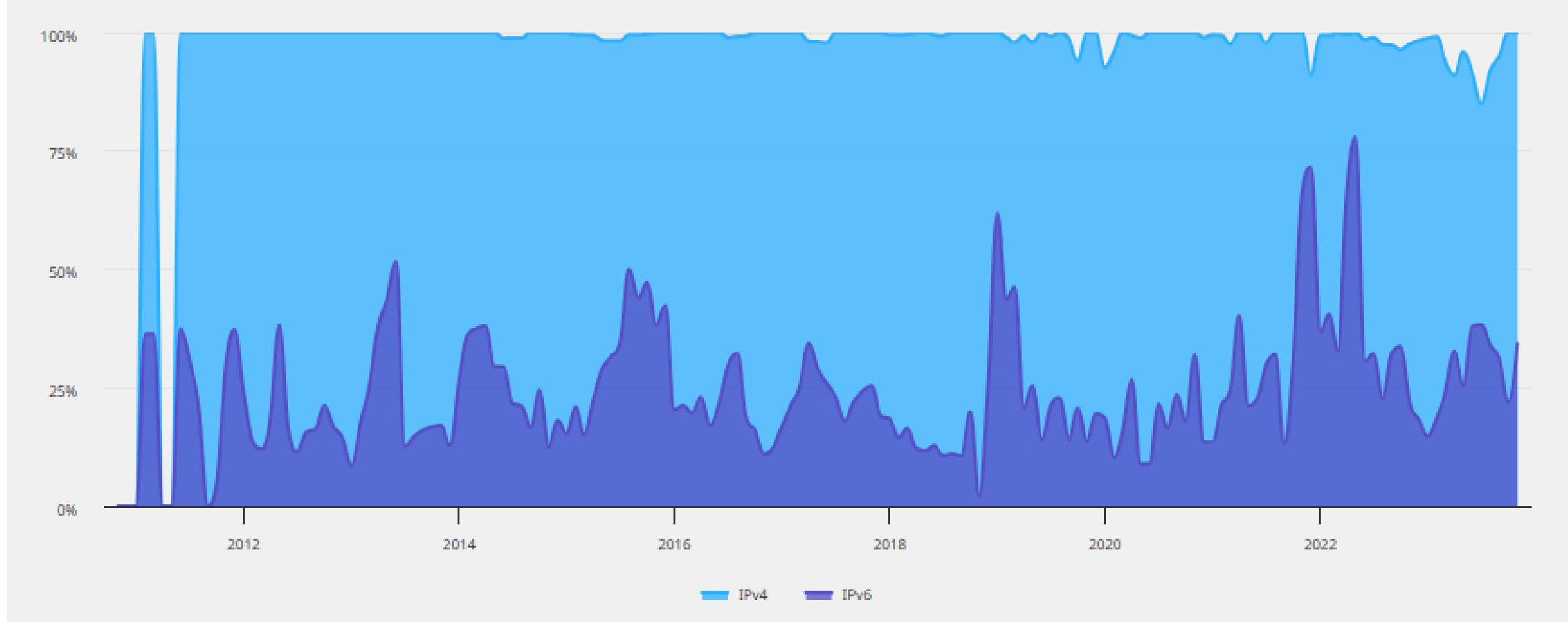
- IPv4 is running out of addresses. IPv6 is the successor to IPv4. IPv6 has a much larger 128-bit address space.
- The development of IPv6 also included fixes for IPv4 limitations and other enhancements.
- With an increasing internet population, a limited IPv4 address space, issues with NAT and the IoT, the time has come to begin the transition to IPv6.



This graph shows the evolution of IPv6 support vs IPv4 for all our connection test.

The numbers are percentages, so we can expect almost 100% of hosts supporting IPv4 with a slow growth for IPv6.

Overall IPv6 and v4 protocol support in Kazakhstan



IPv4 and IPv6 Coexistence

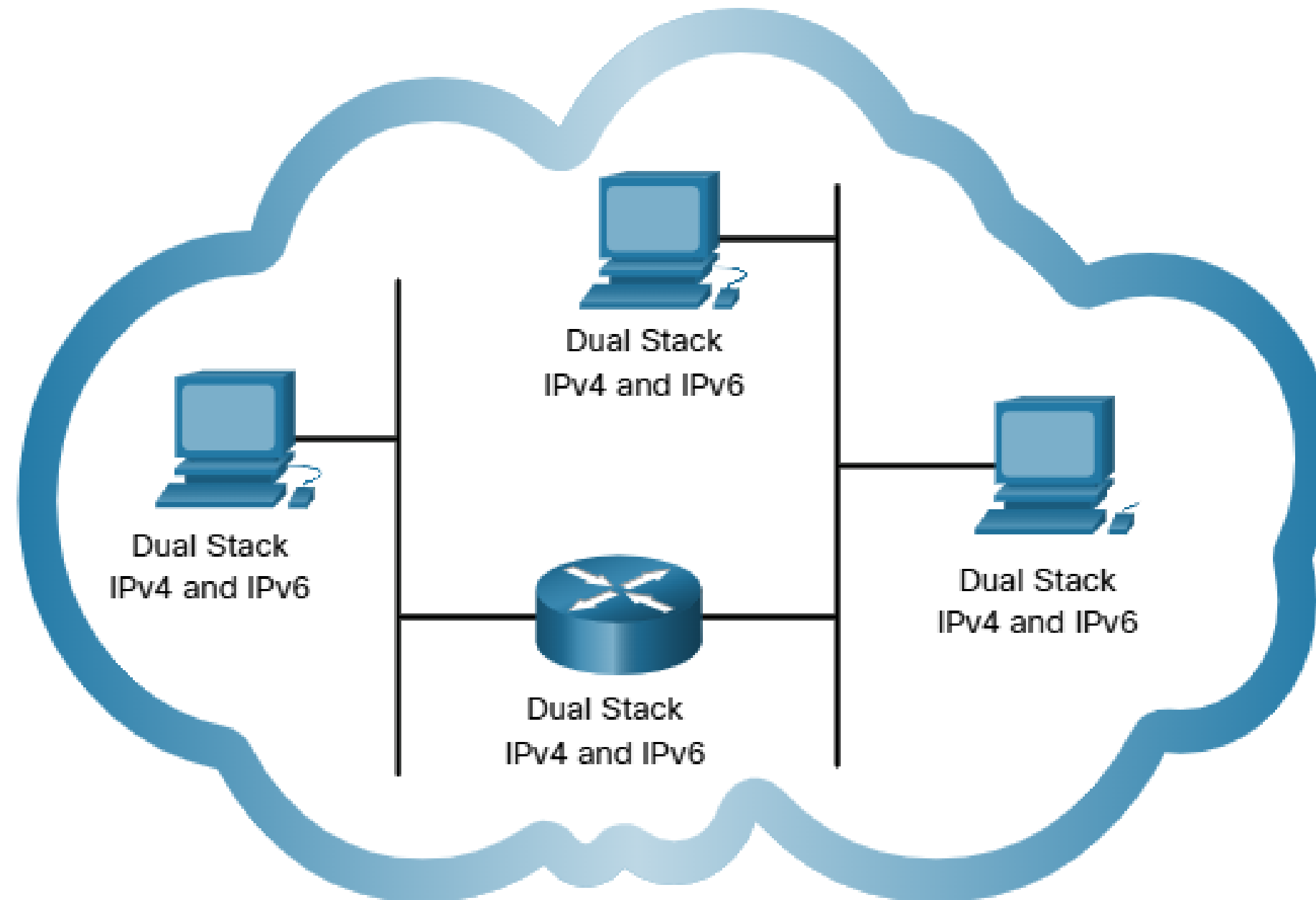
Both IPv4 and IPv6 will coexist in the near future and the transition will take several years.

The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. These migration techniques can be divided into three categories:

- **Dual stack** -The devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling** – A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.
- **Translation** - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4.

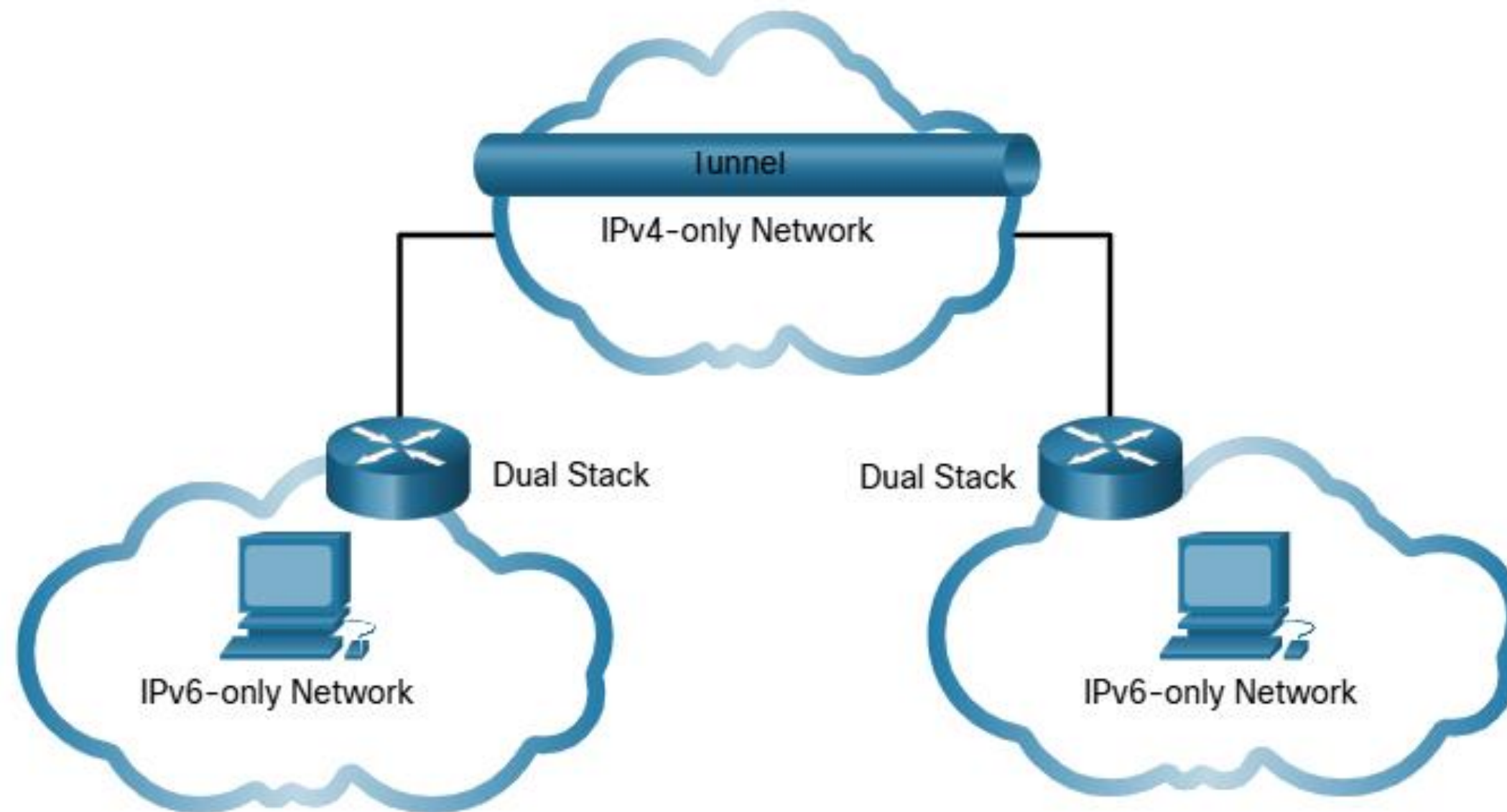
IPv4 and IPv6 Coexistence

- **Dual stack** - Dual stack allows IPv4 and IPv6 to coexist on the same network segment. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously. Known as native IPv6, this means the customer network has an IPv6 connection to their ISP and is able to access content found on the internet over IPv6.



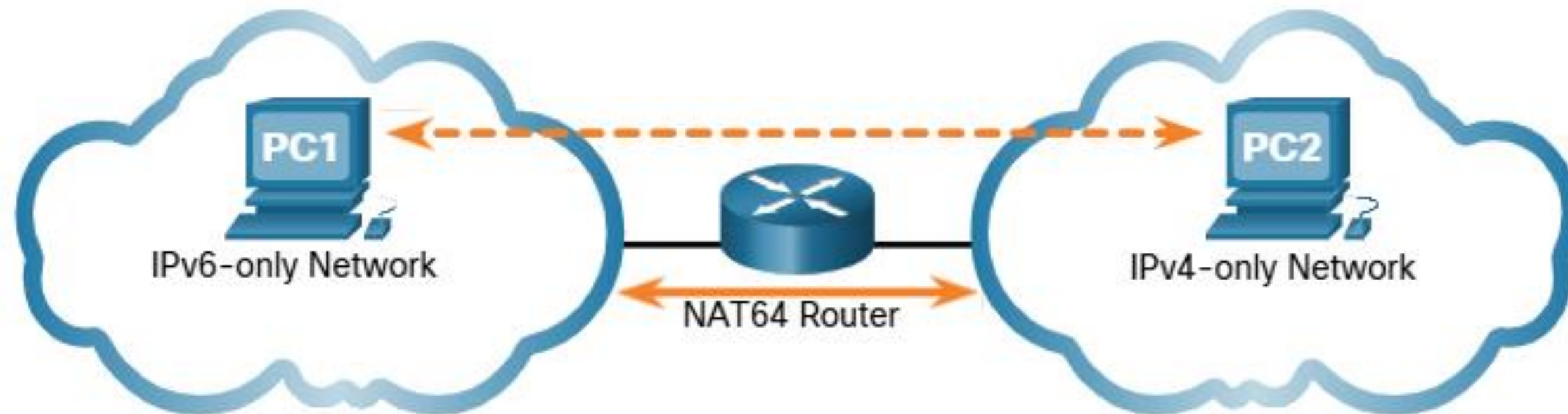
IPv4 and IPv6 Coexistence

- **Tunneling** is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.



IPv4 and IPv6 Coexistence

- **Translation** - Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and an IPv4 packet is translated to an IPv6 packet.





IPv6 Address Representation

IPv6 Address Representation

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written in hexadecimal.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values.
- In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234

X : X : X : X : X : X : X : X

0000 0000 0000 0000 0000 0000 0000 0000
to : to : to : to : to : to
ffff ffff ffff ffff ffff ffff ffff ffff

4 hexadecimal digits = 16 binary digits

0000 0000 0000 0000
to to to to
1111 1111 1111 1111

Rule 1 – Omit Leading Zero

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros).

Examples:

- 01ab can be represented as 1ab
- 09f0 can be represented as 9f0
- 0a00 can be represented as a00
- 00ab can be represented as ab

Note: This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous.

Type	Format
Preferred	2001 : 0 db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0 200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

IPv6 Address Representation

Rule 2 – Double Colon

A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

Example:

- 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

Note: The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressed	2001:db8:0:1111::200

IPv6 Address Types

Unicast, Multicast, Anycast

There are three broad categories of IPv6 addresses:

- **Unicast** – Unicast uniquely identifies an interface on an IPv6-enabled device.
- **Multicast** – Multicast is used to send a single IPv6 packet to multiple destinations.
- **Anycast** – This is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address.

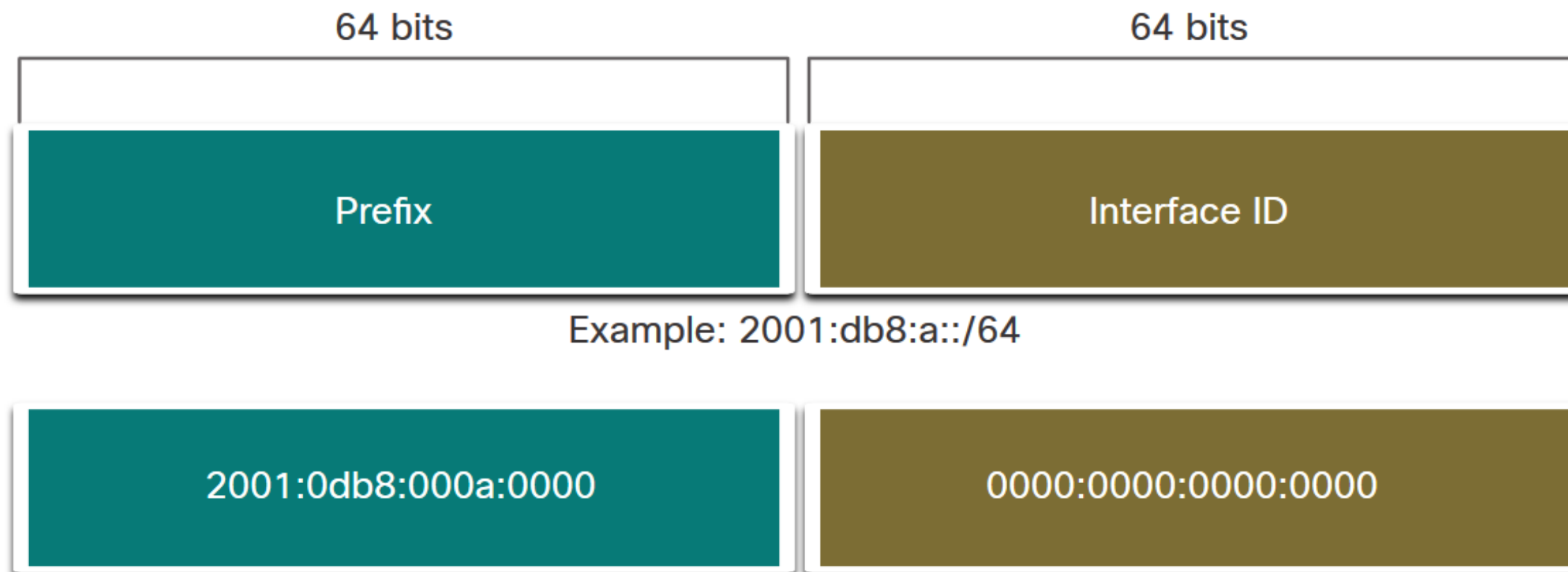
Note: Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Address Types

IPv6 Prefix Length

Prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address.

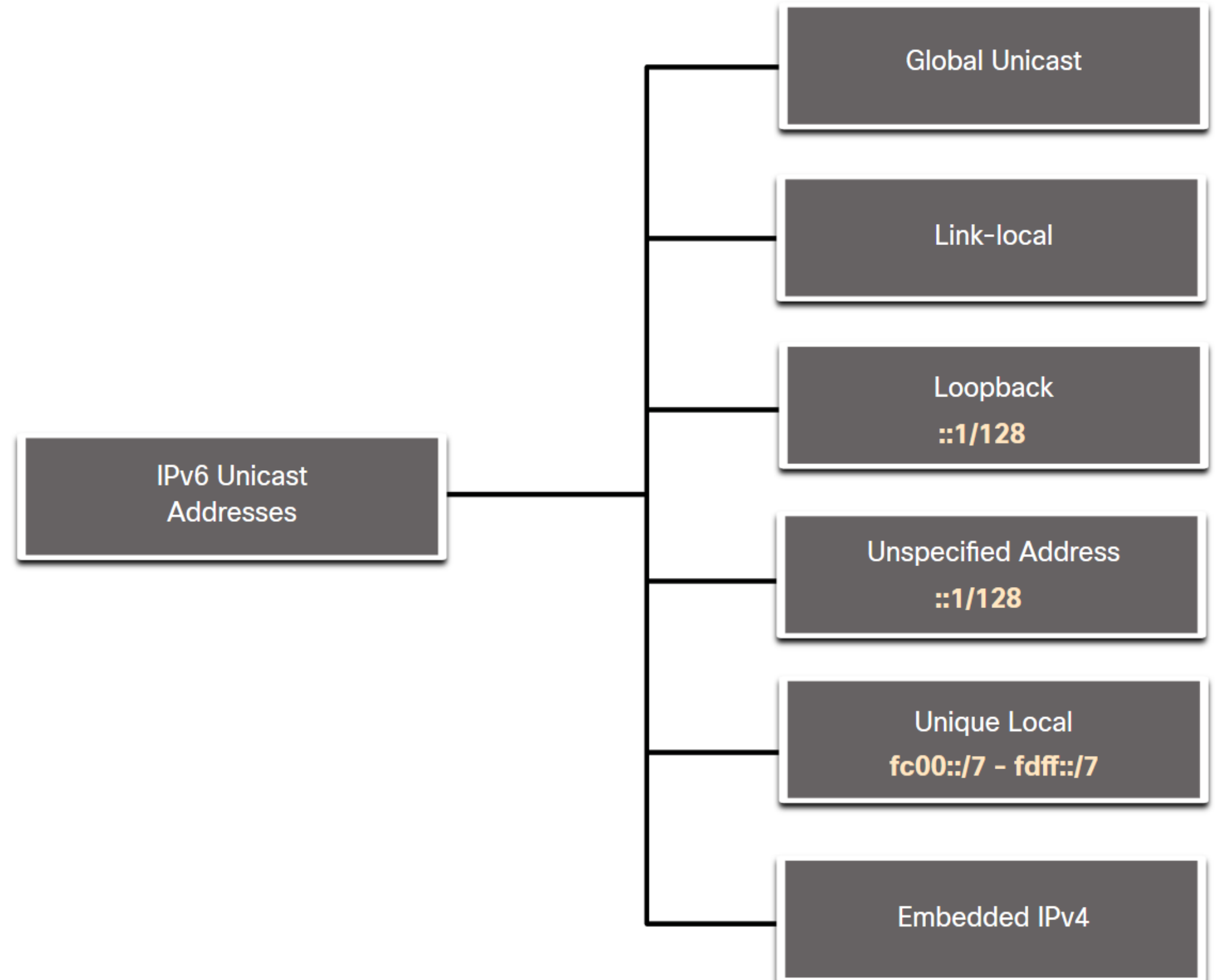
The IPv6 prefix length can range from 0 to 128. The recommended IPv6 prefix length for LANs and most other types of networks is /64.



Types of IPv6 Unicast Addresses

Unlike IPv4 devices that have only a single address, IPv6 addresses typically have two unicast addresses:

- **Global Unicast Address (GUA)** – This is similar to a public IPv4 address. These are globally unique, internet-routable addresses.
- **Link-local Address (LLA)** - Required for every IPv6-enabled device and used to communicate with other devices on the same local link. LLAs are not routable and are confined to a single link.



A Note About the Unique Local Address

The IPv6 unique local addresses (range fc00::/7 to fdff::/7) have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences:

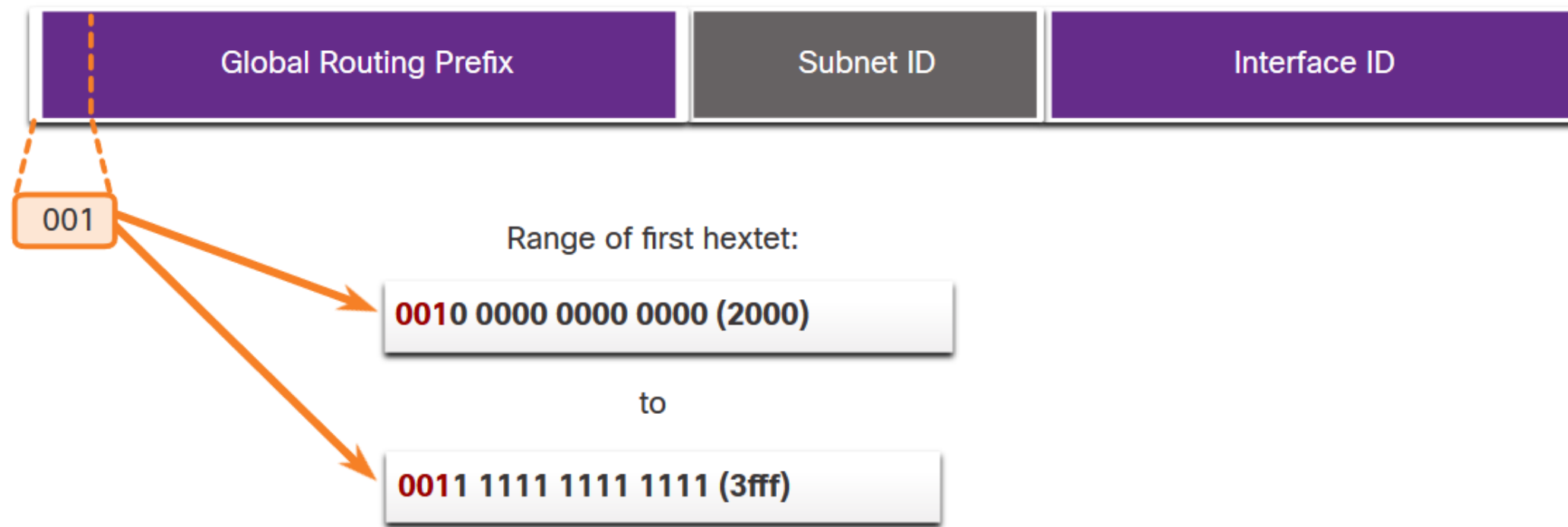
- Unique local addresses are used for local addressing within a site or between a limited number of sites.
- Unique local addresses can be used for devices that will never need to access another network.
- Unique local addresses are not globally routed or translated to a global IPv6 address.

IPv6 Address Types

IPv6 GUA

IPv6 global unicast addresses (GUAs) are globally unique and routable on the IPv6 internet.

- Currently, only GUAs with the first three bits of 001 or 2000::/3 are being assigned.
- Currently available GUAs begins with a decimal 2 or a 3 (This is only 1/8th of the total available IPv6 address space).



IPv6 Address Types

IPv6 GUA Structure

Global Routing Prefix:

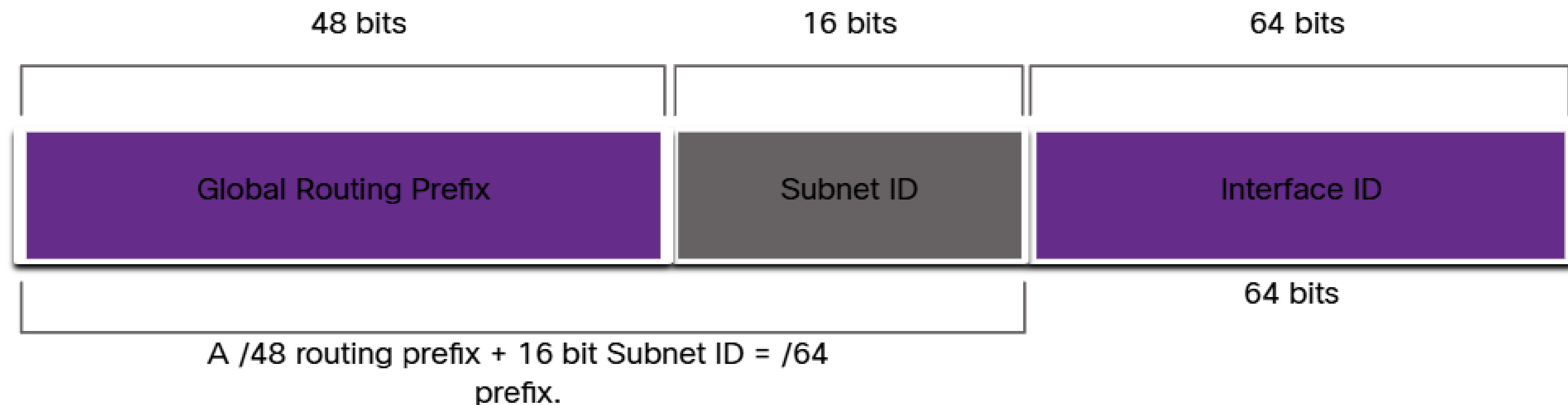
- The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. The global routing prefix will vary depending on ISP policies.

Subnet ID:

- The Subnet ID field is the area between the Global Routing Prefix and the Interface ID. The Subnet ID is used by an organization to identify subnets within its site.

Interface ID:

- The IPv6 interface ID is equivalent to the host portion of an IPv4 address. It is strongly recommended that in most cases /64 subnets should be used, which creates a 64-bit interface ID.

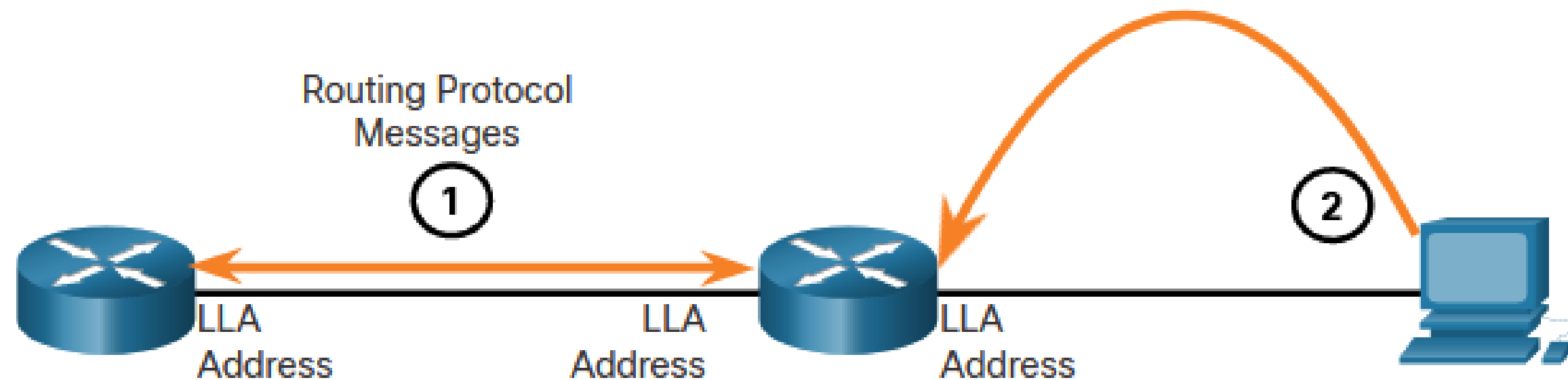


IPv6 Address Types

IPv6 LLA

An IPv6 link-local address (LLA) enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).

- Packets with a source or destination LLA cannot be routed.
- Every IPv6-enabled network interface must have an LLA.
- If an LLA is not configured manually on an interface, the device will automatically create one.
- IPv6 LLAs are in the fe80::/10 range.



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.

GUA and LLA Static Configuration

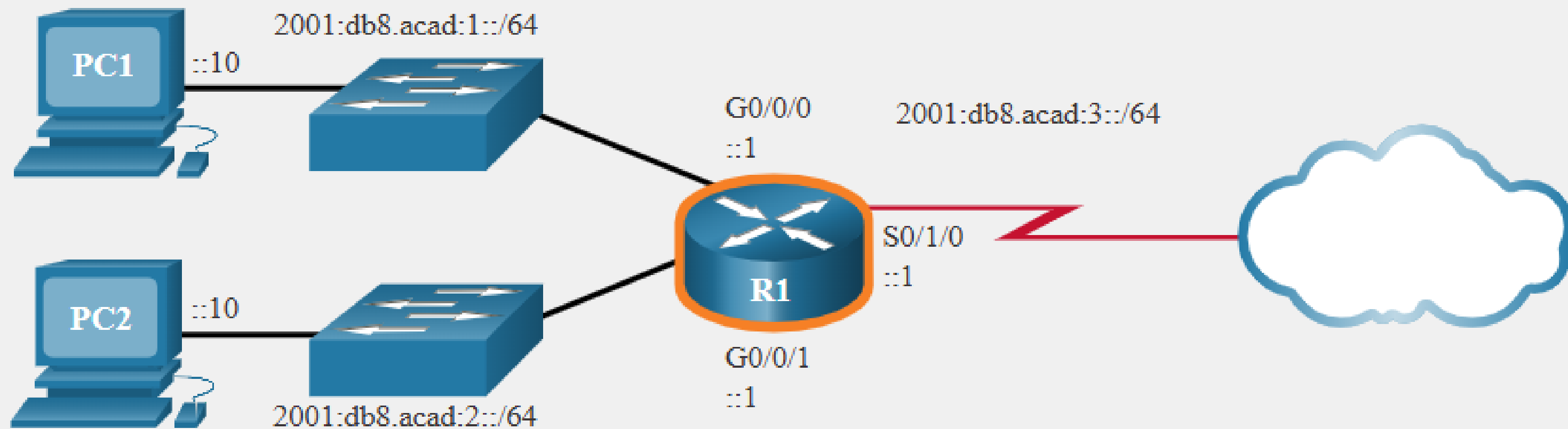
Static GUA Configuration on a Router

Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of **ipv6** in place of **ip** within the commands.

- The command to configure an IPv6 GUA on an interface is: **ipv6 address *ipv6-address/prefix-length***.
- The example shows commands to configure a GUA on the G0/0/0 interface on 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
```

Example Topology



```
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
```

GUA and LLA Static Configuration

Static GUA Configuration on a Windows Host

- Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address.
- The GUA or LLA of the router interface can be used as the default gateway. Best practice is to use the LLA.

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:acad:1::10

Subnet prefix length: 64

Default gateway: 2001:db8:acad:1::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

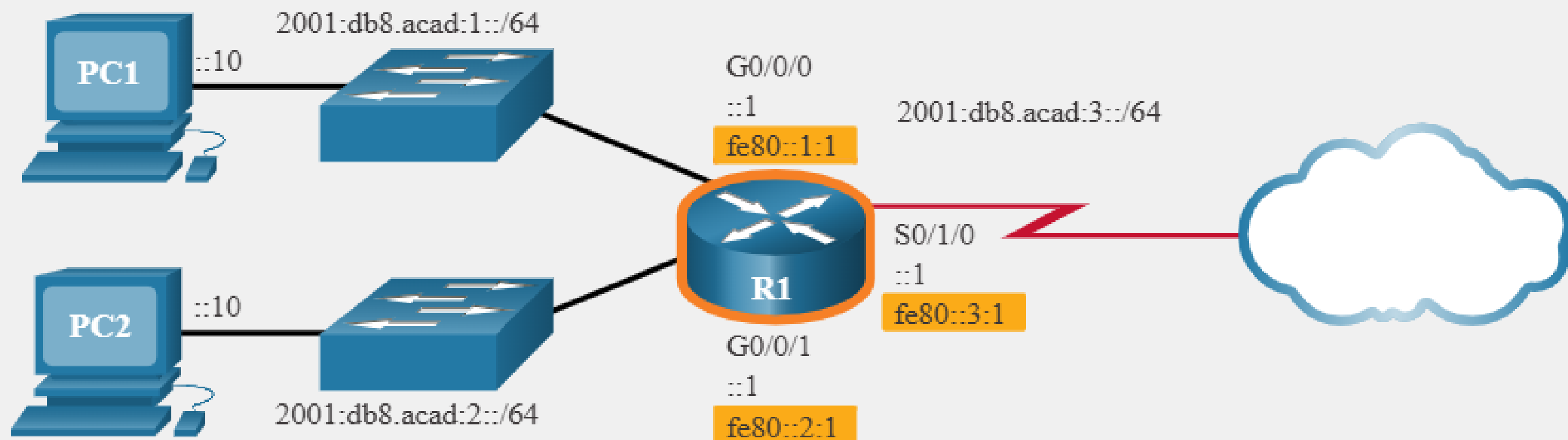
Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

Example Topology with LLAs



Static GUA Configuration of a Link-Local Unicast Address

Configuring the LLA manually lets you create an address that is recognizable and easier to remember.

- LLAs can be configured manually using the **ipv6 address *ipv6-link-local-address* link-local** command.
- The example shows commands to configure a LLA on the G0/0/0 interface on 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
```

Note: The same LLA can be configured on each link as long as it is unique on that link. Common practice is to create a different LLA on each interface of the router to make it easy to identify the router and the specific interface.

Questions

Which three are characteristics of an IPv6 anycast address? (Choose three)

- A. one-to-many communication model
- B. one-to-nearest communication model
- C. any-to-many communication model
- D. a unique IPv6 address for each device in the group
- E. the same address for multiple devices in the group
- F. delivery of packets to the group interface that is closest to the sending device

Which two are features of IPv6? (Choose two)

- A. multicast
- B. broadcast
- C. allcast
- D. podcast
- E. anycast

Which three approaches can be used while migrating from an IPv4 addressing scheme to an IPv6 scheme? (Choose three)

- A. static mapping of IPv4 address to IPv6 addresses
- B. configuring IPv4 tunnels between IPv6 islands
- C. use DHCPv6 to map IPv4 addresses to IPv6 addresses
- D. use proxying and translation (NAT-PT) to translate IPv6 packets into IPv4 packets
- E. configure IPv6 directly
- F. enable dual-stack routing

Which command enables IPv6 forwarding on a cisco router?

- A. IPv6 host
- B. IPv6 unicast-routing
- C. IPv6 local
- D. IPv6 neighbor

Which two statements describe characteristics of IPv6 unicast addressing? (Choose two)

- A. Global addresses start with 2000::/3
- B. Link-local addresses start with FE00:/12
- C. Link-local addresses start with FF00::/10
- D. There is only one loopback address and it is ::1
- E. If a global address is assigned to an interface, then that is the only allowable address for the interface.

What is known as “one-to-nearest” addressing in IPv6?

- A. global unicast
- B. anycast
- C. multicast
- D. unspecified address

Dynamic Addressing for IPv6 GUAs

Dynamic Addressing for IPv6 GUAs

RS and RA Messages

Router Advertisement (RA) messages

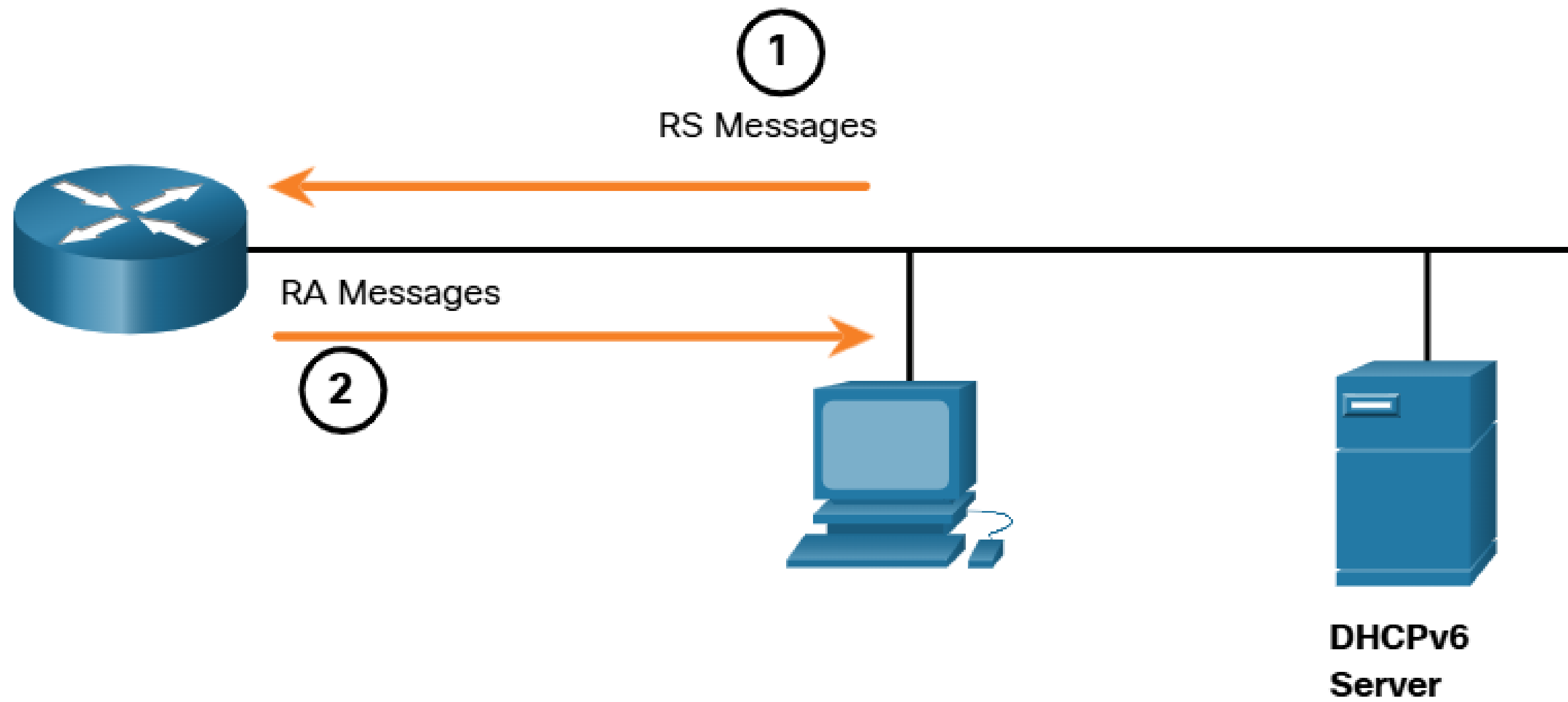
Router Solicitation (RS) messages

The ICMPv6 RA message is a suggestion to a device on how to obtain an IPv6 GUA. The ultimate decision is up to the device operating system. The ICMPv6 RA message includes the following:

Network prefix and prefix length - This tells the device which network it belongs to.

Default gateway address - This is an IPv6 LLA, the source IPv6 address of the RA message.

DNS addresses and domain name - These are the addresses of DNS servers and a domain name.



Dynamic Addressing for IPv6 GUAs

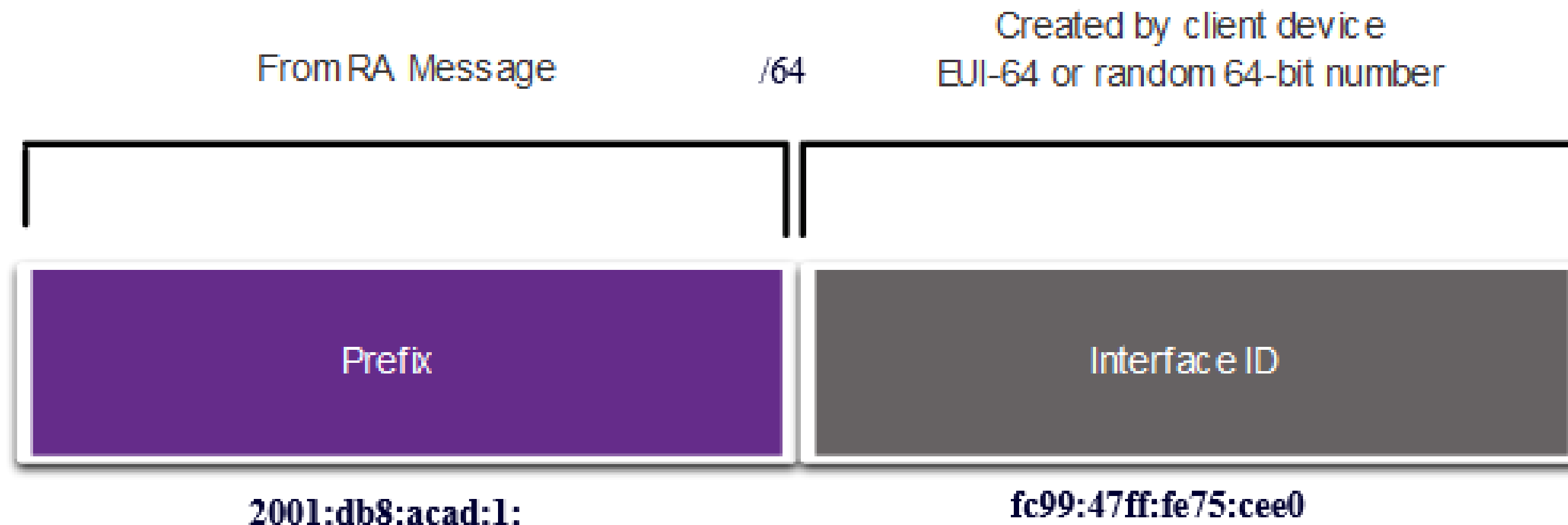
RS and RA Messages

- There are three methods for RA messages:
- Method 1: SLAAC - “I have everything you need including the prefix, prefix length, and default gateway address.”
- Method 2: SLAAC with a stateless DHCPv6 server - “Here is my information but you need to get other information such as DNS addresses from a stateless DHCPv6 server.”
- Method 3: Stateful DHCPv6 (no SLAAC) - “I can give you your default gateway address. You need to ask a stateful DHCPv6 server for all your other information.”

Dynamic Addressing for IPv6 GUAs

Method 1: SLAAC

- SLAAC allows a device to configure a GUA without the services of DHCPv6.
- Devices obtain the necessary information to configure a GUA from the ICMPv6 RA messages of the local router.
- The prefix is provided by the RA and the device uses either the EUI-64 or random generation method to create an interface ID.

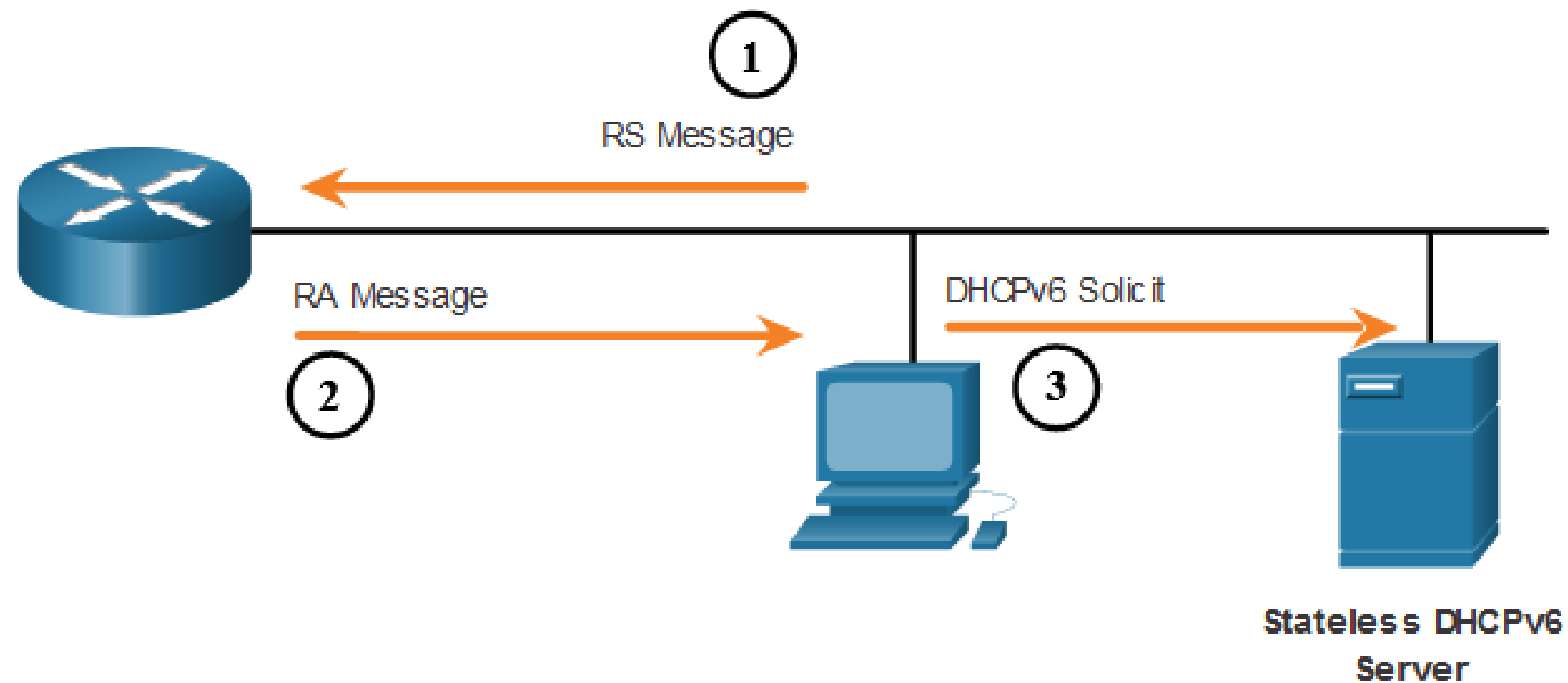


Method 2: SLAAC and Stateless DHCP

An RA can instruct a device to use both SLAAC and stateless DHCPv6.

The RA message suggests devices use the following:

- SLAAC to create its own IPv6 GUA
- The router LLA, which is the RA source IPv6 address, as the default gateway address
- A stateless DHCPv6 server to obtain other information such as a DNS server address and a domain name



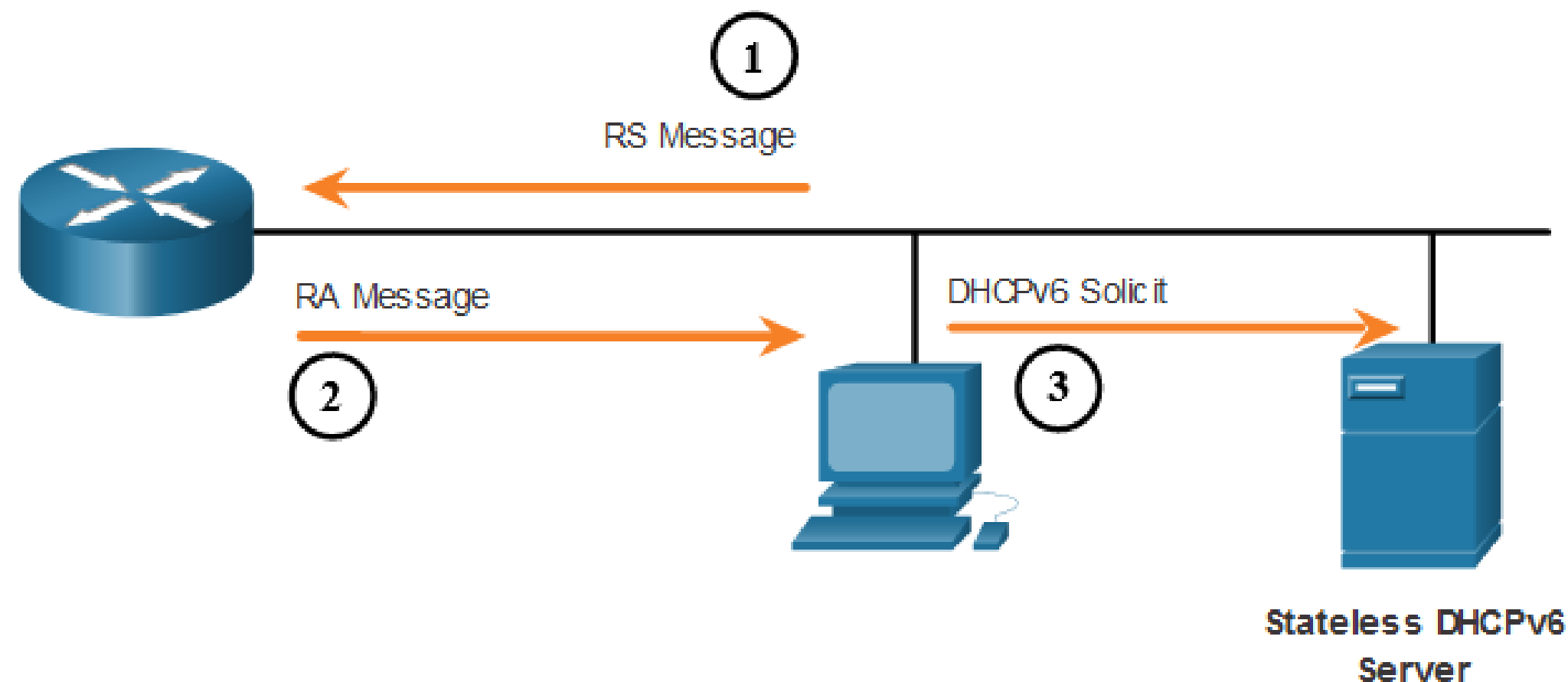
Method 3: Stateful DHCPv6

An RA can instruct a device to use stateful DHCPv6 only.

Stateful DHCPv6 is similar to DHCP for IPv4. A device can automatically receive a GUA, prefix length, and the addresses of DNS servers from a stateful DHCPv6 server.

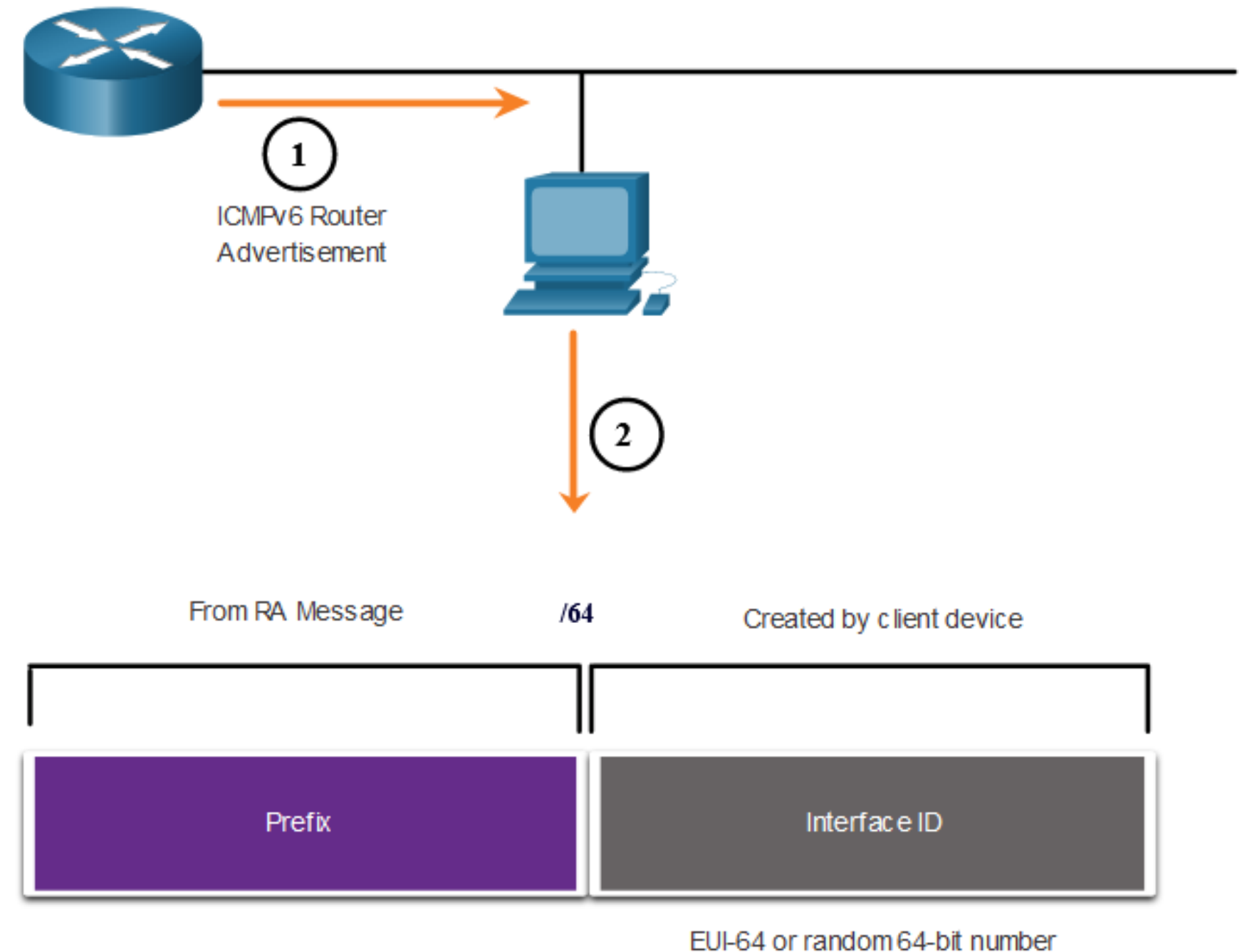
The RA message suggests devices use the following:

- The router LLA, which is the RA source IPv6 address, for the default gateway address.
- A stateful DHCPv6 server to obtain a GUA, DNS server address, domain name and other necessary information.



EUI-64 Process vs. Randomly Generated

- When the RA message is either SLAAC or SLAAC with stateless DHCPv6, the client must generate its own interface ID.
- The interface ID can be created using the EUI-64 process or a randomly generated 64-bit number.



EUI-64 Process

The IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process which performs the following:

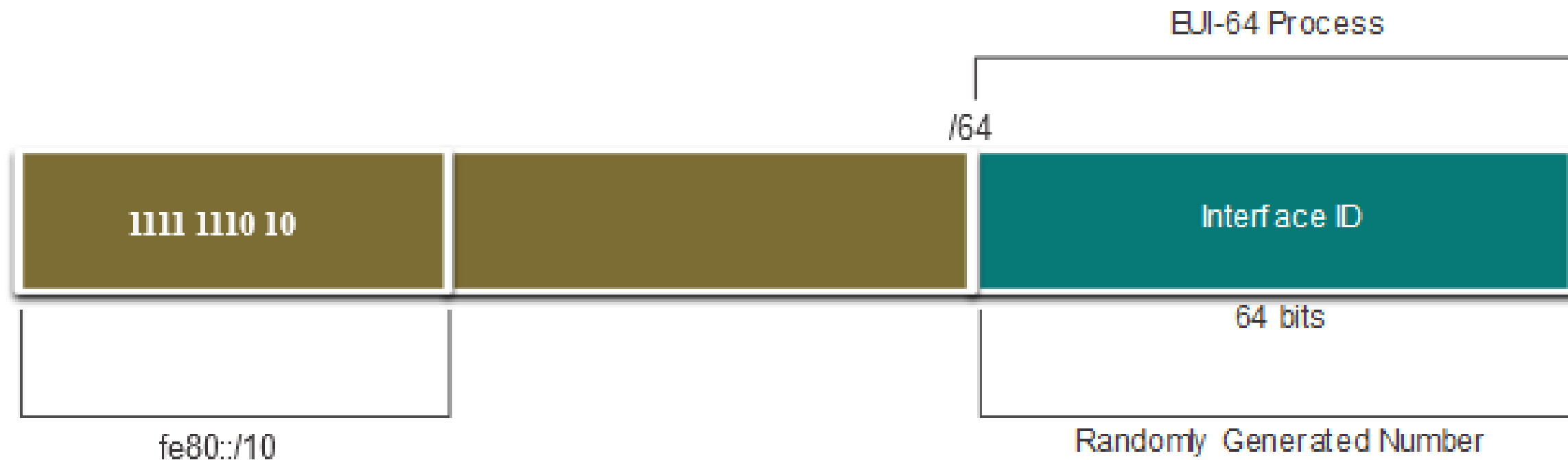
- A 16 bit value of fffe (in hexadecimal) is inserted into the middle of the 48-bit Ethernet MAC address of the client.
- The 7th bit of the client MAC address is reversed from binary 0 to 1.
- Example:

48-bit MAC	fc:99:47:75:ce:e0
EUI-64 Interface ID	fe:99:47:ff:fe:75:ce:e0

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs

- All IPv6 interfaces must have an IPv6 LLA.
- Like IPv6 GUAs, LLAs can be configured dynamically.
- The figure shows the LLA is dynamically created using the fe80::/10 prefix and the interface ID using the EUI-64 process, or a randomly generated 64-bit number.



Dynamic Addressing for IPv6 LLAs

Dynamic LLAs on Windows

Operating systems, such as Windows, will typically use the same method for both a SLAAC-created GUA and a dynamically assigned LLA.

EUI-64 Generated Interface ID:

```
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:\>
```

Random 64-bit Generated Interface ID:

```
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:\>
```

Dynamic Addressing for IPv6 LLAs

Dynamic LLAs on Cisco Routers

Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the interface ID for all LLAs on IPv6 interfaces.

Here is an example of a LLA dynamically configured on the G0/0/0 interface of 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
```

Dynamic Addressing for IPv6 LLAs

Verify IPv6 Address Configuration

Cisco routers automatically create an IPv6 LLA whenever a GUA is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the interface ID for all LLAs on IPv6 interfaces.

Here is an example of a LLA dynamically configured on the G0/0/0 interface of 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
```

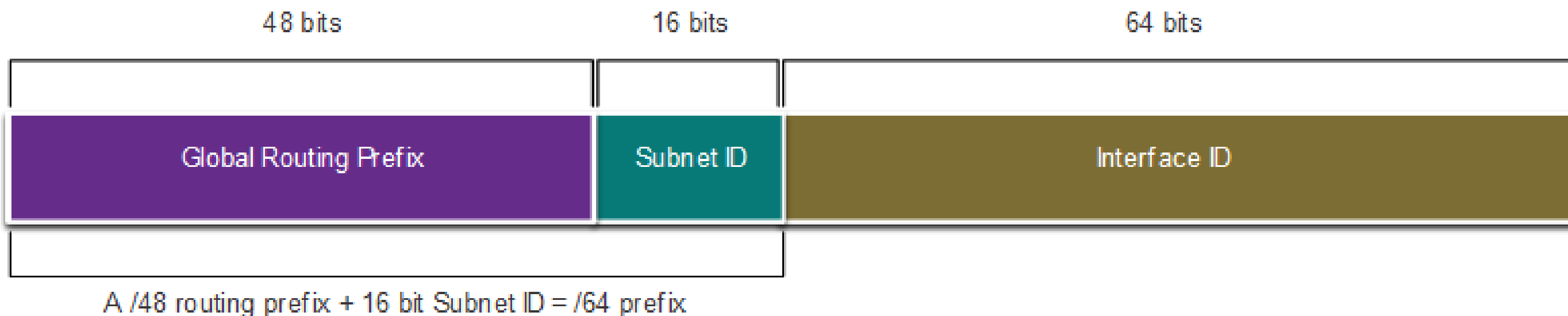
Subnet an IPv6 Network

Subnet an IPv6 Network

Subnet Using the Subnet ID

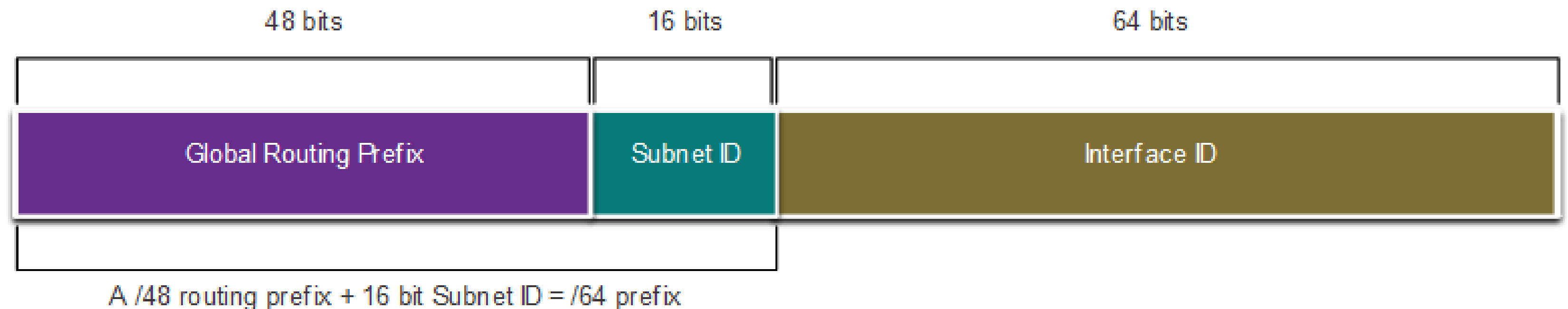
IPv6 was designed with subnetting in mind.

- A separate subnet ID field in the IPv6 GUA is used to create subnets.
- The subnet ID field is the area between the Global Routing Prefix and the interface ID.



The benefit of a 128-bit address is that it can support more than enough subnets and hosts per subnet, for each network. Address conservation is not an issue. For example, if the global routing prefix is a /48, and using a typical 64 bits for the interface ID, this will create a 16-bit subnet ID:

- **16-bit subnet ID** - Creates up to 65,536 subnets.
- **64-bit interface ID** - Supports up to 18 quintillion host IPv6 addresses per subnet




Subnet an IPv6 Network

IPv6 Subnetting Example

Given the 2001:db8:acad::/48
global routing prefix with a 16 bit
subnet ID.

- Allows 65,536 /64 subnets
- The global routing prefix is the same for all subnets.
- Only the subnet ID hextet is incremented in hexadecimal for each subnet.

Increment subnet ID to create 65,536
subnets



2001:db8:acad:0000::/64

2001:db8:acad:0001::/64

2001:db8:acad:0002::/64

2001:db8:acad:0003::/64

2001:db8:acad:0004::/64

2001:db8:acad:0005::/64

2001:db8:acad:0006::/64

2001:db8:acad:0007::/64

2001:db8:acad:0008::/64

2001:db8:acad:0009::/64

2001:db8:acad:000a::/64

2001:db8:acad:000b::/64

2001:db8:acad:000c::/64

Subnets 13 – 65,534 not shown

2001:db8:acad:ffff::/64

Subnet an IPv6 Network

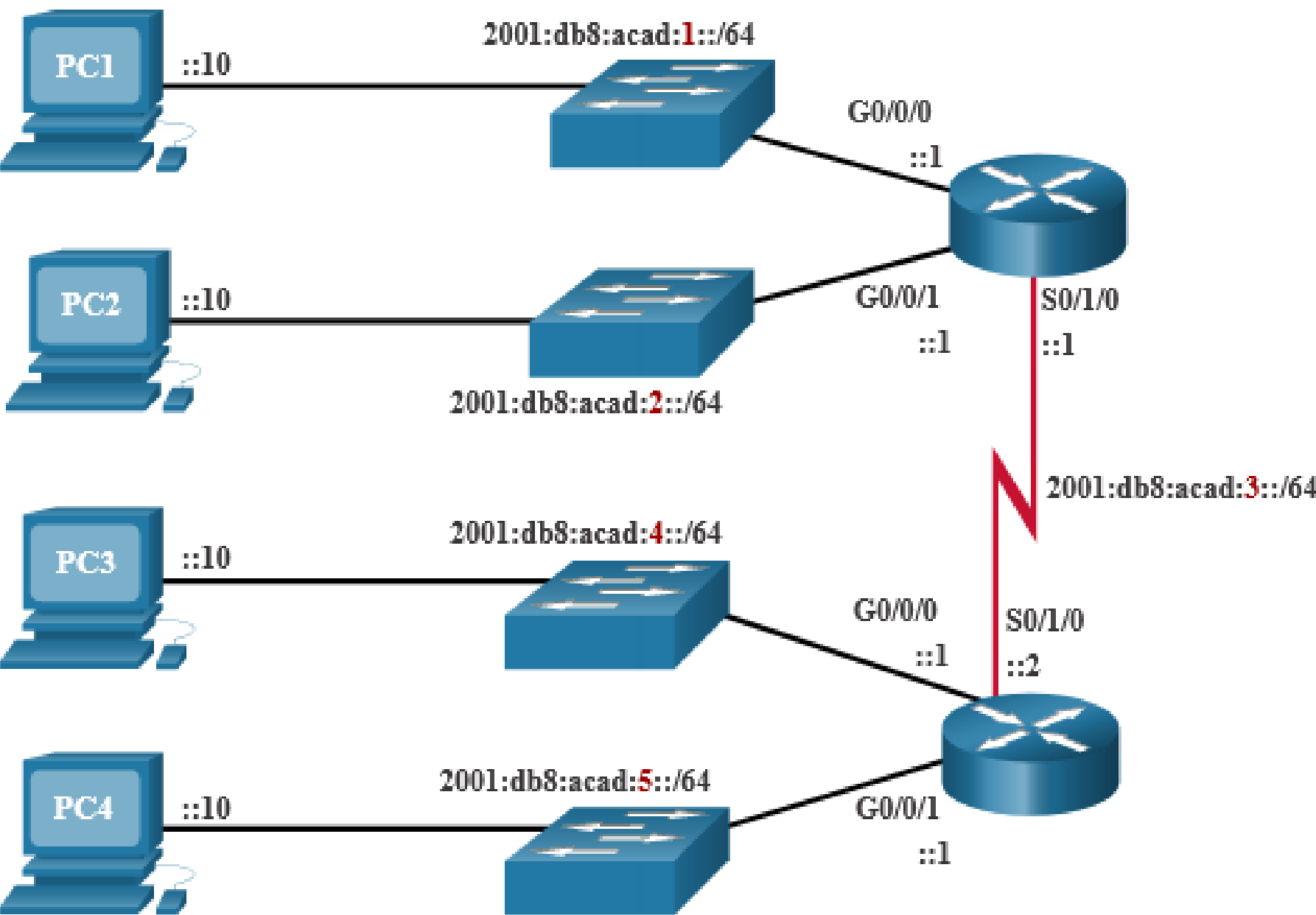
IPv6 Subnet Allocation

Address Block 2001:0db8:acad::/48

5 subnets allocated from 65,536 available subnets

2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64

2001:db8:acad:ffff::/64



Router Configured with IPv6 Subnets

The example shows that each of the router interfaces on R1 has been configured to be on a different IPv6 subnet.

```
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
```

ICMP Messages

ICMP Messages

ICMPv4 and ICMPv6 Messages

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 and ICMPv6 include:
 - Host reachability
 - Destination or Service Unreachable
 - Time exceeded

Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

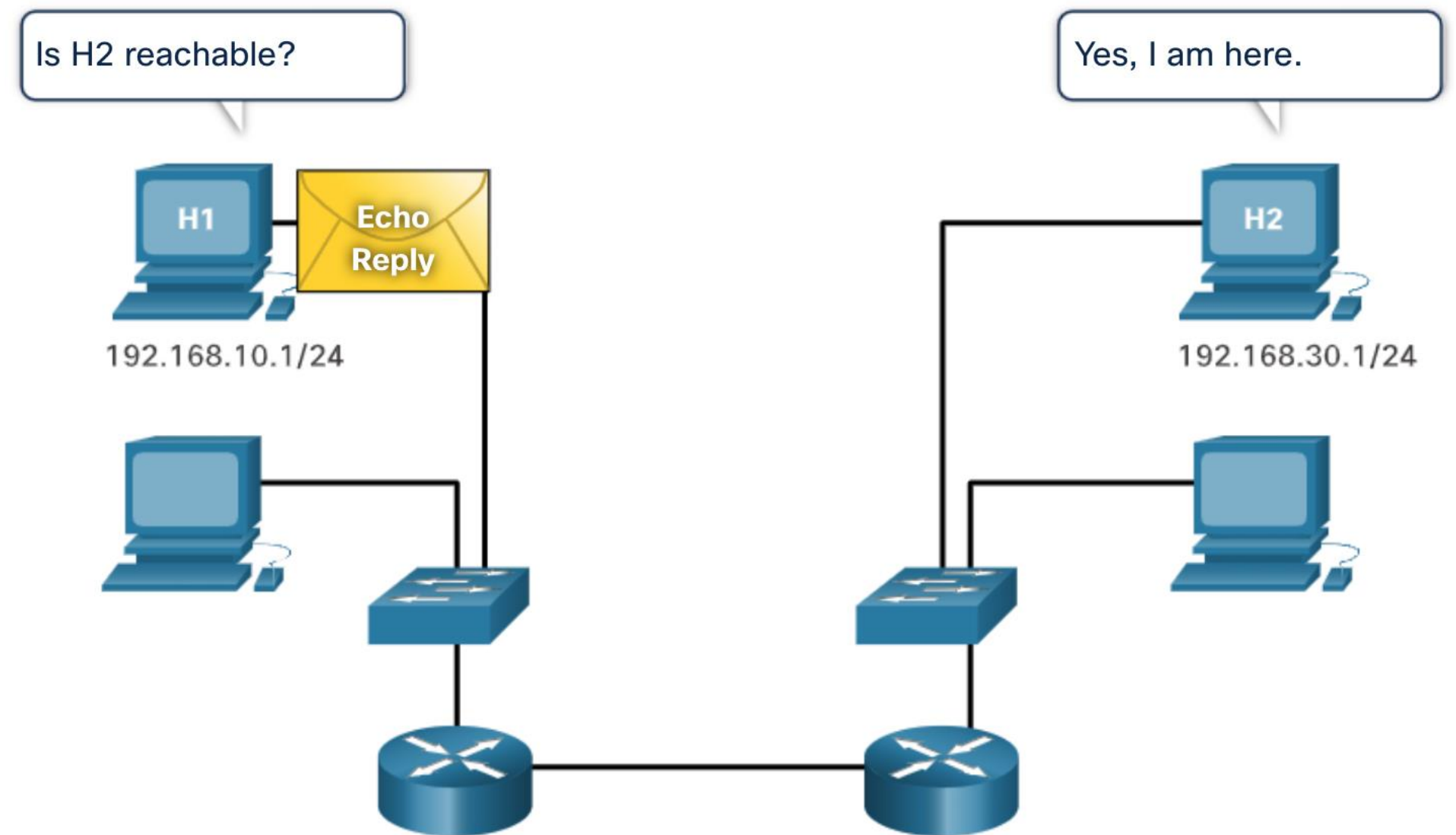
ICMP Messages

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.



ICMP Messages

Destination or Service Unreachable

- An ICMP Destination Unreachable message can be used to notify the source that a destination or service is unreachable.
- The ICMP message will include a code indicating why the packet could not be delivered.

A few Destination Unreachable codes for ICMPv4 are as follows:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

A few Destination Unreachable codes for ICMPv6 are as follows:

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

Note: ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

ICMP Messages

Time Exceeded

- When the Time to Live (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host.
- ICMPv6 also sends a Time Exceeded message. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired.

```
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Note: Time Exceeded messages are used by the **tracert** tool.

ICMP Messages

ICMPv6 Messages

ICMPv6 has new features and improved functionality not found in ICMPv4, including four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device, including dynamic address allocation are as follows:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

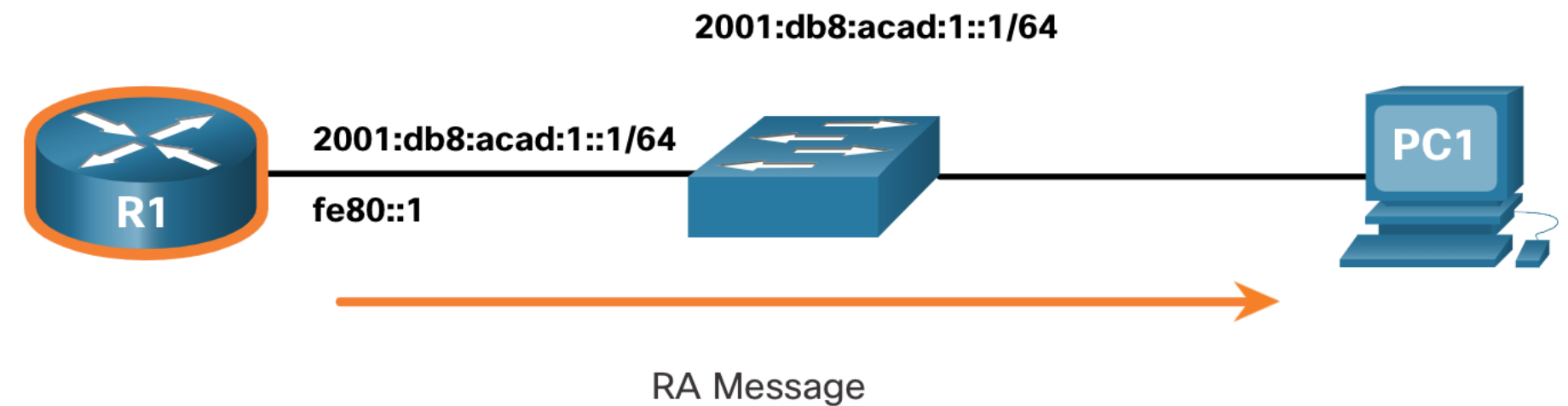
Messaging between IPv6 devices, including duplicate address detection and address resolution are as follows:

- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

ICMP Messages

ICMPv6 Messages (Cont.)

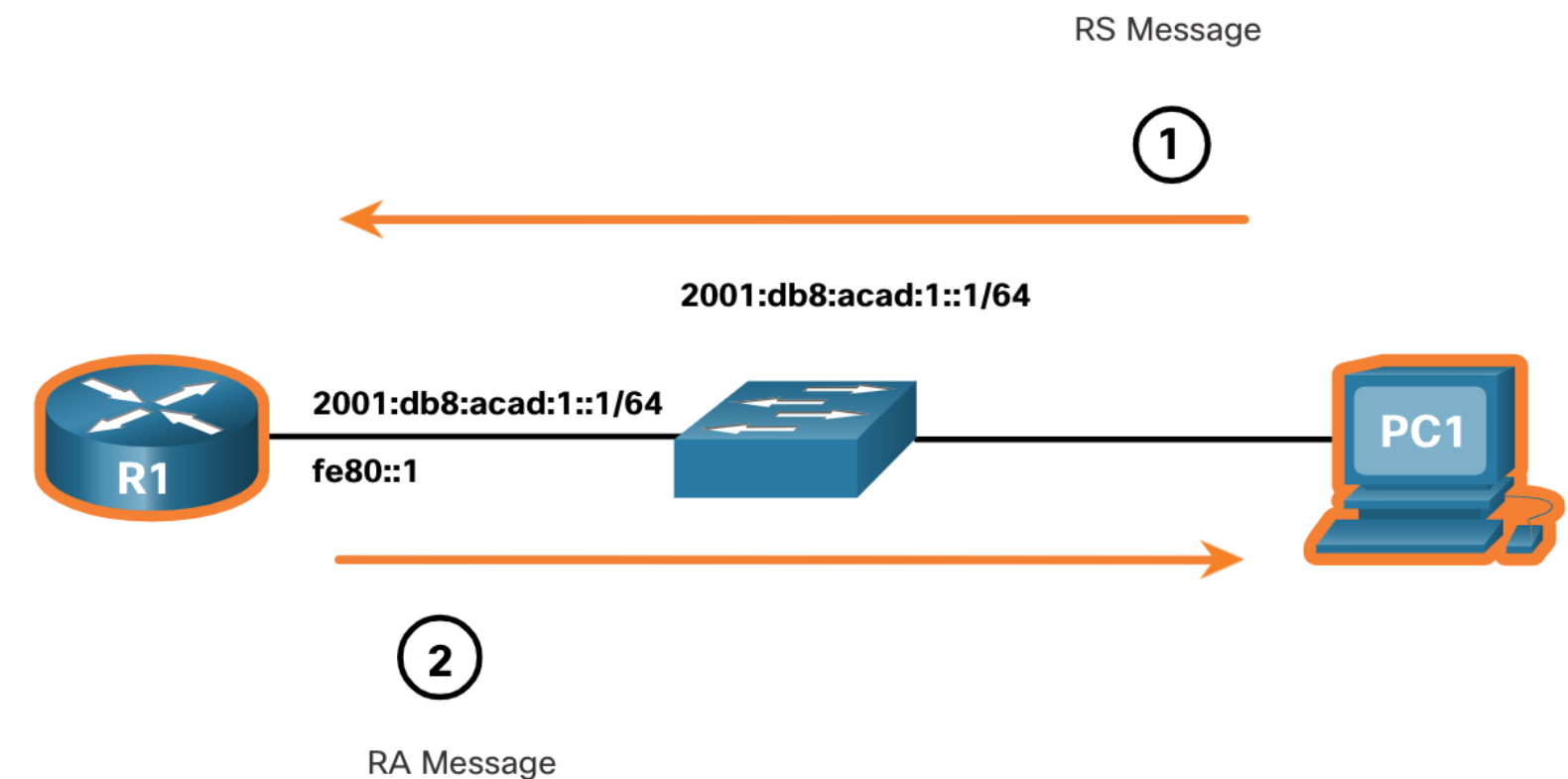
- RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts.
- RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name.
- A host using Stateless Address Autoconfiguration (SLAAC) will set its default gateway to the link-local address of the router that sent the RA.



ICMP Messages

ICMPv6 Messages (Cont.)

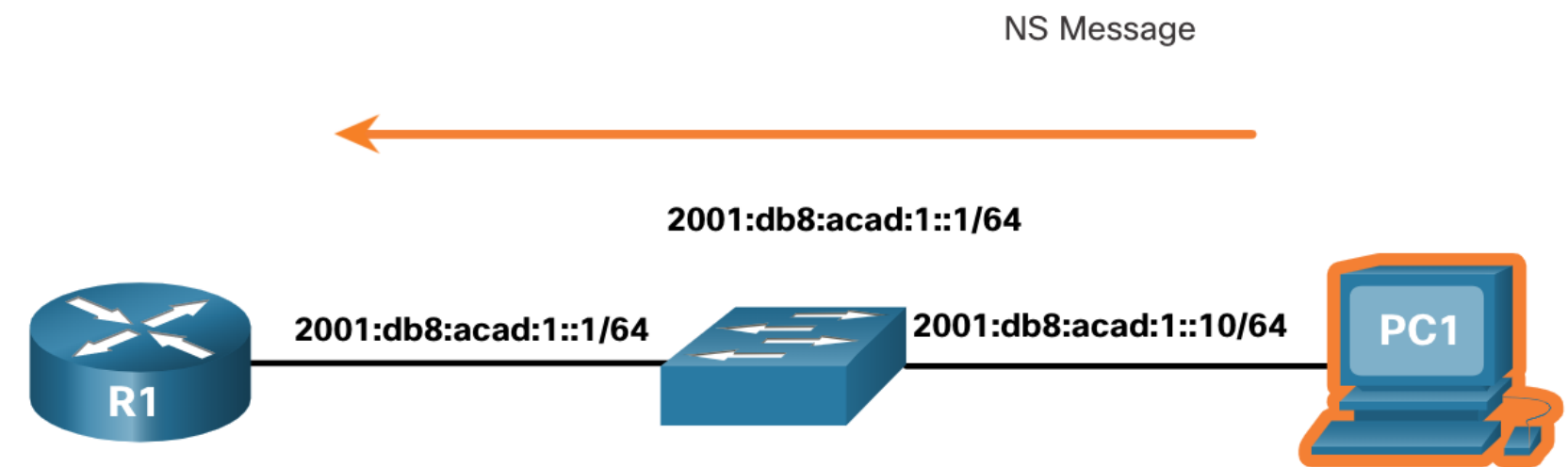
- An IPv6-enabled router will also send out an RA message in response to an RS message.
- In the figure, PC1 sends a RS message to determine how to receive its IPv6 address information dynamically.
 - R1 replies to the RS with an RA message.
 - PC1 sends an RS message, “Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically.”
 - R1 replies with an RA message. “Hi all IPv6-enabled devices. I’m R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway.”



ICMP Messages

ICMPv6 Messages (Cont.)

- A device assigned a global IPv6 unicast or link-local unicast address, may perform duplicate address detection (DAD) to ensure that the IPv6 address is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address.
- If another device on the network has this address, it will respond with an NA message notifying to the sending device that the address is in use.

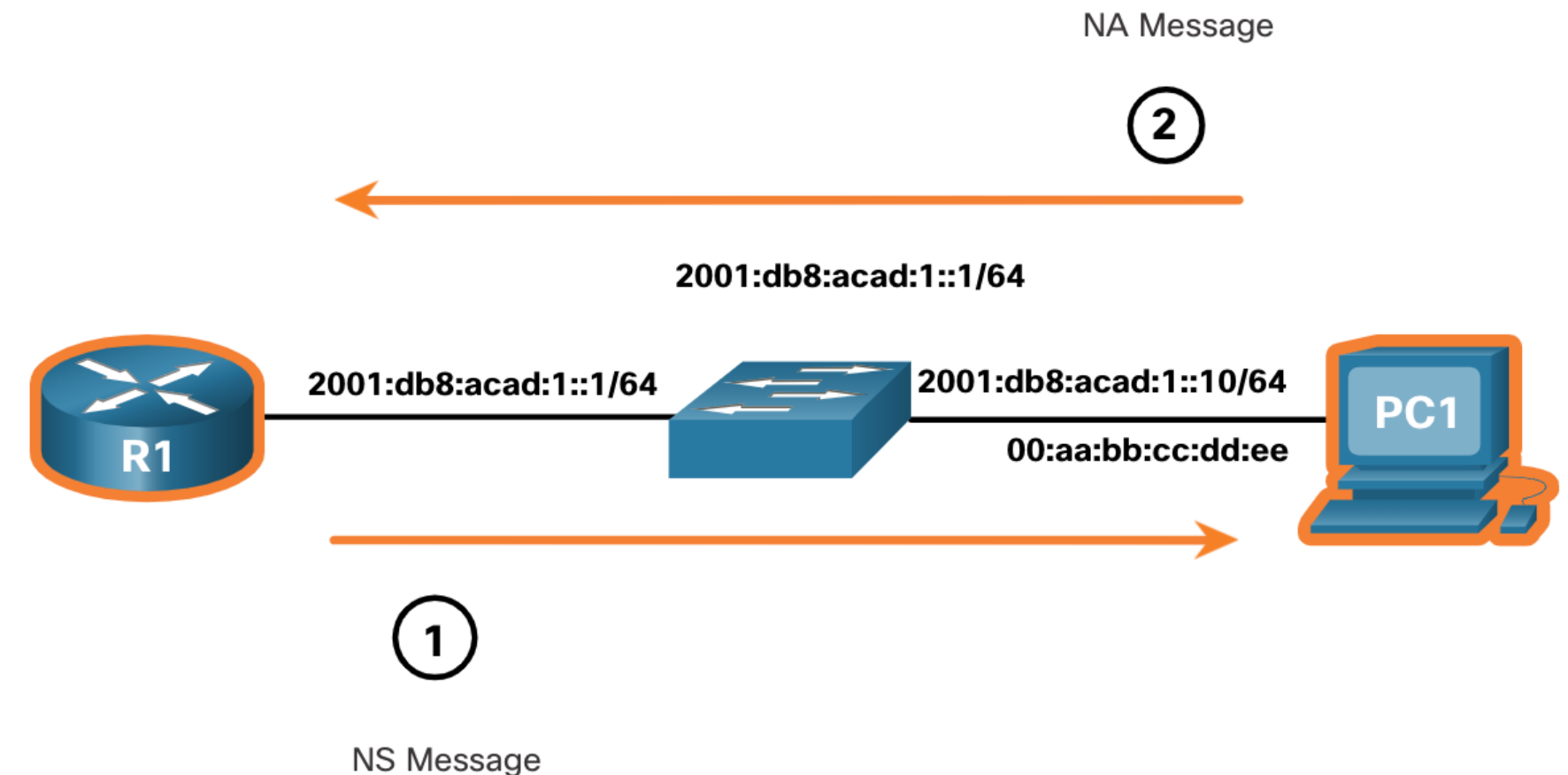


Note: DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.

ICMP Messages

ICMPv6 Messages (Cont.)

- To determine the MAC address for the destination, the device will send an NS message to the solicited node address.
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
- In the figure, R1 sends a NS message to 2001:db8:acad:1::10 asking for its MAC address.



Ping and Traceroute Tests

Ping and Traceroute Tests

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.
- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.
- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
```

```
!!!!!
```

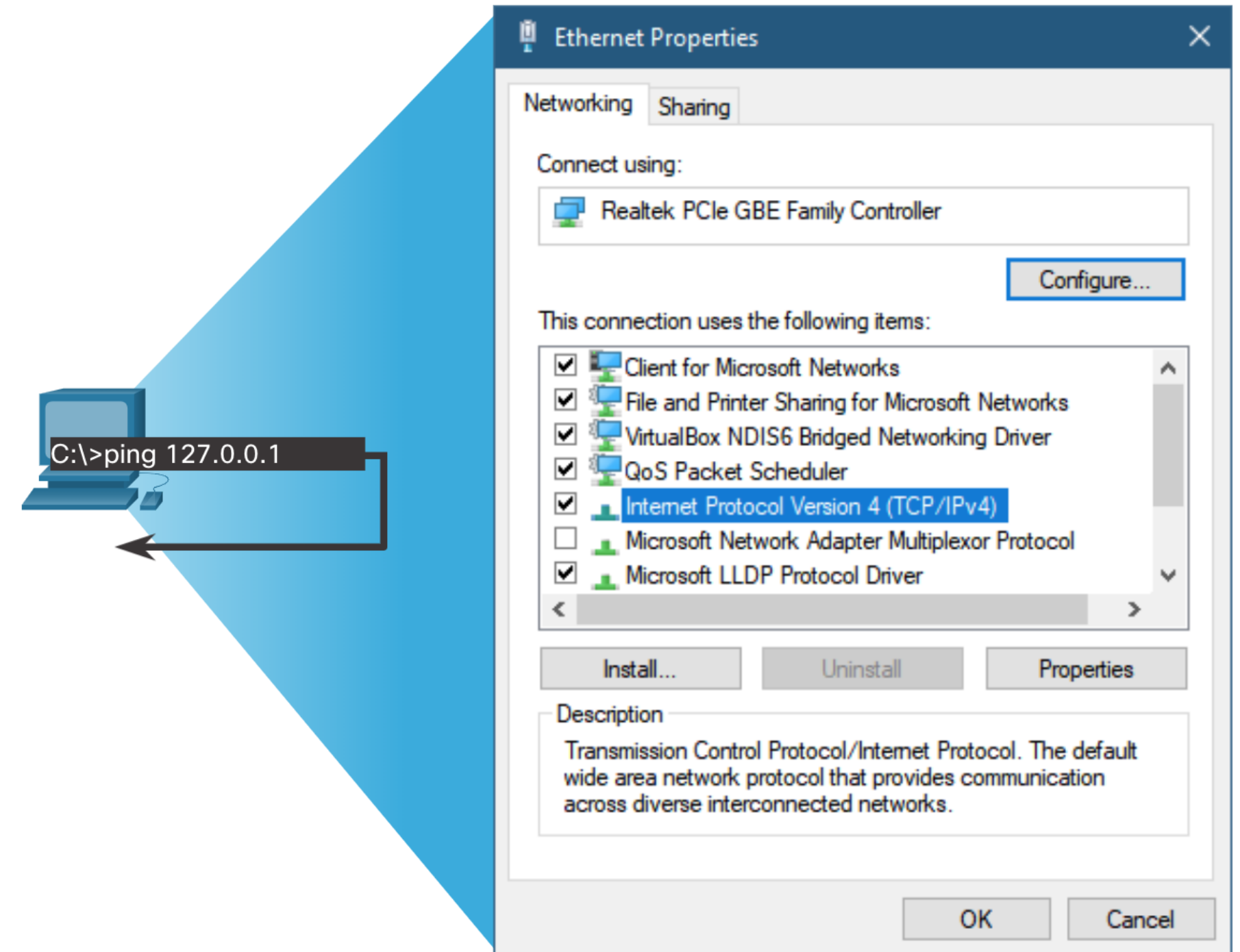
```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping and Traceroute Tests

Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **ping** the local loopback address of 127.0.0.1 for IPv4 (:::1 for IPv6).

- A response from 127.0.0.1 for IPv4, or :::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.



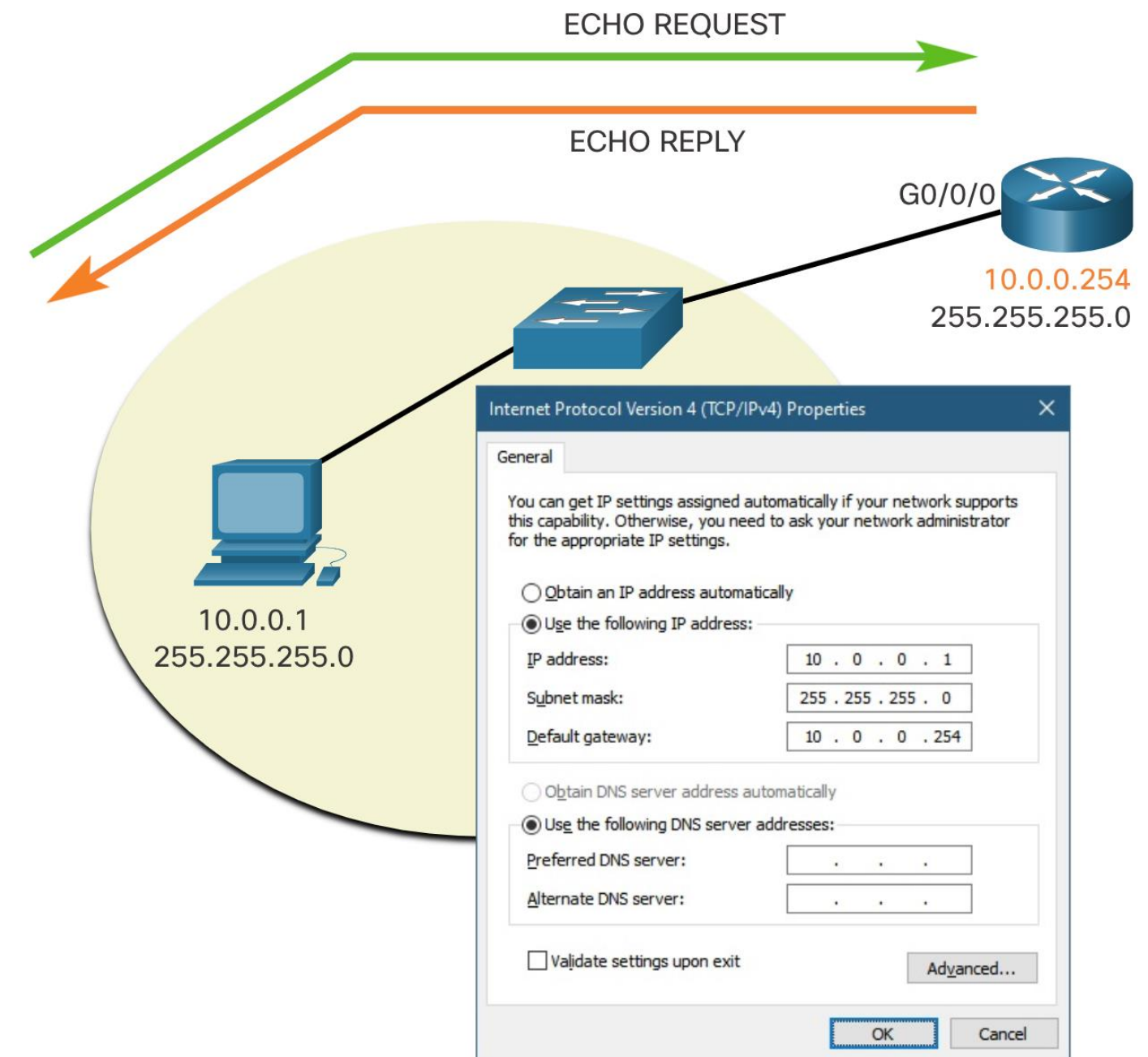
Ping and Traceroute Tests

Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is known to be operational.



Ping and Traceroute Tests

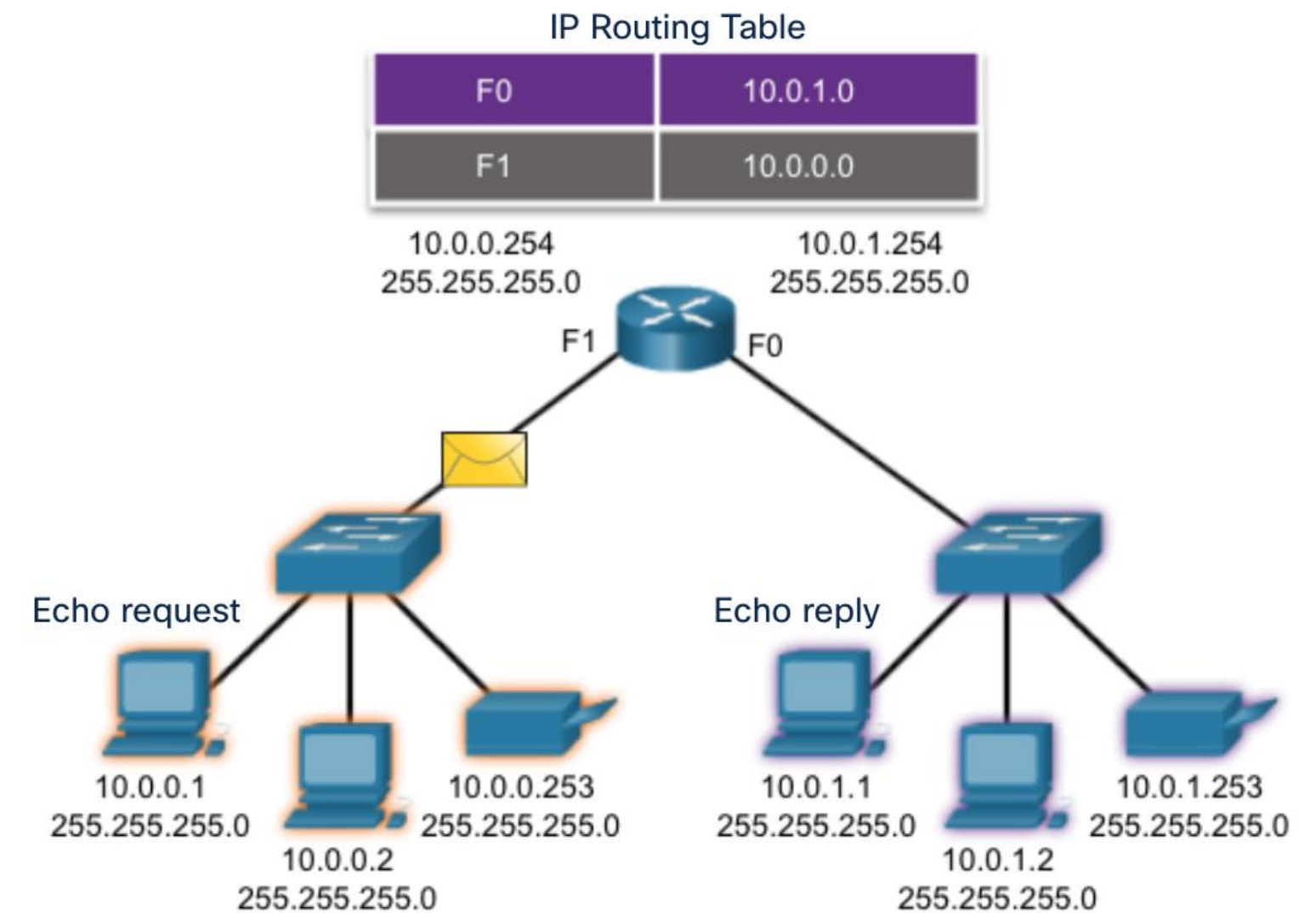
Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

A local host can ping a host on a remote network.

A successful **ping** across the internetwork confirms communication on the local network.

Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.



Traceroute – Test the Path

- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.
- Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. An asterisk (*) is used to indicate a lost or unreplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.

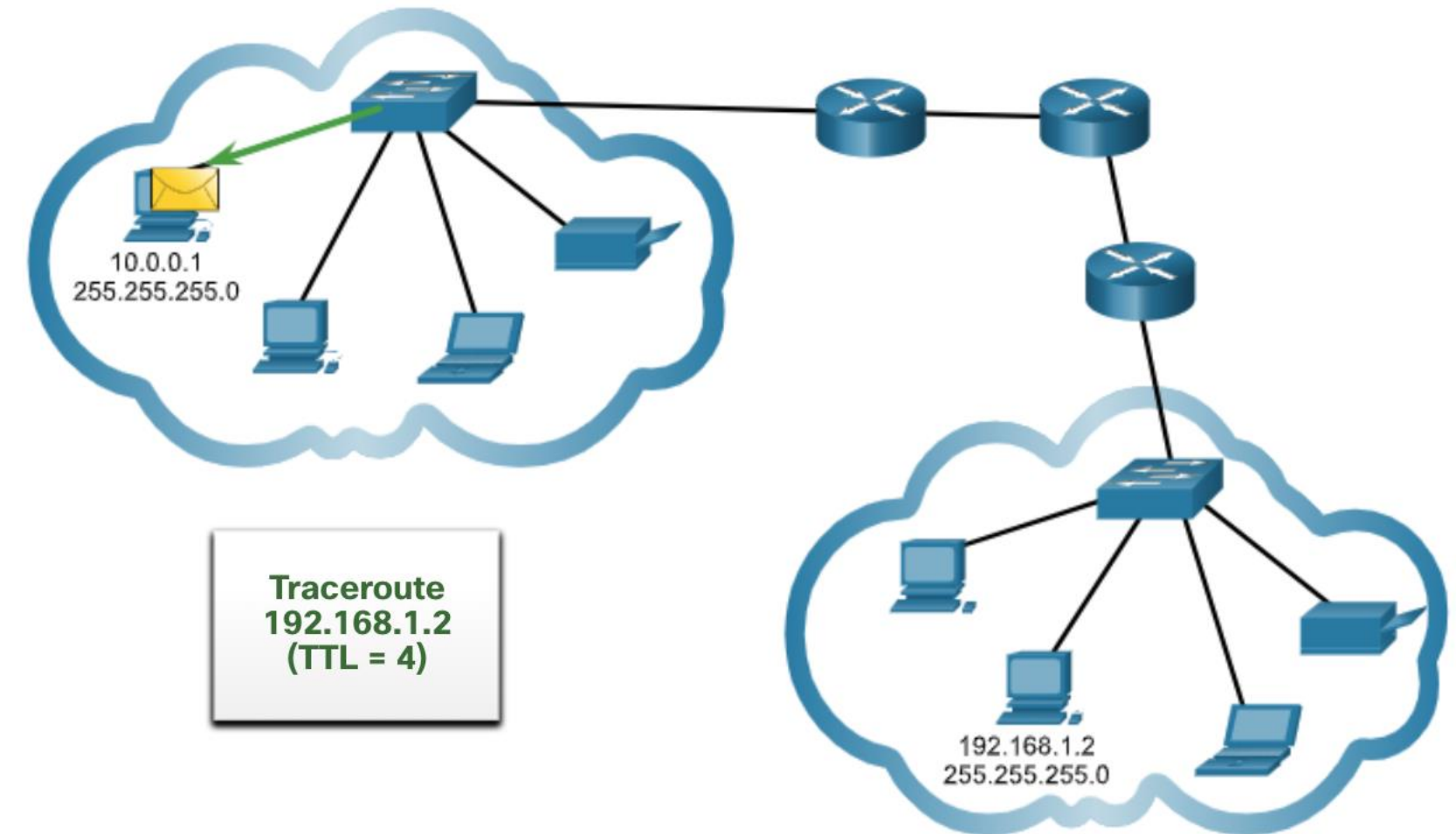
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

 1  192.168.10.2      1 msec    0 msec    0 msec
 2  192.168.20.2      2 msec    1 msec    0 msec
 3  192.168.30.2      1 msec    0 msec    0 msec
 4  192.168.40.2      0 msec    0 msec    0 msec
```

Note: Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

Traceroute – Test the Path (Cont.)

- The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.
- Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path.
- The TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum.



THANK YOU!