



Module 11: IPv4 Addressing

Introduction to Networks v7.0
(ITN)



Module Objectives

Module Title: IPv4 Addressing

Module Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

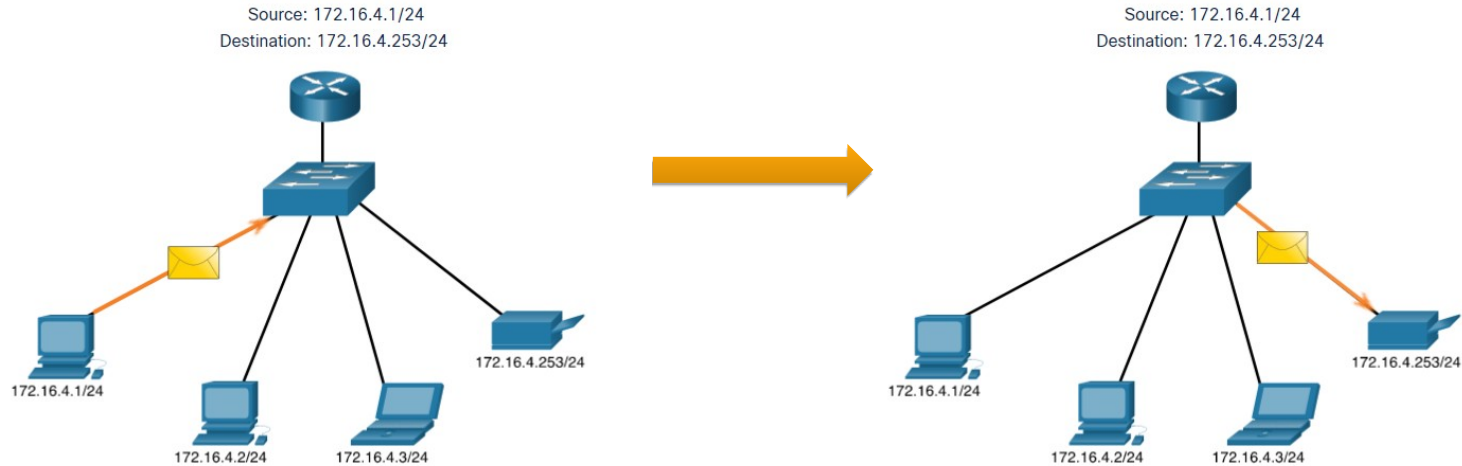
Topic Title	Topic Objective
IPv4 Address Structure ✓	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types of IPv4 Addresses ✓	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explain how subnetting segments a network to enable better communication.
Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.

11.2 IPv4 Unicast, Broadcast, and Multicast

IPv4 Unicast, Broadcast, and Multicast

Unicast

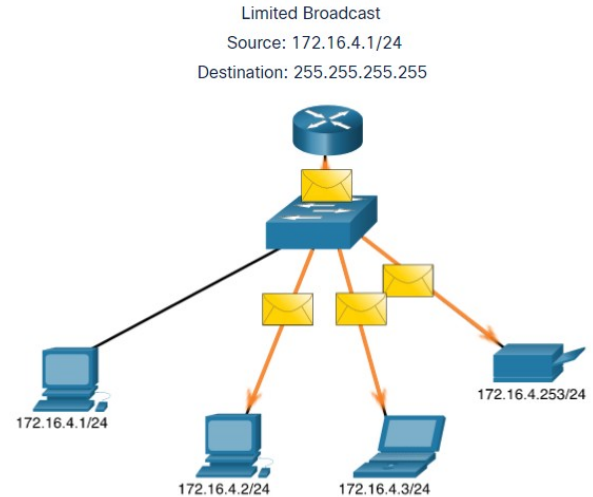
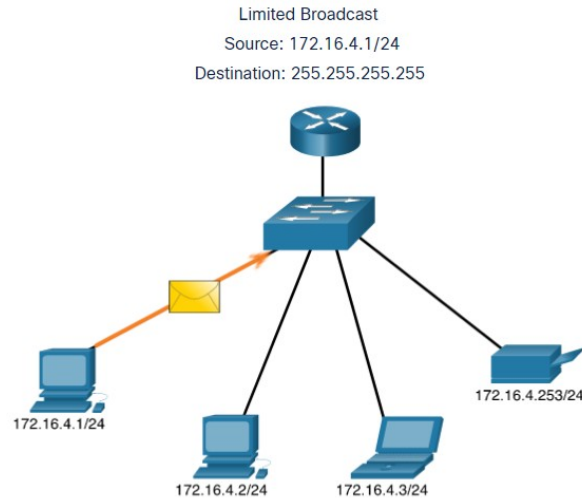
- Unicast transmission is sending a packet to one destination IP address.
- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.



IPv4 Unicast, Broadcast, and Multicast

Broadcast

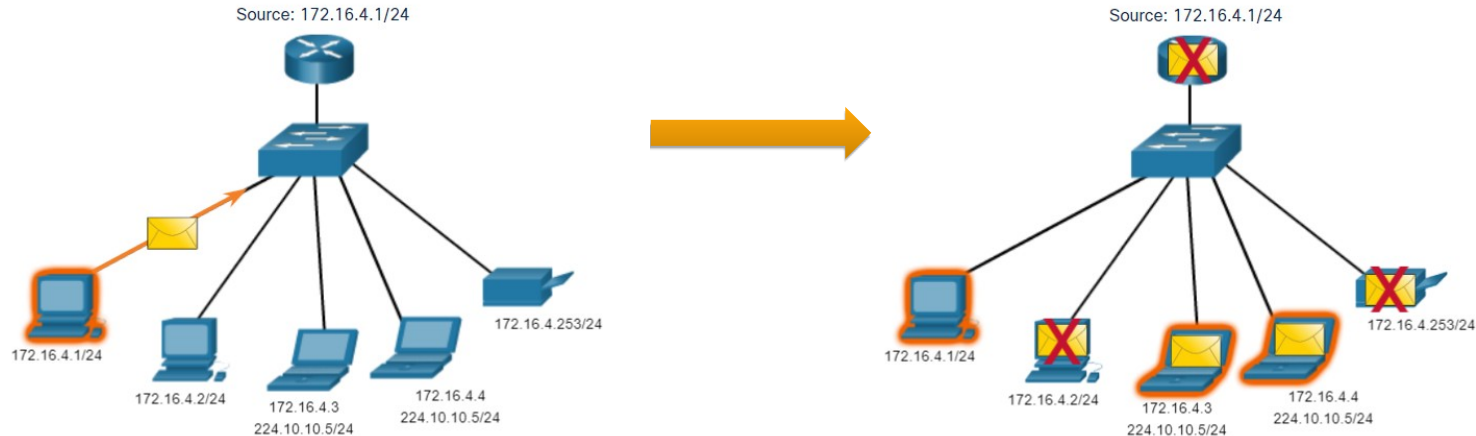
- Broadcast transmission is sending a packet to all other destination IP addresses.
- For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts.



IPv4 Unicast, Broadcast, and Multicast

Multicast

- Multicast transmission is sending a packet to a multicast address group.
- For example, the PC at 172.16.4.1 sends a multicast packet to the multicast group address 224.10.10.5.

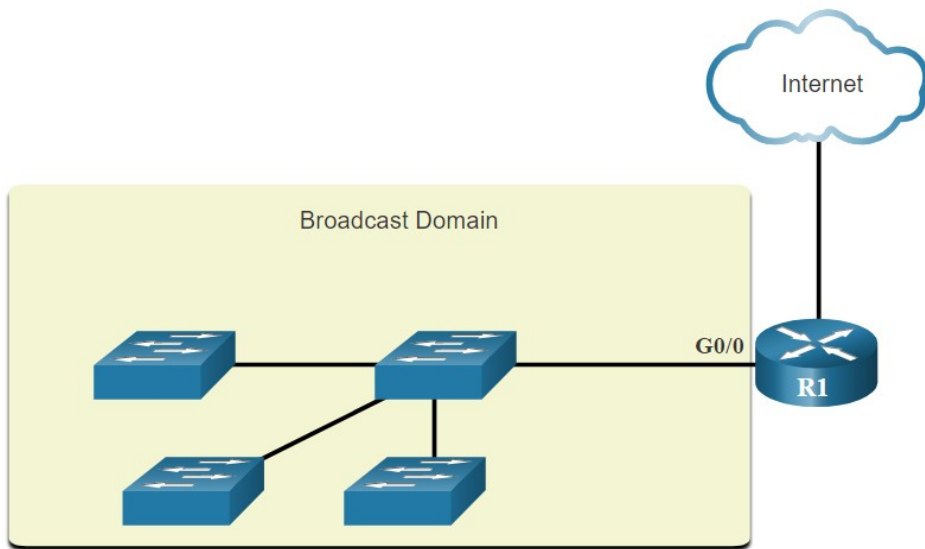


11.4 Network Segmentation

Network Segmentation

Broadcast Domains and Segmentation

- Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server.)
- Switches propagate broadcasts out all interfaces except the interface on which it was received.

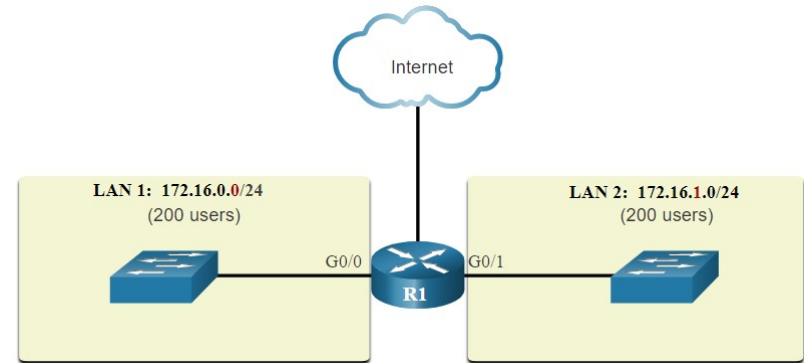
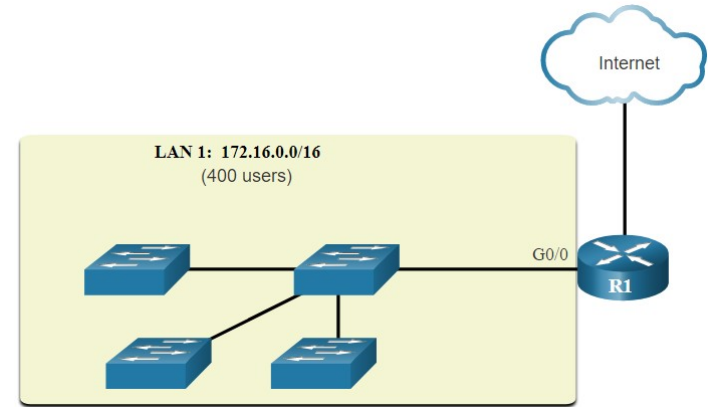


- The only device that stops broadcasts is a router.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

Network Segmentation

Problems with Large Broadcast Domains

- A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting.
- Dividing the network address 172.16.0.0 /16 into two subnets of 200 users each: 172.16.0.0 /24 and 172.16.1.0 /24.
- Broadcasts are only propagated within the smaller broadcast domains.

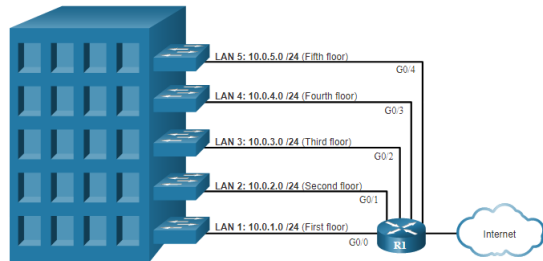


Network Segmentation

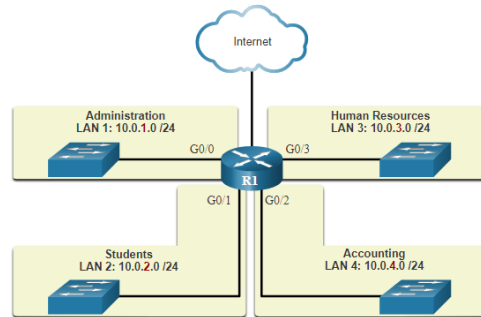
Reasons for Segmenting Networks

- Subnetting reduces overall network traffic and improves network performance.
- It can be used to implement security policies between subnets.
- Subnetting reduces the number of devices affected by abnormal broadcast traffic.
- Subnets are used for a variety of reasons including by:

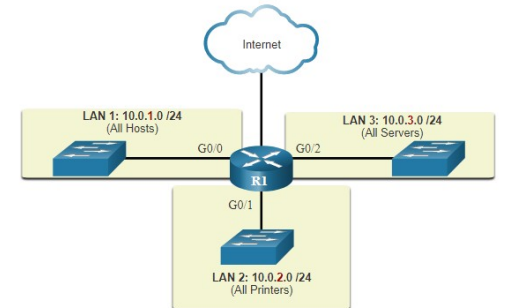
Location



Group or Function



Device Type



11.5 Subnet an IPv4 Network

Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn . hhhhhhhh . hhhhhhhh . hhhhhhhh 11111111 . 00000000 . 00000000 . 00000000	16,777,214
/16	255.255.0.0	nnnnnnnn . nnnnnnnn . hhhhhhhh . hhhhhhhh 11111111 . 11111111 . 00000000 . 00000000	65,534
/24	255.255.255.0	nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh 11111111 . 11111111 . 11111111 . 00000000	254

Subnet on an Octet Boundary (Cont.)

- In the first table 10.0.0.0/8 is subnetted using /16 and in the second table, a /24 mask.

Subnet Address (256 Possible Subnets)	Host Range (65,534 possible hosts per subnet)	Broadcast
10.0.0.0/16	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0/16	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0/16	10.2.0.1 - 10.2.255.254	10.2.255.255
10.3.0.0/16	10.3.0.1 - 10.3.255.254	10.3.255.255
10.4.0.0/16	10.4.0.1 - 10.4.255.254	10.4.255.255
10.5.0.0/16	10.5.0.1 - 10.5.255.254	10.5.255.255
10.6.0.0/16	10.6.0.1 - 10.6.255.254	10.6.255.255
10.7.0.0/16	10.7.0.1 - 10.7.255.254	10.7.255.255
...
10.255.0.0/16	10.255.0.1 - 10.255.255.254	10.255.255.255

Subnet Address (65,536 Possible Subnets)	Host Range (254 possible hosts per subnet)	Broadcast
10.0.0.0/24	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0/24	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0/24	10.0.2.1 - 10.0.2.254	10.0.2.255
...
10.0.255.0/24	10.0.255.1 - 10.0.255.254	10.0.255.255
10.1.0.0/24	10.1.0.1 - 10.1.0.254	10.1.0.255
10.1.1.0/24	10.1.1.1 - 10.1.1.254	10.1.1.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.255
...
10.100.0.0/24	10.100.0.1 - 10.100.0.254	10.100.0.255
...
10.255.255.0/24	10.255.255.1 - 10.255.255.254	10.255.255.255

Subnet within an Octet Boundary

- Refer to the table to see six ways to subnet a /24 network.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nhhhhhhhh 11111111 . 11111111 . 11111111 . 10000000	2	126
/26	255.255.255.192	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnhhhhhhh 11111111 . 11111111 . 11111111 . 11000000	4	62
/27	255.255.255.224	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnhhhhhh 11111111 . 11111111 . 11111111 . 11100000	8	30
/28	255.255.255.240	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnnhhhh 11111111 . 11111111 . 11111111 . 11110000	16	14
/29	255.255.255.248	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnnnhhh 11111111 . 11111111 . 11111111 . 11111000	32	6
/30	255.255.255.252	nnnnnnnnn . nnnnnnnnn . nnnnnnnnn . nnnnnnnhh 11111111 . 11111111 . 11111111 . 11111100	64	2


11.7 Subnet to Meet Requirements

Subnet to Meet Requirements

Minimize Unused Host IPv4 Addresses and Maximize Subnets

There are two considerations when planning subnets:

- The number of host addresses required for each network
- The number of individual subnets needed



Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nhhhhhhhhh 11111111 . 11111111 . 11111111 . 10000000	2	126
/26	255.255.255.192	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnhhhhhhh 11111111 . 11111111 . 11111111 . 11000000	4	62
/27	255.255.255.224	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnhhhhh 11111111 . 11111111 . 11111111 . 11100000	8	30
/28	255.255.255.240	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnnhhhh 11111111 . 11111111 . 11111111 . 11110000	16	14
/29	255.255.255.248	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnnnhhh 11111111 . 11111111 . 11111111 . 11111000	32	6
/30	255.255.255.252	nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnnn . nnnnnnnnhh 11111111 . 11111111 . 11111111 . 11111100	64	2

Subnetting Formulas


To calculate the number of subnets.

$$2^b$$

b ~ bits borrowed

192 . 168 . 1 . 0

nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh



Borrowing 1 bit:	$2^1 = 2$
Borrowing 2 bits:	$2^2 = 4$
Borrowing 3 bits:	$2^3 = 8$
Borrowing 4 bits:	$2^4 = 16$
Borrowing 5 bits:	$2^5 = 32$
Borrowing 6 bits:	$2^6 = 64$

Subnetting Formulas (cont.)

To calculate the number of hosts.

192. 168. 1. 0 000 0000

7 bits remain in host field

$2^7 = 128$ hosts per subnet
 $2^7 - 2 = 126$ valid hosts per subnet

$$2^{h'} - 2$$

h' ~ number of bits
remaining in the host field

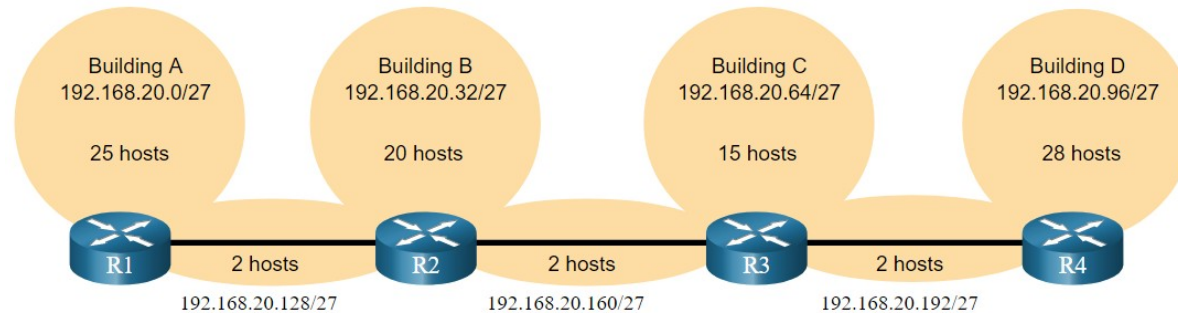
11.8 VLSM

VLSM

IPv4 Address Conservation

Given the topology, 7 subnets are required (i.e, four LANs and three WAN links) and the largest number of host is in Building D with 28 hosts.

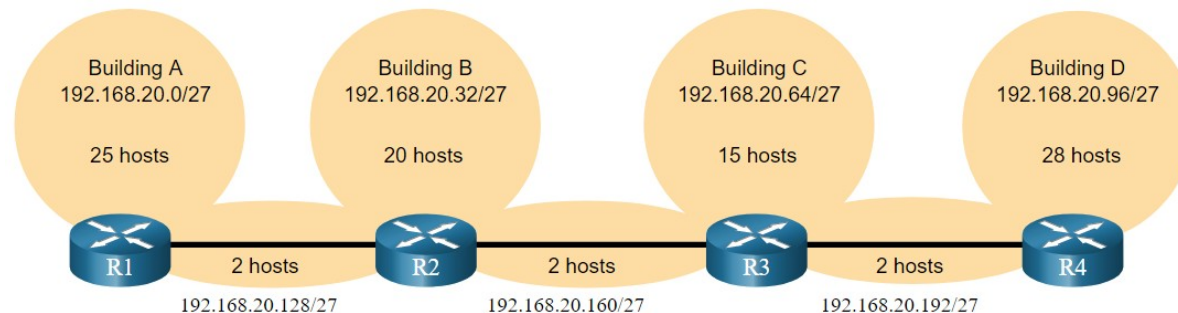
- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.



IPv4 Address Conservation (Cont.)

However, the point-to-point WAN links only require two addresses and therefore waste 28 addresses each for a total of 84 unused addresses.

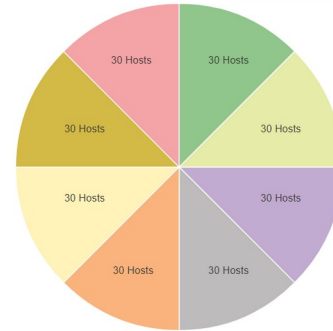
Host portion
 $2^5 - 2 = 30$ host IP addresses per subnet
 $30 - 2 = 28$
 Each WAN subnet wastes 28 addresses
 $28 \times 3 = 84$
 84 addresses are unused



- Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.
- VLSM was developed to avoid wasting addresses by enabling us to subnet a subnet.

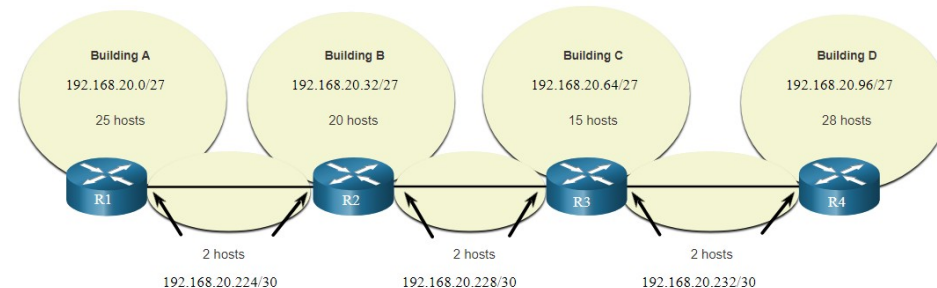
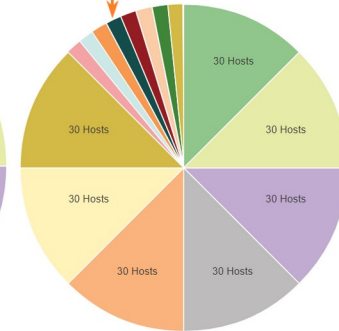
- The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how VLSM can be used to subnet a subnet and divided the last subnet into eight /30 subnets.
- When using VLSM, always begin by satisfying the host requirements of the largest subnet and continue subnetting until the host requirements of the smallest subnet are satisfied.
- The resulting topology with VLSM applied.

Traditional Subnetting Creates Equal Sized Subnets



Subnets of Varying Sizes

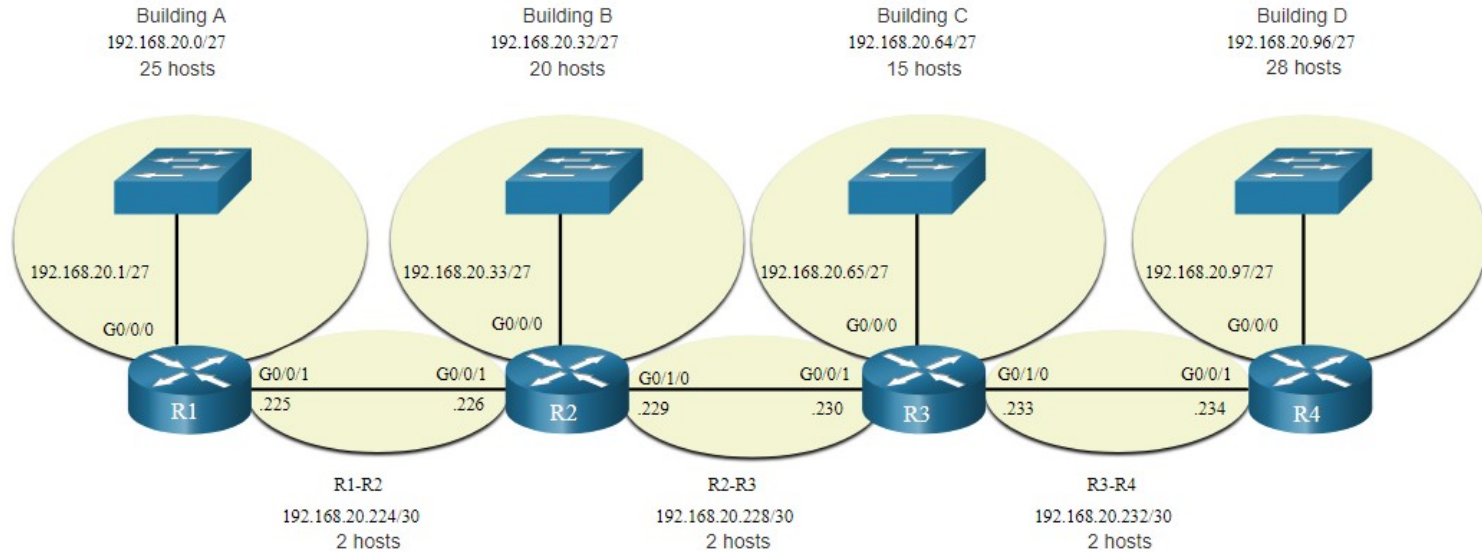
One subnet was further divided to create 8 smaller subnets of 2 hosts each.



VLSM

VLSM Topology Address Assignment

- Using VLSM subnets, the LAN and inter-router networks can be addressed without unnecessary waste as shown in the logical topology diagram.



IP Addressing and Subnetting IP networks examples

Libor Polčák

Vysoké učení technické v Brně, Fakulta informačních technologií

Božetěchova 1/2, 612 66 Brno

ipolcak@fit.vutbr.cz



Cvičebnice v souborech předmětu

- Příklady (examples)

- Ip_Addressing_and_Subnetting_Workbook_-_Student_Version_v2_0.pdf
- VLSM_Workbook__Student_Edition_-_v2_0.pdf

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

$$147 = 128 + 16 + 2 + 1$$

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

$$147 = 128 + 16 + 2 + 1$$

$$229 = 128 + 64 + 32 + 4 + 1$$

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

$$147 = 128 + 16 + 2 + 1$$

$$229 = 128 + 64 + 32 + 4 + 1$$

$$176 = 128 + 32 + 16$$

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

$$147 = 128 + 16 + 2 + 1$$

$$229 = 128 + 64 + 32 + 4 + 1$$

$$176 = 128 + 32 + 16$$

$$19 = 16 + 2 + 1$$

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1 10010011

229 = 128 + 64 + 32 + 4 + 1 11100101

176 = 128 + 32 + 16 10110000

19 = 16 + 2 + 1 00010011

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1 10010011

229 = 128 + 64 + 32 + 4 + 1 11100101

176 = 128 + 32 + 16 10110000

19 = 16 + 2 + 1 00010011

10010011.11100101.10110000.00010011

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
```

```
...
```

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
```

```
link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
```

```
inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
```

```
valid_lft forever preferred_lft forever
```

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
```

```
...
```

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
```

```
link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
```

```
inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
```

```
valid_lft forever preferred_lft forever
```

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

\$ ip addr show

...

4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000

link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff

inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2

valid_lft forever preferred_lft forever

- Délka prefixu: /23

→ 23 jedniček, zbytek 0

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

\$ ip addr show

...

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000  
link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff  
inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2  
valid_lft forever preferred_lft forever
```

- Délka prefixu: /23
→ 23 jedniček, zbytek 0
- 11111111.11111111.11111110.00000000

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

\$ ip addr show

...

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000  
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff  
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2  
        valid_lft forever preferred_lft forever
```

- Délka prefixu: /23
→ 23 jedniček, zbytek 0
- 11111111.11111111.11111110.00000000
- 255.255.254.0

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----
```

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----
10010011.11100101.10110000.00000000
```


Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----
10010011.11100101.10110000.00000000
```

Adresa sítě: 147.229.176.0

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----
10010011.11100101.10110000.00000000
```

Adresa sítě: 147.229.176.0

Všesměrová adresa: 147.229.177.255

Počet podsítí

- Víte, že VUT má k dispozici IP adresy 147.229.0.0/16 a server merlin používá rozsah /23, kolik podsítí v rozsahu /23 může na VUT maximálně existovat?

Počet podsítí

- Víte, že VUT má k dispozici IP adresy 147.229.0.0/16 a server merlin používá rozsah /23, kolik podsítí v rozsahu /23 může na VUT maximálně existovat?

$$2^{23-16}=2^7=128$$

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

$$32-23=9$$

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

$$32-23=9$$

$$2^9-2=510 \text{ zařízení}$$

Podsítování

- Máte k dispozici rozsah IP adres 10.15.80.0/22. Máte za úkol vytvořit podsítě pro A) nejméně 40 zařízení, B) nejméně 60 zařízení, C) nejméně 16 zařízení, D) nejméně 14 zařízení, E) nejméně 8 point-to-point propojů. Navrhněte podsítování, kolik volných adres vám zbyde v rezervě?

Podsítování

Podsítování

■ 10.15.80.0/22

Podsítování

- 10.15.80.0/22
- A) 40 zařízení

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - ◆ $2^6 \rightarrow /26$
- B) 60 zařízení

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

.80.0

.83.255

Podsítování

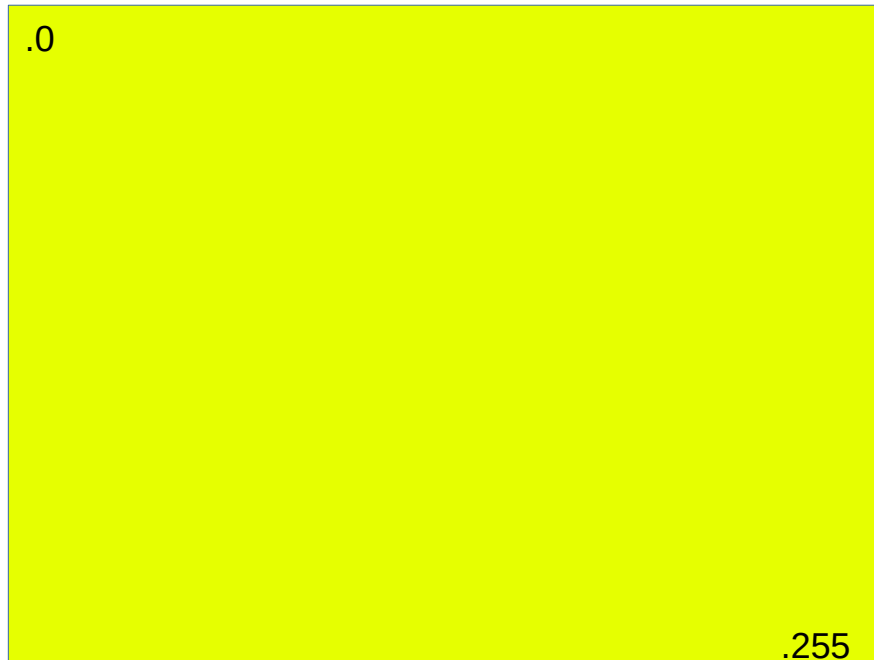
- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

.80.0	.82.0
.81.0	.83.0

Podsítování

10.15.83.0/24

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

10.15.83.0/24

.0	.128
.127	.255

Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

10.15.83.0/24

.0	.128
.63	.191
.64	.192
.127	.255

Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

10.15.83.0/24

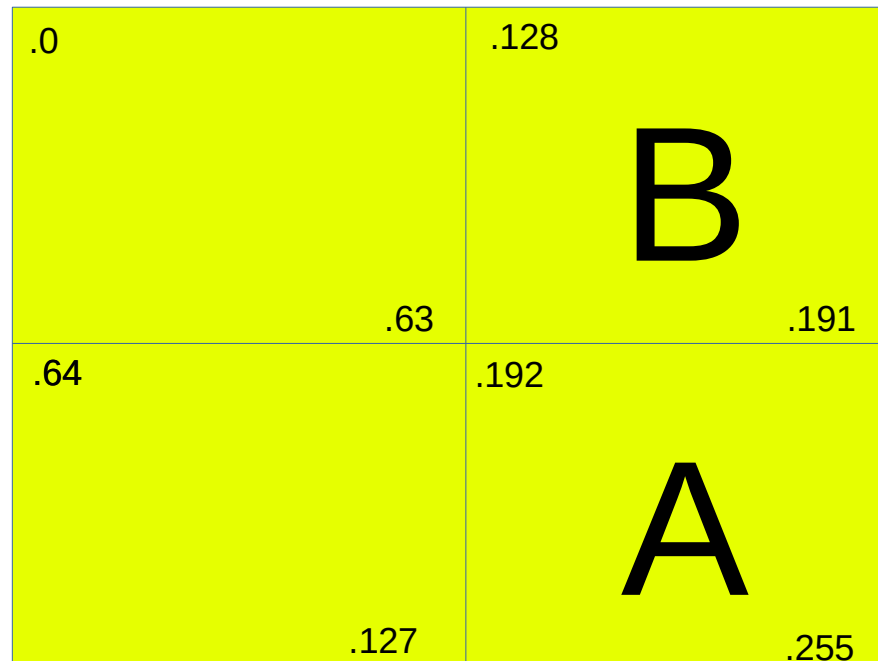
.0	.128
.63	.191
.64	.192
.127	.255

A

Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

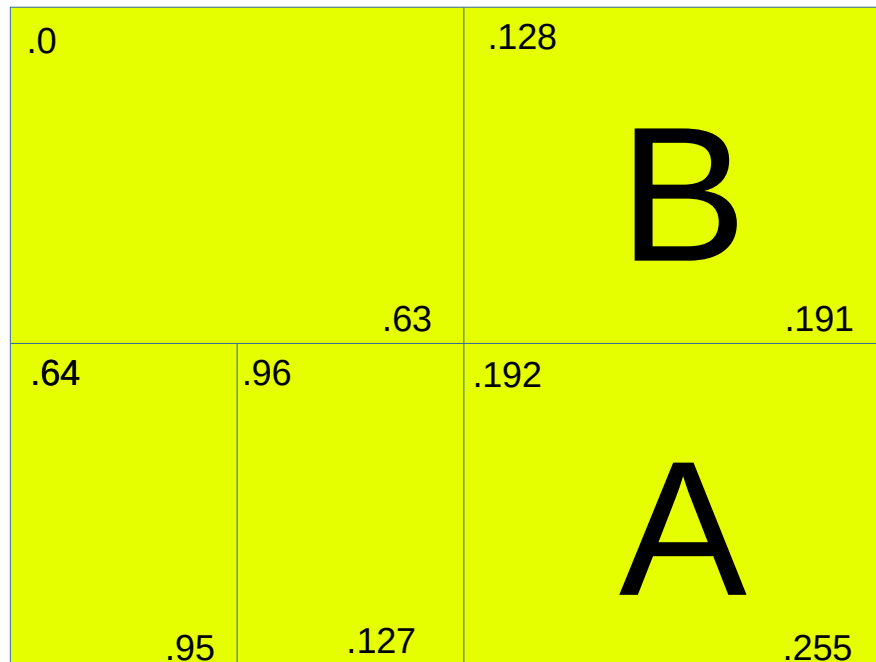
10.15.83.0/24



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

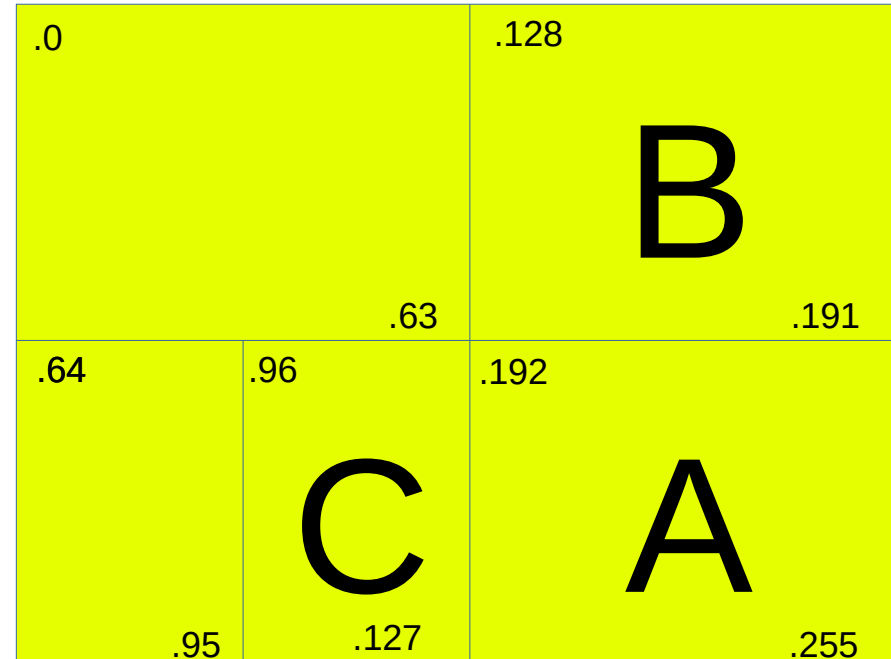
10.15.83.0/24



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

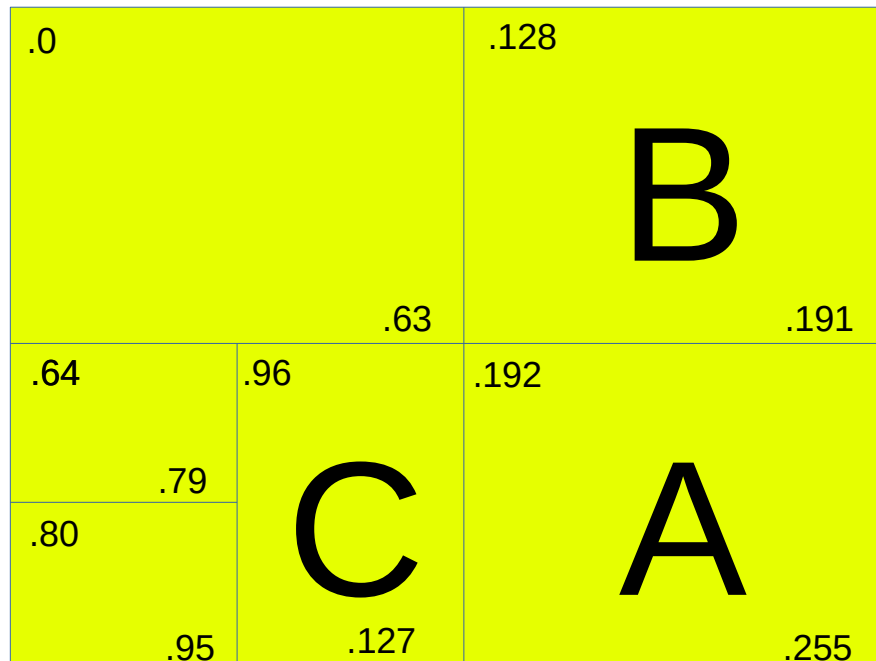
10.15.83.0/24



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

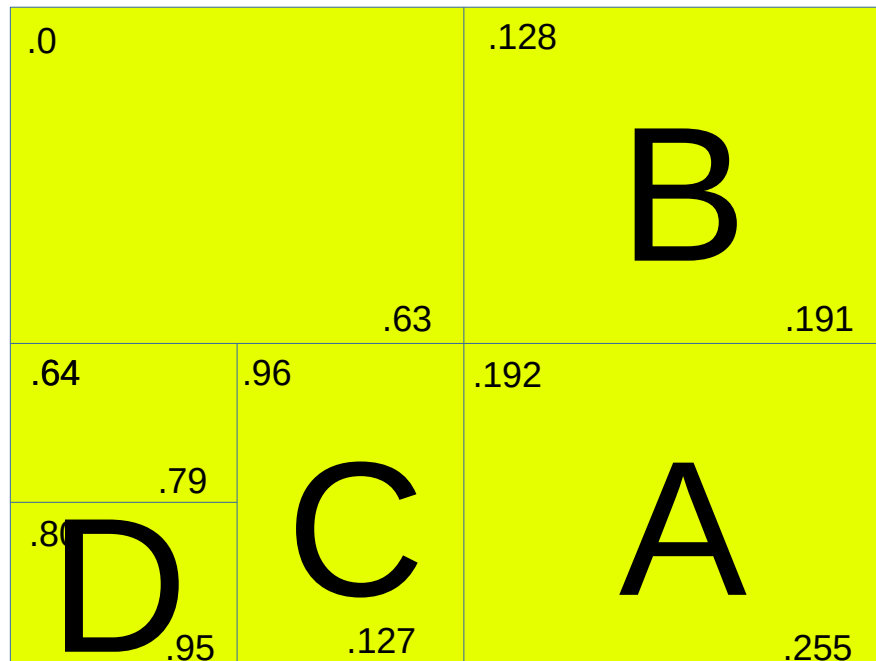
10.15.83.0/24



Podsítování

10.15.83.0/24

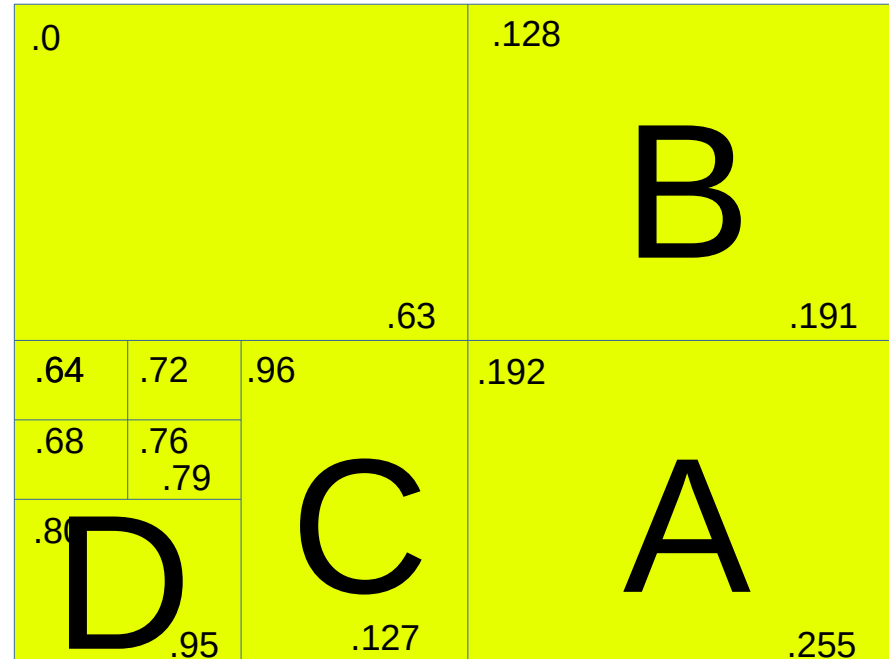
- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)



Podsítování

- 10.15.80.0/22
- A) 40 zařízení
 - $2^6 \rightarrow /26$
- B) 60 zařízení
 - $2^6 \rightarrow /26$
- C) 16 zařízení
 - $2^5 \rightarrow /27$
- D) 14 zařízení
 - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

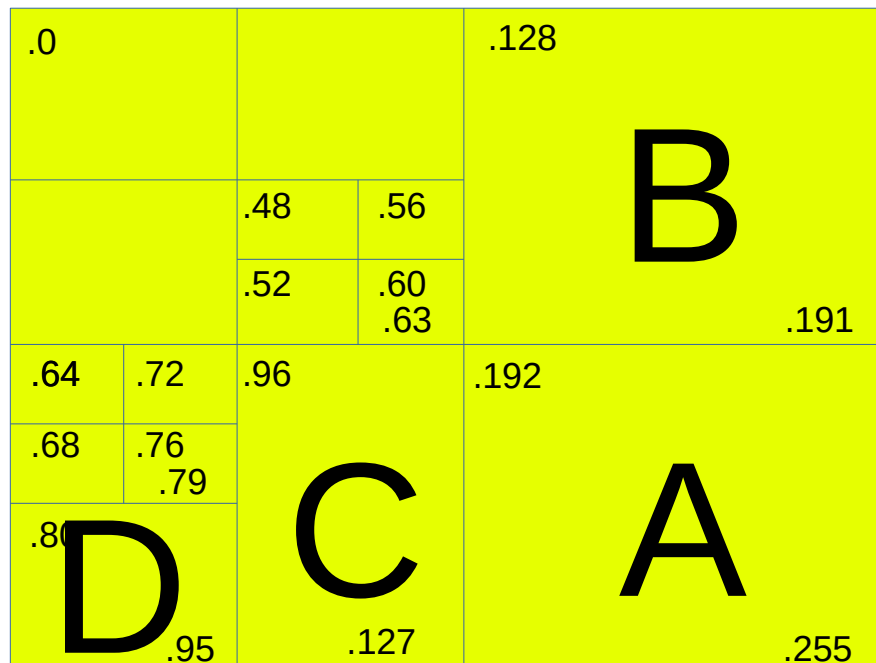
10.15.83.0/24



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - $2^6 \rightarrow /26$
 - B) 60 zařízení
 - $2^6 \rightarrow /26$
 - C) 16 zařízení
 - $2^5 \rightarrow /27$
 - D) 14 zařízení
 - $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - $2^2 \rightarrow /30$ (8-krát)

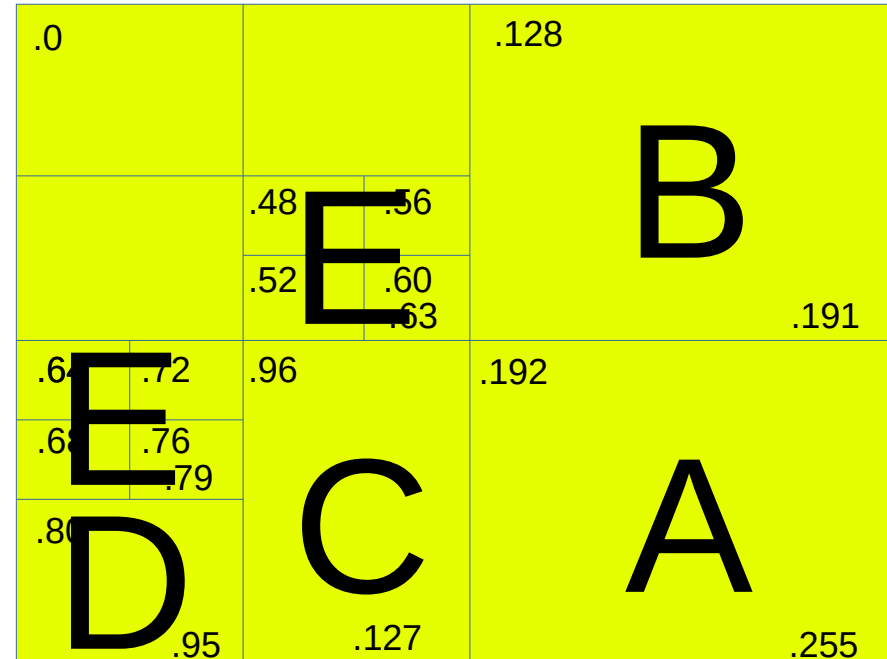
10.15.83.0/24



Podsítování

- 10.15.80.0/22
 - A) 40 zařízení
 - ◆ $2^6 \rightarrow /26$
 - B) 60 zařízení
 - ◆ $2^6 \rightarrow /26$
 - C) 16 zařízení
 - ◆ $2^5 \rightarrow /27$
 - D) 14 zařízení
 - ◆ $2^4 \rightarrow /28$
 - E) 8 point-to-point propojů
 - ◆ $2^2 \rightarrow /30$ (8-krát)

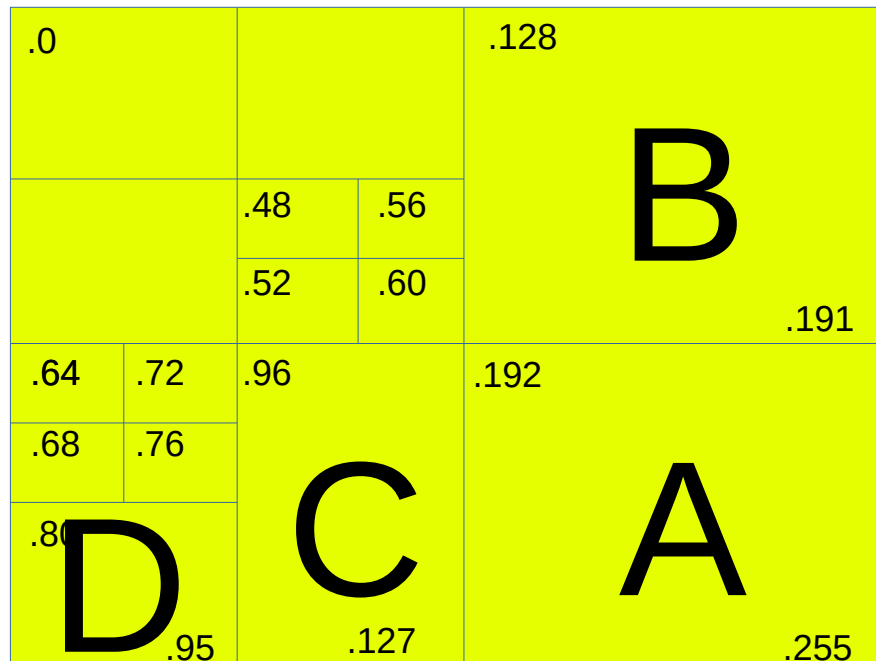
10.15.83.0/24

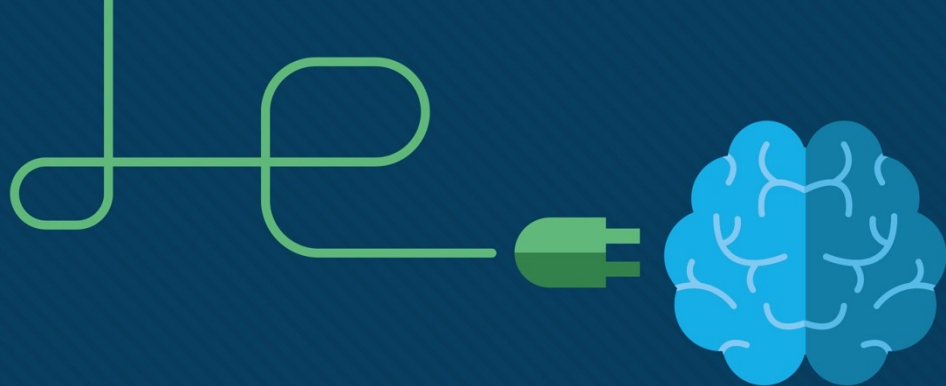


Podsítování

- 10.15.80.0/22
- A) 10.15.83.192/26
- B) 10.15.83.128/26
- C) 10.15.83.96/27
- D) 10.15.83.80/28
- E) 8 point-to-point propojů
 - 10.15.83.48/30
 - 10.15.83.52/30
 - 10.15.83.56/30
 - 10.15.83.60/30
 - 10.15.83.64/30
 - 10.15.83.68/30
 - 10.15.83.72/30
 - 10.15.83.76/30

10.15.83.0/24





Module 9: Address Resolution

Introduction to Networks v7.0
(ITN)



Module Objectives

Module Title: Address Resolution

Module Objective: Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery » IPv6	Describe the operation of IPv6 neighbor discovery.

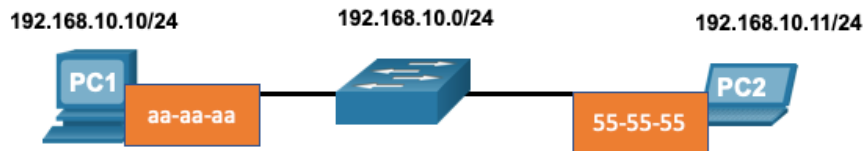
9.1 MAC and IP

Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.



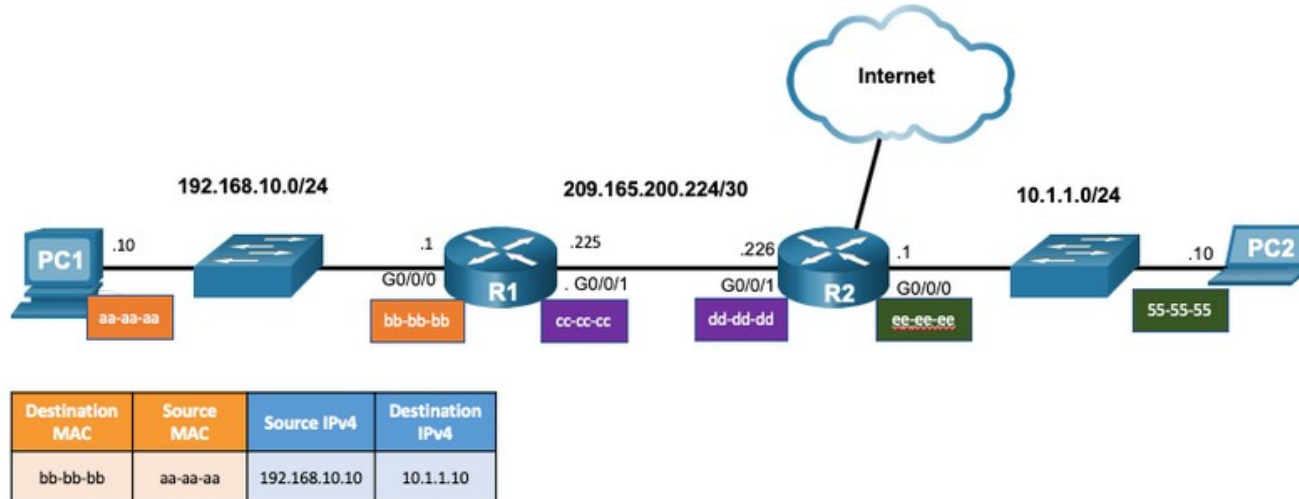
Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

MAC and IP

Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



9.2 ARP (IPv4)

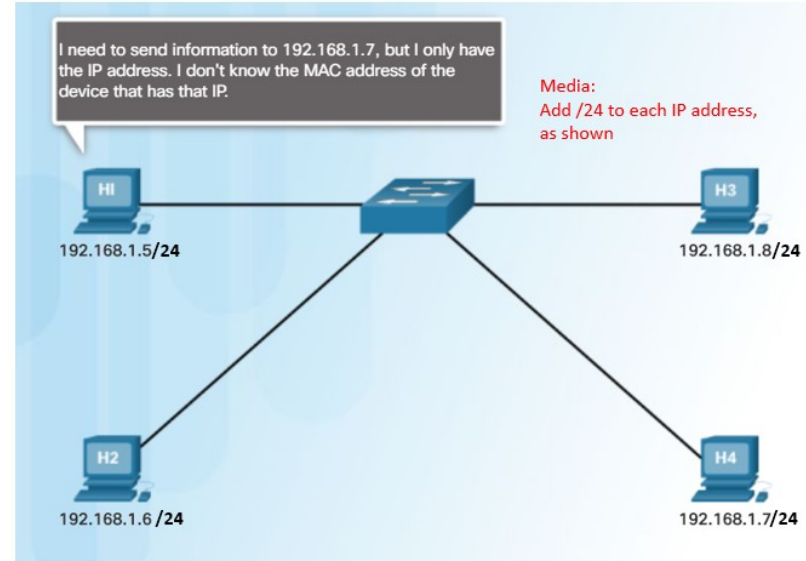
ARP

ARP Overview

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining an ARP table of IPv4 to MAC address mappings



ARP

ARP Functions

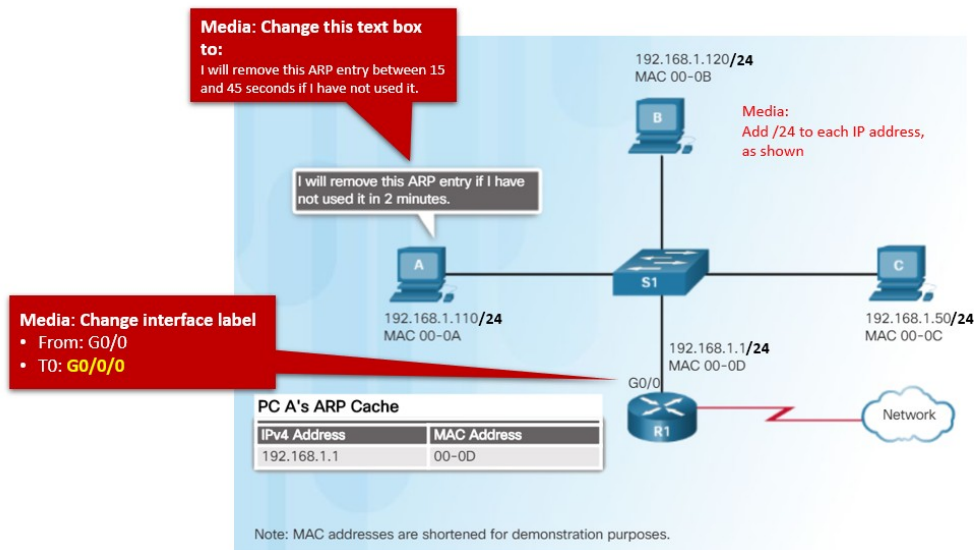
To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's **destination IPv4 address is on the same network**, the device will *search the ARP table for the destination IPv4 address*.
- If the **destination IPv4 address is on a different network**, the device will *search the ARP table for the IPv4 address of the default gateway*.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If there is **no ARP table entry is found**, then the device sends an **ARP request**.

ARP

Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer **expires after a specified period of time**.
- The duration of the ARP cache timer **differs depending on the operating system**.
- ARP table entries can also be removed manually by the administrator.



ARP

ARP Tables on Networking Devices

- The **show ip arp** command displays the ARP table on a Cisco router.
- The **arp -a** command displays the ARP table on a Windows 10 PC.

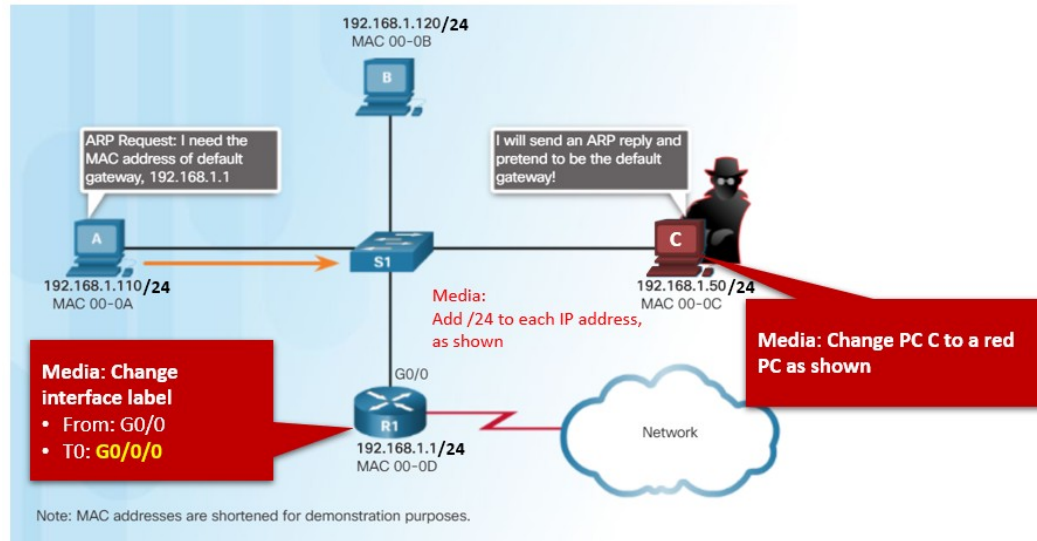
```
R1# show ip arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 192.168.10.1    -         a0e0.af0d.e140 ARPA   GigabitEthernet0/0/0
```

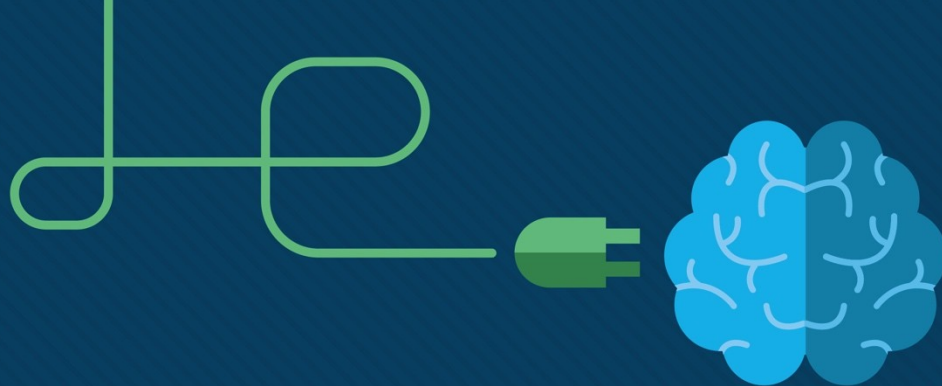
```
C:\Users\PC> arp -a
```

```
Interface: 192.168.1.124 --- 0x10
Internet Address      Physical Address      Type
192.168.1.1           c8-d7-19-cc-a0-86     dynamic
192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

ARP Issues – ARP Broadcasting and ARP Spoofing

- ARP requests are received and **processed by every device** on the local network.
- Excessive ARP broadcasts can cause some **reduction in performance**.
- ARP replies can be **spoofed** by a threat actor to perform an ARP poisoning attack.
- Enterprise level switches include **mitigation techniques** to protect against ARP attacks.



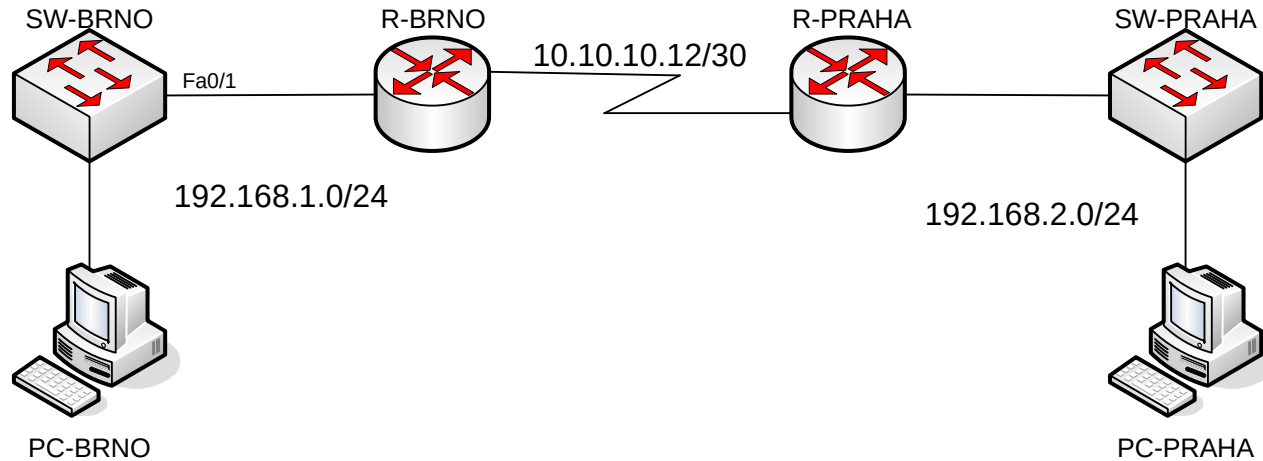


Module 14: Routing Concepts

Switching, Routing, and Wireless Essentials v7.0
(SRWE)



Motivation from the last lab



Module Objectives

Module Title: Routing Concepts

Module Objective: Explain how routers use information in packets to make forwarding decisions.

Topic Title	Topic Objective
Path Determination	Explain how routers determine the best path.
Packet Forwarding	Explain how routers forward packets to the destination.
Basic Router Configuration Review	Configure basic settings on a router.
IP Routing Table	Describe the structure of a routing table.
Static and Dynamic Routing	Compare static and dynamic routing concepts.

14.1 Path Determination

Two Functions of a Router

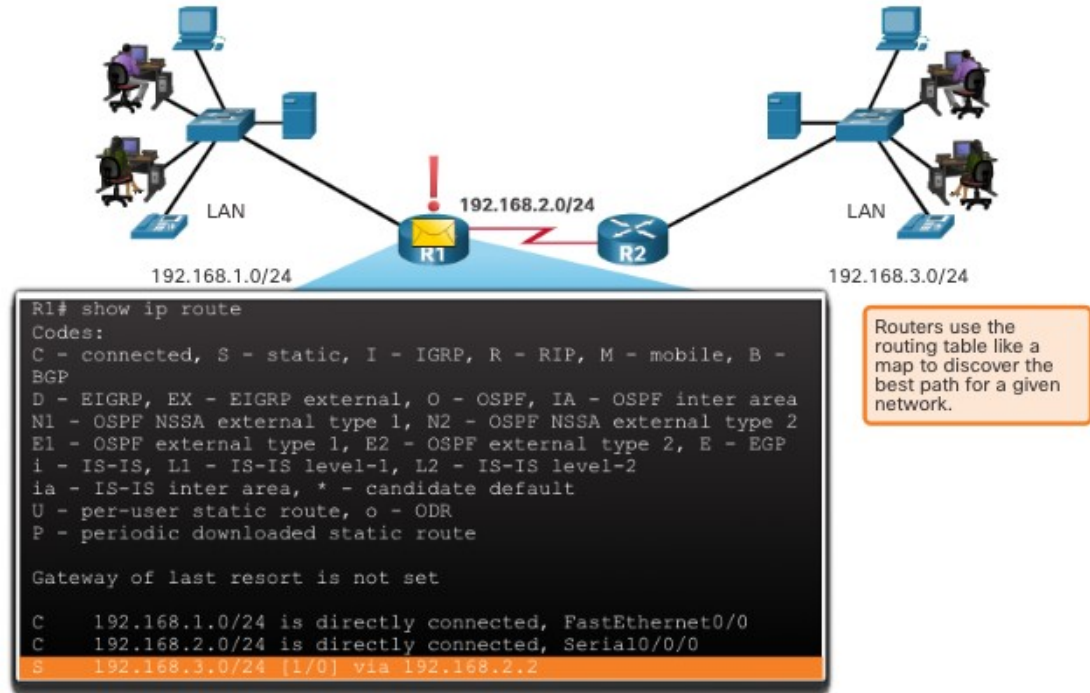
The primary functions of a router are to **determine the best path to forward packets based on the information in its routing table**, and to forward packets toward their destination.

When a router receives an IP packet on one interface, it determines which interface to use to **forward the packet to the destination**. This is known as **routing**. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network. Each network that a router connects to typically requires a separate interface, but this may not always be the case.

Path Determination

Router Functions Example

The router uses its IP routing table to determine which path (route) to use to forward a packet. R1 and R2 will use their respective IP routing tables to first determine the best path, and then forward the packet.



Best Path Equals Longest Match

- The best path in the routing table is also known as the longest match.
- The **routing table** contains route entries consisting of a
 - **prefix (network address) and prefix length.**
 - For there to be a match between the destination IP address of a packet and a route in the routing table, a minimum number of far-left bits must match between the IP address of the packet and the route in the routing table. The **prefix length** of the route in the routing table is used to determine the **minimum number of far-left bits that must match.**
- **The longest match** is the route in the routing table that has the **greatest number of far-left matching bits with the destination IP address of the packet.** The longest match is always the preferred route.

Note: The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.

IPv4 Longest Match Example

In the table, an IPv4 packet has the destination IPv4 address 172.16.0.10. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and would be chosen to forward the packet. For any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.

Destination IPv4 Address		Address in Binary
172.16.0.10		10101100.00010000.00000000.00001010
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	172.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.0/26	10101100.00010000.00000000.00001010

IPv6 Longest Match Example

An IPv6 packet has the destination IPv6 address 2001:db8:c000::99. This example shows three route entries, but only two of them are a valid match, with one of those being the longest match. The first two route entries have prefix lengths that have the required number of matching bits as indicated by the prefix length. The third route entry is not a match because its /64 prefix requires 64 matching bits.

Destination	2001:db8:c000::99/48	
Route Entry	Prefix/Prefix Length	Does it match?
1	2001:db8:c000::/40	Match of 40 bits
2	2001:db8:c000::/48	Match of 48 bits (longest match)
3	2001:db8:c000:5555::/64	Does not match 64 bits

Path Determination

Build the Routing Table

Directly Connected Networks: Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

Remote Networks: Networks that are not directly connected to the router. Routers learn about remote networks in two ways:

- **Static routes** - Added to the routing table when a route is manually configured.
- **Dynamic routing protocols** - Added to the routing table when routing protocols dynamically learn about the remote network.

Default Route: Specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. The default route can be entered **manually as a static route, or learned automatically from a dynamic routing protocol.**

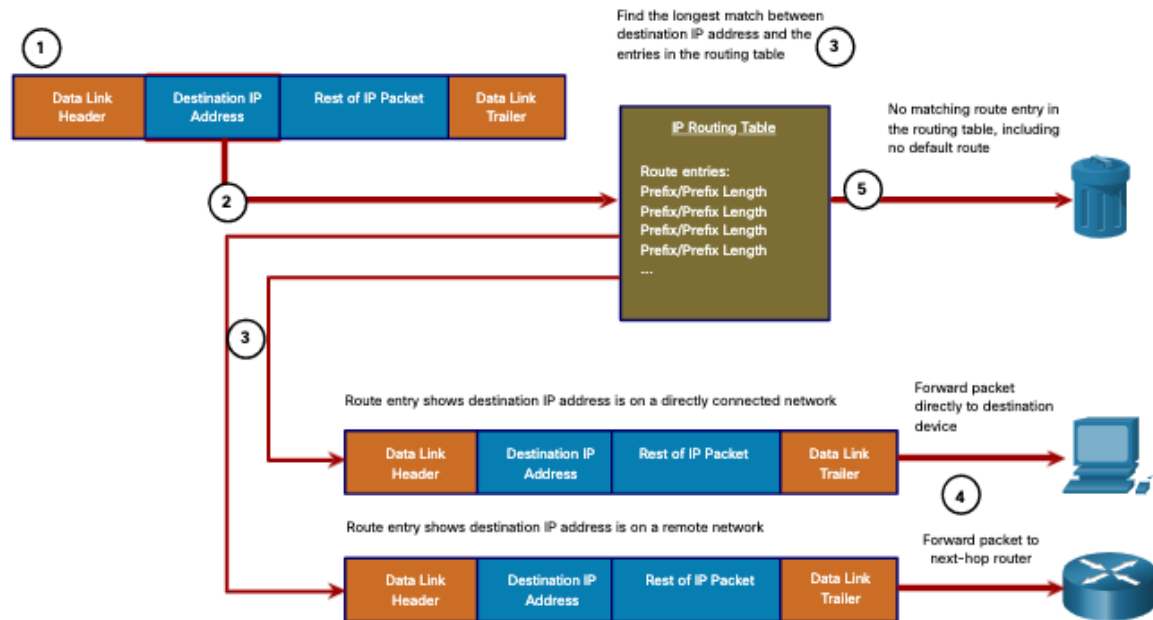
- A default route has a /0 prefix length. This means that no bits need to match the destination IP address for this route entry to be used. If there are no routes with a match longer than 0 bits, the default route is used to forward the packet. The default route is sometimes referred to as a gateway of last resort.

14.2 Packet Forwarding

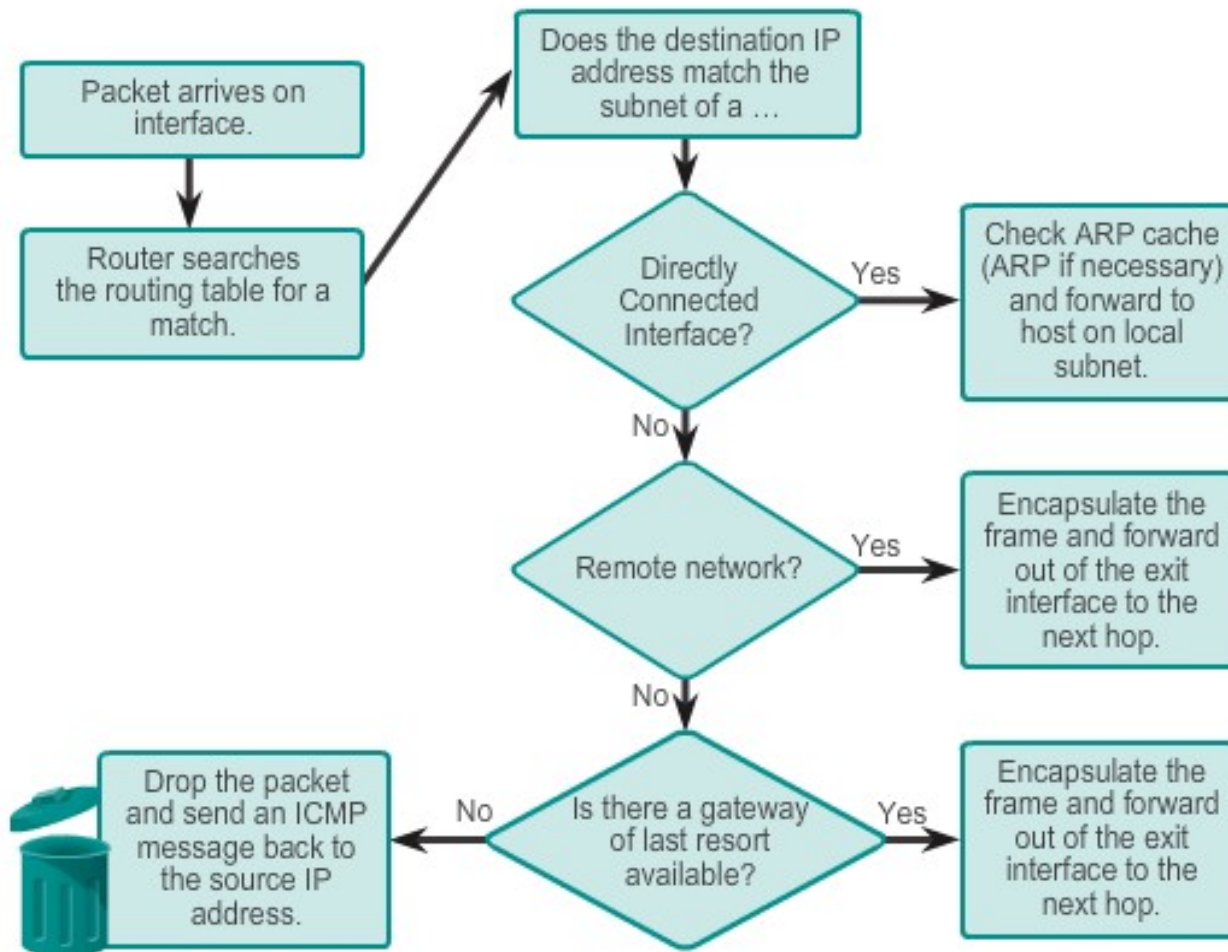
Packet Forwarding

Packet Forwarding Decision Process

1. The data link frame with an encapsulated IP packet arrives on the ingress interface.
2. The router examines the **destination IP address** in the packet header and consults its IP routing table.
3. The router **finds the longest matching prefix** in the routing table.
4. The router **encapsulates** the packet in a **data link frame** and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.
5. However, if there is **no matching route** entry the packet is dropped.



Packet Forwarding Decision Process



Packet Forwarding Mechanisms

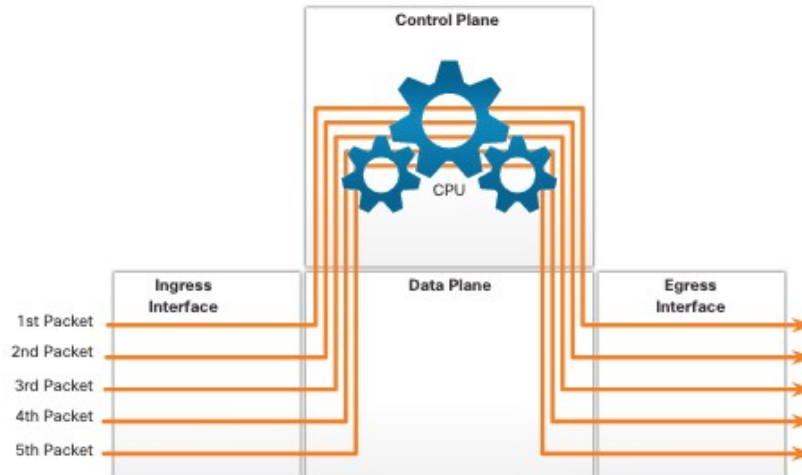
The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface. The more efficiently a router can perform this task, the faster packets can be forwarded by the router.

Routers support the following three packet forwarding mechanisms:

- **Process switching**
- **Fast switching**
- **Cisco Express Forwarding (CEF)**

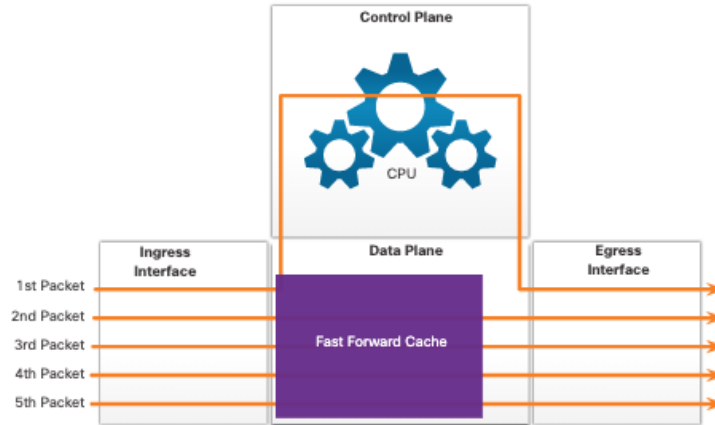
Packet Forwarding Mechanisms (Cont.)

Process Switching: An older packet forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane where the **CPU matches the destination address** with an entry in its routing table, and then determines the exit interface and forwards the packet. It is important to understand that the router does this for **every packet**, even if the destination is the same for a stream of packets.



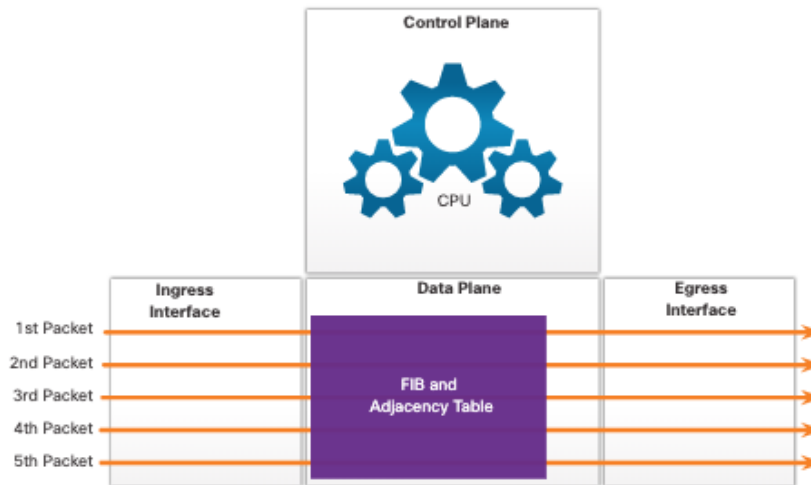
Packet Forwarding Mechanisms (Cont.)

- **Fast Switching:** Another, older packet forwarding mechanism which was the successor to process switching. Fast switching uses a **fast-switching cache** to store next-hop information. When a packet arrives on an interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache. If it is not there, it is **process-switched** and forwarded to the exit interface. The flow information for the packet is then **stored in the fast-switching cache**. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is re-used without CPU intervention.



Packet Forwarding Mechanisms (Cont.)

- **Cisco Express Forwarding (CEF):** The most recent and **default** Cisco IOS packet-forwarding mechanism. CEF builds a **Forwarding Information Base (FIB)**, and an **adjacency table**. The table entries are not packet-triggered like fast switching but **change-triggered**, such as when something changes in the network topology. When a network has **converged**, the FIB and adjacency tables contain **all the information** that a router would have to consider when forwarding a packet.



14.3 Basic Router Configuration Review

Basic Router Configuration Review

Verification Commands

Common verification commands include the following:

- **show ip interface brief**
- **show running-config interface** *interface-type number*
- **show interfaces**
- **show ip interface**
- **show ip route**
- **ping**

In each case, replace **ip** with **ipv6** for the IPv6 version of the command.

Basic Router Configuration Review

Filter Command Output

Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the **show** command and then enter a filtering parameter and a filtering expression.

The filtering parameters that can be configured after the pipe include:

- **section** - This displays the entire section that starts with the filtering expression.
- **include** - This includes all output lines that match the filtering expression.
- **exclude** - This excludes all output lines that match the filtering expression.
- **begin** - This displays all the output lines from a certain point, starting with the line that matches the filtering expression.

Note: Output filters can be used in combination with any **show** command.

14.4 IP Routing Table

IP Routing Table

Route Sources

A routing table contains a **list of routes to known networks** (prefixes and prefix lengths). The source of this information is derived from the following:

- **Directly connected networks**
- **Static routes**
- **Dynamic routing protocols**

The source for each route in the routing table is identified by a code. Common codes include the following:

- **L** - Identifies the address assigned to a router interface.
- **C** - Identifies a directly connected network.
- **S** - Identifies a static route created to reach a specific network.
- **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
- **R** - Identifies a dynamically learned network from another router using the RIP routing protocol.
- ***** - This route is a candidate for a default route.

IP Routing Table

Routing Table Principles

There are three routing table principles as described in the table. These are issues that are addressed by the proper configuration of dynamic routing protocols or static routes on all the routers between the source and destination devices.

Routing Table Principle	Example
Every router makes its decision alone , based on the information it has in its own routing table.	<ul style="list-style-type: none">•R1 can only forward packets using its own routing table.•R1 does not know what routes are in the routing tables of other routers (e.g., R2).
The information in a routing table of one router does not necessarily match the routing table of another router .	Just because R1 has route in its routing table to a network in the internet via R2, that does not mean that R2 knows about that same network.
Routing information about a path does not provide return routing information (routes are one-way).	R1 receives a packet with the destination IP address of PC1 and the source IP address of PC3. Just because R1 knows to forward the packet out its G0/0/0 interface, doesn't necessarily mean that it knows how to forward packets originating from PC1 back to the remote network of PC3

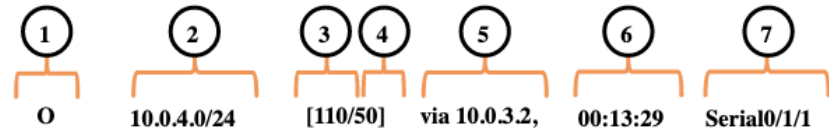
IP Routing Table

Routing Table Entries

In the figure, the numbers identify the following information:

- **Route source** - This identifies how the route was learned.
- **Destination network (prefix and prefix length)** - This identifies the address of the remote network.
- **Administrative distance** - This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
- **Metric** - This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next-hop** - This identifies the IP address of the next router to which the packet would be forwarded.
- **Route timestamp** - This identifies how much time has passed since the route was learned.
- **Exit interface** - This identifies the egress interface to use for outgoing packets to reach their final destination.

IPv4 Routing Table



IPv6 Routing Table



Note: The prefix length of the destination network specifies the minimum number of far-left bits that must match between the IP address of the packet and the destination network (prefix) for this route to be used.

IP Routing Table

Directly Connected Networks

To learn about any remote networks, the router must have at least one active interface configured with an IP address and subnet mask (prefix length). This is known as a directly connected network or a directly connected route. **Routers add a directly connected route to its routing table when an interface is configured with an IP address and is activated.**

- A directly connected network is denoted by a status code of **C** in the routing table. The route contains a network prefix and prefix length.
- The routing table also contains a local route for each of its directly connected networks, indicated by the status code of **L**.
- For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match. The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

IP Routing Table

Static Routes

After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks. **Static routes are manually configured.** They define an explicit path between two networking devices. They are not automatically updated and must be manually reconfigured if the network topology changes.

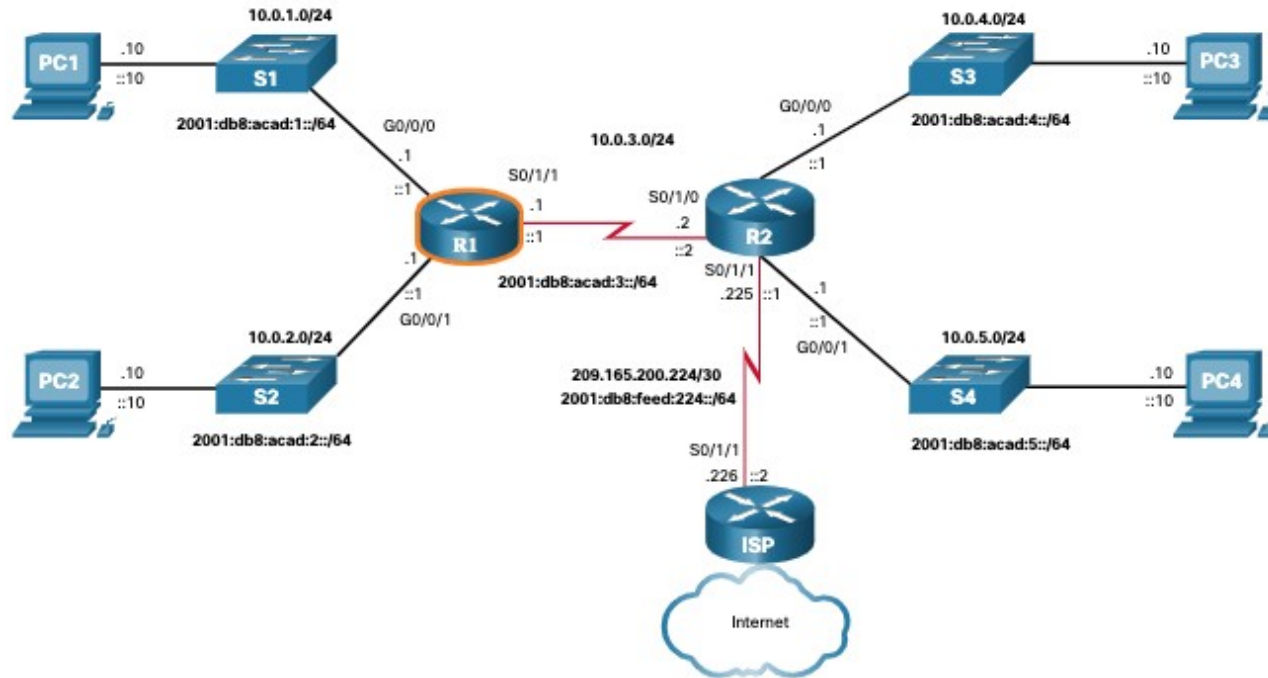
Static routing has three primary uses:

- It provides ease of routing table maintenance in **smaller networks** that are not expected to grow significantly.
- It uses a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.
- It routes to and from **stub networks**. A stub network is a network accessed by a single route, and the router has only one neighbor.

Basic Router Configuration Review

Topology

The topology in the figure will be used for configuration and verification examples. It will also be used in the next topic to discuss the IP routing table.



Basic Router Configuration Review

Configuration Commands

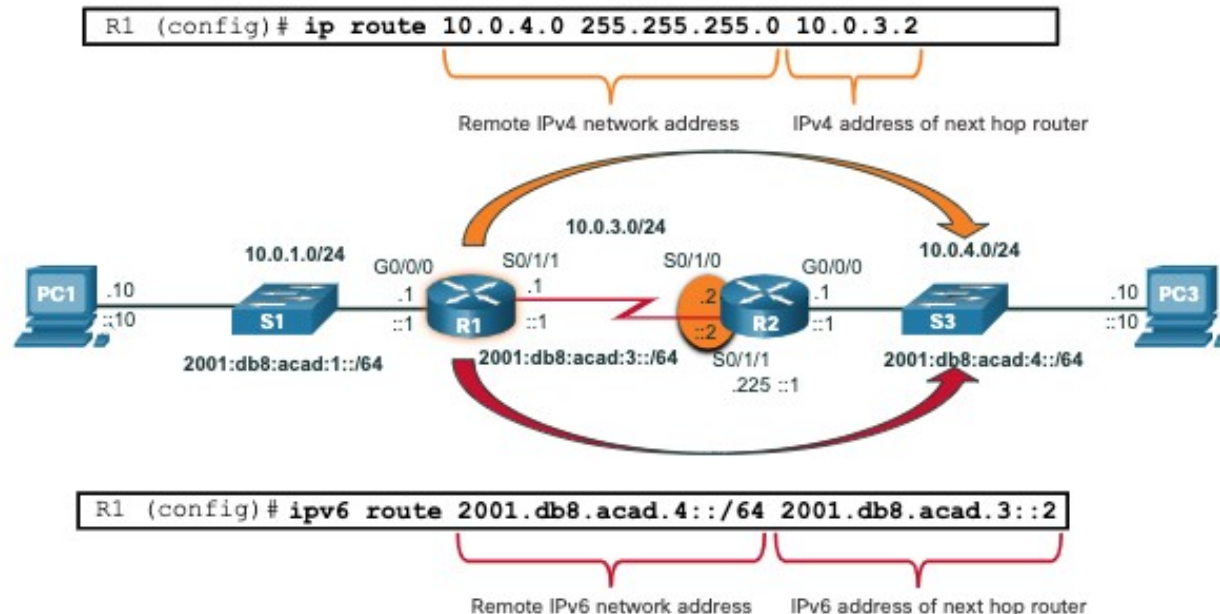
```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption R1(config)#
banner motd #
*****
WARNING: Unauthorized access is prohibited!
*****
#
```

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

IP Routing Table

Static Routes in the IP Routing Table

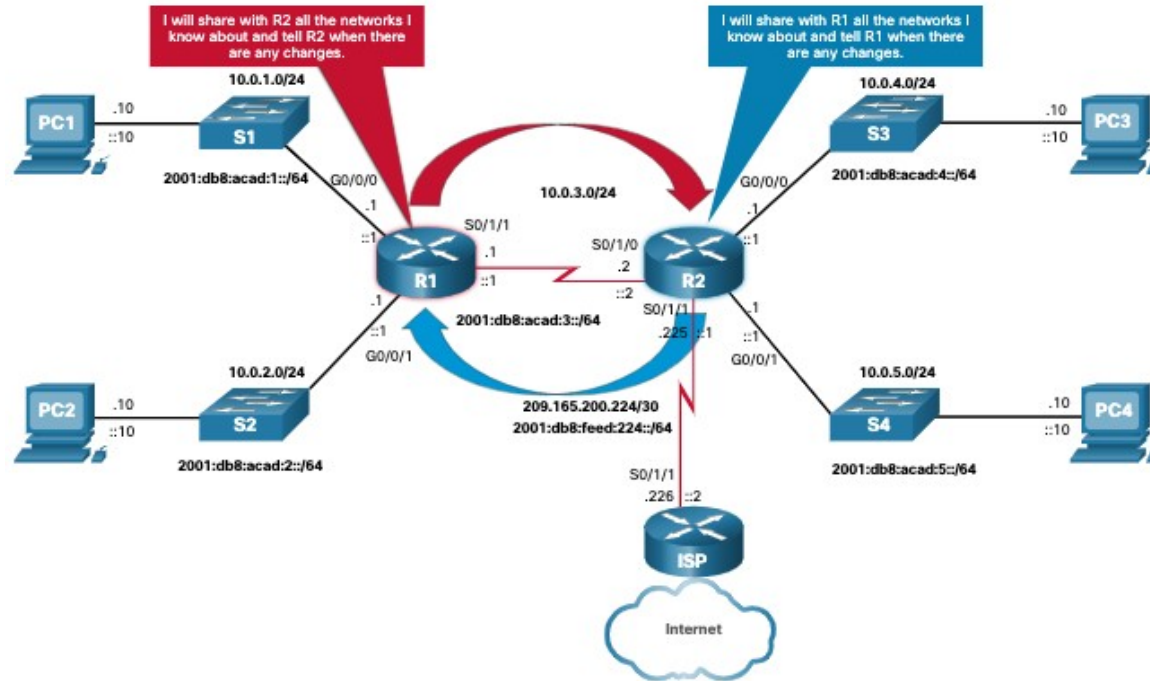
The topology in the figure is simplified to show only one LAN attached to each router. The figure shows IPv4 and IPv6 static routes **configured** on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2.



IP Routing Table

Dynamic Routing Protocols

Dynamic routing protocols are used by routers to **automatically share information about the reachability and status of remote networks**. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.



IP Routing Table

Dynamic Routes in the Routing Table

OSPF is now being used in our sample topology to dynamically learn all the networks connected to R1 and R2. The routing table entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol. Both entries also include the IP address of the next-hop router, via *ip-address*.

Note: IPv6 routing protocols use the link-local address of the next-hop router.

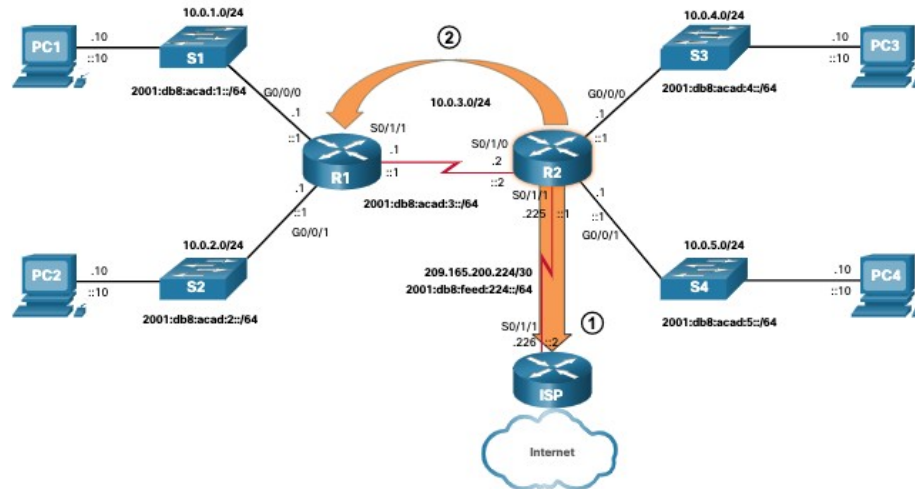
Note: OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

```
R1# 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
(output omitted for brevity)
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
NDR - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O 2001:DB8:ACAD:4::/64 [110/50]
  via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
  via FE80::2:C, Serial0/1/1
```

IP Routing Table

Default Route

The default route specifies a next-hop router to use **when the routing table does not contain a specific route** that matches the destination IP address. A default route can be either a **static route** or **learned automatically from a dynamic routing protocol**. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or **no bits need to match between the destination IP address** and the default route.



IP Routing Table

Structure of an IPv4 Routing Table

IPv4 was standardized using the now obsolete classful addressing architecture. The IPv4 **routing table is organized using this same classful structure**. Although **the lookup process no longer uses classes**, the structure of the IPv4 routing table still retains in this format.

- An indented entry is known as a **child route**. A route entry is indented if it is the subnet of a classful address (class A, B or C network).
- Directly connected networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32.
- The child route will include the route source and all the forwarding information such as the next-hop address.
- The classful network address of this subnet will be shown above the route entry, less indented, and without a source code. That route is known as a **parent route**.

```
Router# show ip route
(Output omitted)
    192.168.1.0/24 is variably..
C    192.168.1.0/24 is direct..
L    192.168.1.1/32 is direct..
O    192.168.2.0/24 [110/65]..
O    192.168.3.0/24 [110/65]..
    192.168.12.0/24 is variab..
C    192.168.12.0/30 is direct..
L    192.168.12.1/32 is direct..
    192.168.13.0/24 is variably..
C    192.168.13.0/30 is direct..
L    192.168.13.1/32 is direct..
    192.168.23.0/30 is subnette..
O    192.168.23.0/30 [110/128]..
Router#
```

IP Routing Table

Structure of an IPv6 Routing Table

The concept of classful addressing was never part of IPv6, so the structure of an IPv6 routing table is very straight forward. Every IPv6 route entry is formatted and aligned the same way.

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
    via FE80::2:C, Serial0/0/1
C 2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/1, receive
O 2001:DB8:ACAD:4::/64 [110/50]
    via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
    via FE80::2:C, Serial0/1/1
L FF00::/8 [0/0]
    via Null0, receive
R1#
```


IP Routing Table

Administrative Distance

A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, **it is possible that the routing table learns about the same network address from more than one routing source**. Except for very specific circumstances, only one dynamic routing protocol should be implemented on a router. Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.

This raises a few questions, such as the following:

- How does the router know which source to use?
- Which route should it install in the routing table?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. **The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.**

IP Routing Table

Administrative Distance (Cont.)

The table lists various routing protocols and their associated ADs.

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

14.5 Static and Dynamic Routing

Static and Dynamic Routing

Static or Dynamic?

Static and dynamic routing are not mutually exclusive. Rather, most networks use a combination of dynamic routing protocols and static routes.

Static routes are commonly used in the following scenarios:

- As a **default route** forwarding packets to a service provider
- For routes outside the routing domain and not learned by the dynamic routing protocol
- When the network administrator wants to **explicitly define the path** for a specific network
- For **routing between stub networks**

Static routes are useful for smaller networks with only one path to an outside network. They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.

Static and Dynamic Routing

Static or Dynamic? (Cont.)

Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers. Dynamic routing protocols are scalable and automatically determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

- In networks consisting of more than just a few routers (**larger networks**)
- When a change in the network topology requires the network to **automatically determine another path**
- For **scalability**. As the network grows, the dynamic routing protocol automatically learns about any new networks.

Static and Dynamic Routing

Static or Dynamic? (Cont.)

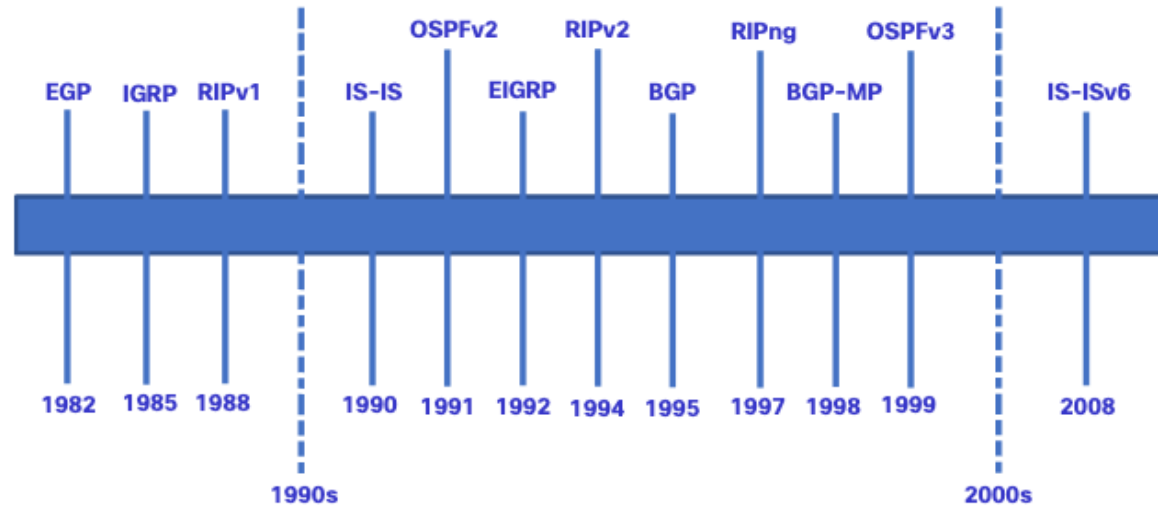
The table shows a comparison of some the differences between dynamic and static routing.

Feature	Dynamic Routing	Static Routing
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed
Path Predictability	Route depends on topology and routing protocol used	Explicitly defined by the administrator

Static and Dynamic Routing

Dynamic Routing Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969. As networks evolved and became more complex, new routing protocols emerged.



Static and Dynamic Routing

Dynamic Routing Paradigms

- **Interior Gateway Protocols (IGPs)** are routing protocols used to exchange routing information within a routing domain administered by a single organization.
- **Exterior Gateway Protocol** (There is only one EGP – BGP) is used to exchange routing information between different organizations, known as autonomous systems (AS). BGP is used by ISPs to route packets over the internet.
- Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Static and Dynamic Routing

Dynamic Routing Protocol Concepts

A routing protocol is a **set of processes, algorithms, and messages** that are used to exchange routing information and populate the routing table with the choice of best paths. The purpose of dynamic routing protocols includes the following:

- **Discovery of remote networks**
- **Maintaining up-to-date routing information**
- **Choosing the best path to destination networks**
- Ability to **find a new best path** if the current path is no longer available

Dynamic Routing Protocol Concepts (Cont.)

The main components of dynamic routing protocols include the following:

- **Data structures** - Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages** - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm** - An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for the best path determination.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table if there is not another routing source with a lower AD.

Static and Dynamic Routing

Best Path

The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. **The best path to a network is the path with the lowest metric.**

Dynamic routing protocols typically use their **own rules and metrics** to build and update routing tables. The following table lists common dynamic protocols and their metrics.

Routing Protocol	Metric
Routing Information Protocol (RIP)	<ul style="list-style-type: none">•The metric is “hop count”.•Each router along a path adds a hop to the hop count.•A maximum of 15 hops allowed.
Open Shortest Path First (OSPF)	<ul style="list-style-type: none">•The metric is “cost” which is based on the cumulative bandwidth from source to destination.•Faster links are assigned lower costs compared to slower (higher cost) links.
Enhanced Interior Gateway Routing Protocol (EIGRP)	<ul style="list-style-type: none">•It calculates a metric based on the slowest bandwidth and delay values.•It could also include load and reliability into the metric calculation.

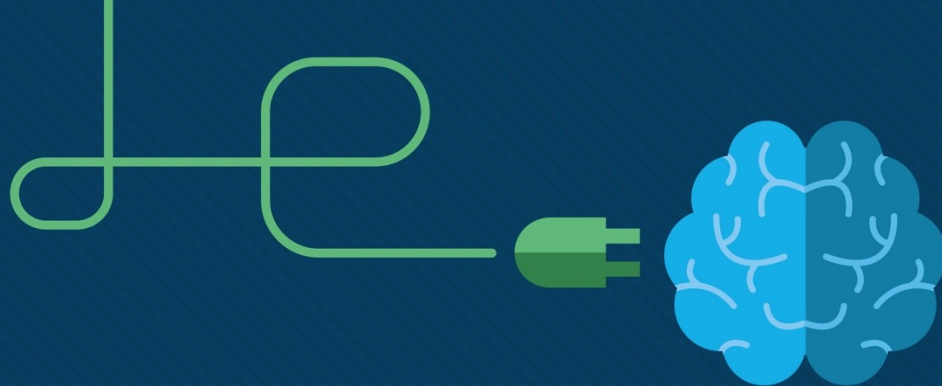
Static and Dynamic Routing

Load Balancing

When a router has **two or more paths to a destination with equal cost metrics**, then the router forwards the packets using both paths equally. This is called equal cost load balancing.

- The routing table contains the single destination network, but has **multiple exit interfaces**, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.
- If configured correctly, load balancing can **increase the effectiveness and performance** of the network.
- Equal cost load balancing is implemented automatically by dynamic routing protocols. It is enabled with static routes when there are multiple static routes to the same destination network using different next-hop routers.

Note: Only EIGRP supports unequal cost load balancing.



Module 15: IP Static Routing

Switching, Routing, and Wireless Essentials v7.0
(SRWE)



Module Objectives

Module Title: IP Static Routing

Module Objective: Configure IPv4 and IPv6 static routes.

Topic Title	Topic Objective
Static Routes	Describe the command syntax for static routes.
Configure IP Static Routes	Configure IPv4 and IPv6 static routes.
Configure IP Default Static Routes	Configure IPv4 and IPv6 default static routes.
Configure Floating Static Routes	Configure a floating static route to provide a backup connection.
Configure Static Host Routes	Configure IPv4 and IPv6 static host routes that direct traffic to a specific host.

15.1 Static Routes

Types of Static Routes

Static routes are commonly implemented on a network. This is true even when there is a dynamic routing protocol configured.

Static routes can be configured for IPv4 and IPv6. Both protocols support the following types of static routes:

- **Standard** static route
- **Default** static route
- **Floating** static route
- **Summary** static route

Static routes are configured using the **ip route** and **ipv6 route** global configuration commands.

Static Routes

Next-Hop Options

When configuring a static route, the next hop can be identified by an **IP address, exit interface, or both**. How the destination is specified creates one of the three following types of static route:

- **Next-hop route** - Only the next-hop IP address is specified
- **Directly connected static route** - Only the router exit interface is specified
- **Fully specified static route** - The next-hop IP address and exit interface are specified

IPv4 Static Route Command

IPv4 static routes are configured using the following global configuration command:

```
Router(config)# ip route network-address subnet-mask { ip-address  
| exit-intf [ip-address] } [distance]
```

Note: Either the *ip-address*, *exit-intf*, or the *ip-address* and *exit-intf* parameters must be configured.

IPv6 Static Route Command

IPv6 static routes are configured using the following global configuration command:

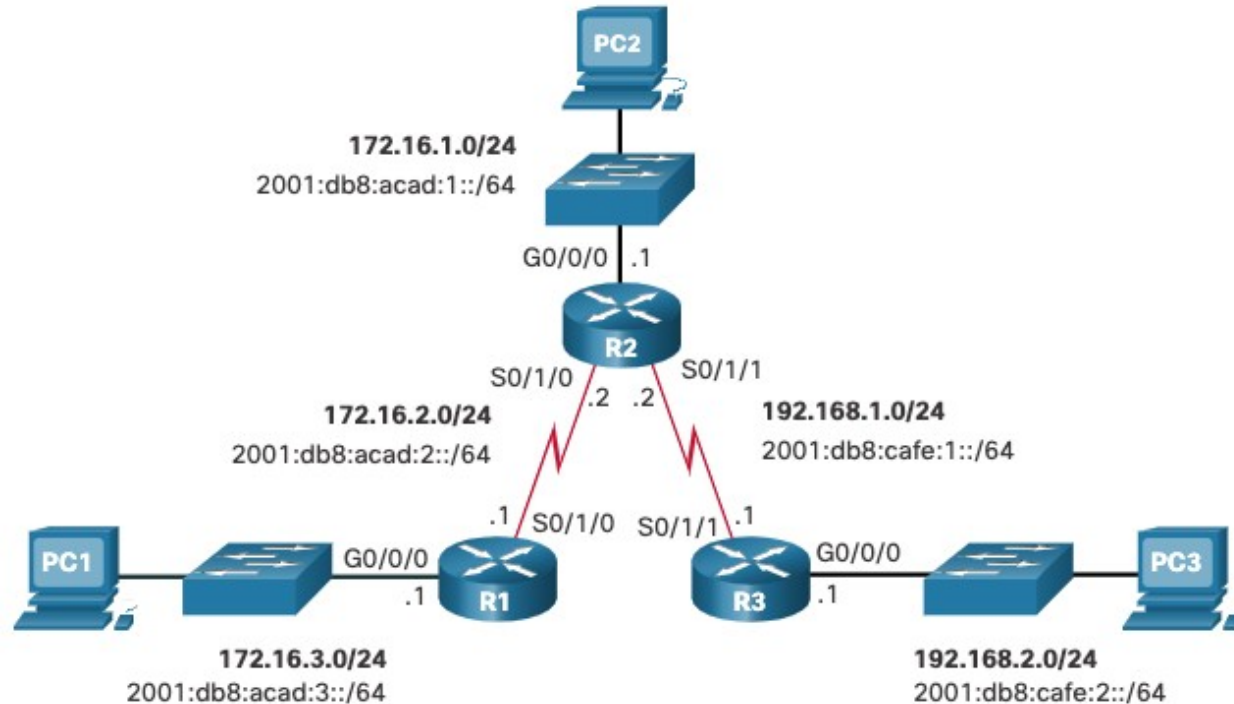
```
Router(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-address  
| exit-intf [ipv6-address]} [distance]
```

Most of parameters are identical to the IPv4 version of the command.

Static Routes

Dual-Stack Topology

The figure shows a dual-stack network topology. Currently, no static routes are configured for either IPv4 or IPv6.



Static Routes

IPv4 Starting Routing Tables

- Each router has entries only for directly connected networks and associated local addresses.
- R1 can ping R2, but cannot ping the R3 LAN

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.16.2.0/24 is directly connected, Serial0/1/0
L    172.16.2.1/32 is directly connected, Serial0/1/0
C    172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L    172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
R1#
R1# ping 172.16.2.2
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5)
R1# ping 192.168.2.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2
seconds: .....
Success rate is 0 percent (0/5)
```

IPv6 Starting Routing Tables

- Each router has entries only for directly connected networks and associated local addresses.
- R1 can ping R2, but cannot ping the R3 LAN.

```
R1# show ipv6 route | begin C
C 2001:DB8:ACAD:2::/64 [0/0]
  via Serial0/1/0, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
  via Serial0/1/0, receive
C 2001:DB8:ACAD:3::/64 [0/0]
  via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
  via GigabitEthernet0/0/0, receive
L FF00::/8 [0/0]
  via Null0, receive

R1#
R1# ping 2001:db8:acad:2::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
R1# ping 2001:DB8:cafe:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:2::1, timeout is 2 seconds:
% No valid route for destination
Success rate is 0 percent (0/1)
```

15.2 Configure IP Static Routes

Configure IP Static Routes

IPv4 Next-Hop Static Route

In a next-hop static route, only the **next-hop IP address** is specified. The exit interface is derived from the next hop. For example, three next-hop IPv4 static routes are configured on R1 using the IP address of the next hop, R2.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
```

```
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
```

```
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

The resulting routing table entries on R1:

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S      192.168.1.0/24 [1/0] via 172.16.2.2
S      192.168.2.0/24 [1/0] via 172.16.2.2
```


Configure IP Static Routes

IPv6 Next-Hop Static Route

The commands to configure R1 with the IPv6 static routes to the three remote networks are as follows:

```
R1(config)# ipv6 unicast-routing
```

```
R1(config)# ipv6 route 2001:db8:acad:1::/64  
2001:db8:acad:2::2
```

```
R1(config)# ipv6 route 2001:db8:cafe:1::/64  
2001:db8:acad:2::2
```

```
R1(config)# ipv6 route 2001:db8:cafe:2::/64  
2001:db8:acad:2::2
```

The routing table for R1 now has routes to the three remote IPv6 networks.

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, la - LISP away, le - LISP extranet-policy
       a - Application
S  2001:DB8:ACAD:1::/64 [1/0]
   via 2001:DB8:ACAD:2::2
C  2001:DB8:ACAD:2::/64 [0/0]
   via Serial0/1/0, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
   via Serial0/1/0, receive
C  2001:DB8:ACAD:3::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
S  2001:DB8:CAFE:1::/64 [1/0]
   via 2001:DB8:ACAD:2::2
S  2001:DB8:CAFE:2::/64 [1/0]
   via 2001:DB8:ACAD:2::2
L  FF00::/8 [0/0]
   via Null0, receive
```

IPv4 Directly Connected Static Route

When configuring a static route, another option is to use the **exit interface** to specify the next-hop address. Three directly connected IPv4 static routes are configured on R1 using the exit interface.

Note: Using a next-hop address is generally recommended. Directly connected static routes should only be used with point-to-point serial interfaces.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 s0/1/0
```

```
R1(config)# ip route 192.168.1.0 255.255.255.0 s0/1/0
```

```
R1(config)# ip route 192.168.2.0 255.255.255.0 s0/1/0
```

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 is directly connected, Serial0/1/0
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S       192.168.1.0/24 is directly connected, Serial0/1/0
S       192.168.2.0/24 is directly connected, Serial0/1/0
```

Configure IP Static Routes

IPv6 Directly Connected Static Route

In the example, three directly connected IPv6 static routes are configured on R1 using the exit interface.

Note: Using a next-hop address is generally recommended. Directly connected static routes should only be used with point-to-point serial interfaces.

```
R1(config)# ipv6 route 2001:db8:acad:1::/64  
s0/1/0
```

```
R1(config)# ipv6 route 2001:db8:cafe:1::/64  
s0/1/0
```

```
R1(config)# ipv6 route 2001:db8:cafe:2::/64  
s0/1/0
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S 2001:DB8:ACAD:1::/64 [1/0]
  via Serial0/1/0, directly connected
C 2001:DB8:ACAD:2::/64 [0/0]
  via Serial0/1/0, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
  via Serial0/1/0, receive
C 2001:DB8:ACAD:3::/64 [0/0]
  via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
  via GigabitEthernet0/0/0, receive
S 2001:DB8:CAFE:1::/64 [1/0]
  via Serial0/1/0, directly connected
S 2001:DB8:CAFE:2::/64 [1/0]
  via Serial0/1/0, directly connected
L FF00::/8 [0/0]
  via Null0, receive
IPv6 Routing Table - default - 8 entries
R1#
```

Configure IP Static Routes

IPv4 Fully Specified Static Route

- In a fully specified static route, **both the exit interface and the next-hop IP address are specified**. This form of static route is used when the exit interface is a multi-access interface and it is necessary to explicitly identify the next hop. The next hop must be directly connected to the specified exit interface. Using an exit interface is optional, however it is necessary to use a next-hop address.
- It is recommended that when the exit interface is an Ethernet network, that the static route includes a next-hop address. You can also use a fully specified static route that includes both the exit interface and the next-hop address.

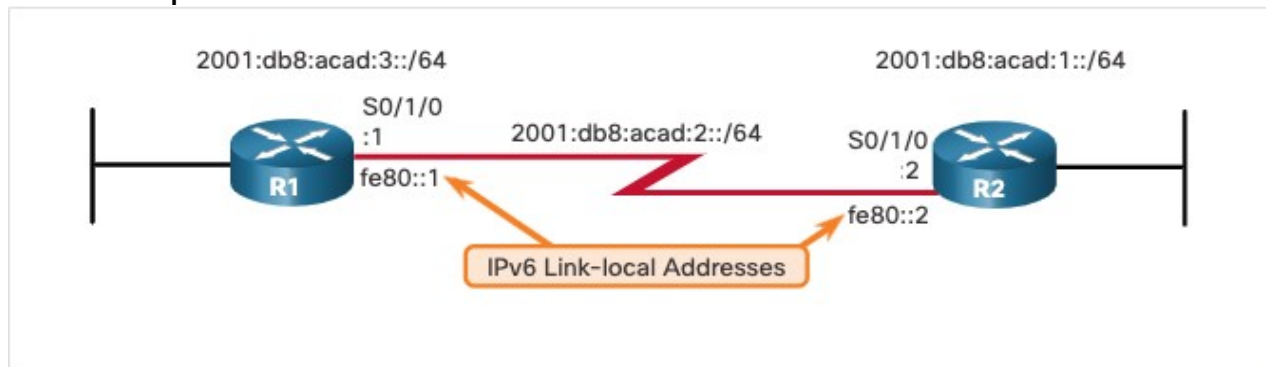
```
R1(config)# ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
```

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
C       172.16.2.0/24 is directly connected, GigabitEthernet0/0/1
L       172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S      192.168.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
S      192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
```

Configure IP Static Routes

IPv6 Fully Specified Static Route

In a fully specified static route, both the exit interface and the next-hop IPv6 address are specified. There is a situation in IPv6 when a fully specified static route must be used. **If the IPv6 static route uses an IPv6 link-local address as the next-hop address, use a fully specified static route.** The figure shows an example of a fully specified IPv6 static route using an IPv6 link-local address as the next-hop address.



```
R1(config)# ipv6 route 2001:db8:acad:1::/64 fe80::2
%Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2
```

```
R1# show ipv6 route static | begin 2001:db8:acad:1::/64
S    2001:DB8:ACAD:1::/64 [1/0]
    via FE80::2, Serial0/1/0
```

Configure IP Static Routes

Verify a Static Route

Along with **show ip route**, **show ipv6 route**, **ping** and **tracert**, other useful commands to verify static routes include the following:

- **show ip route static**
- **show ip route *network***
- **show running-config | section ip route**

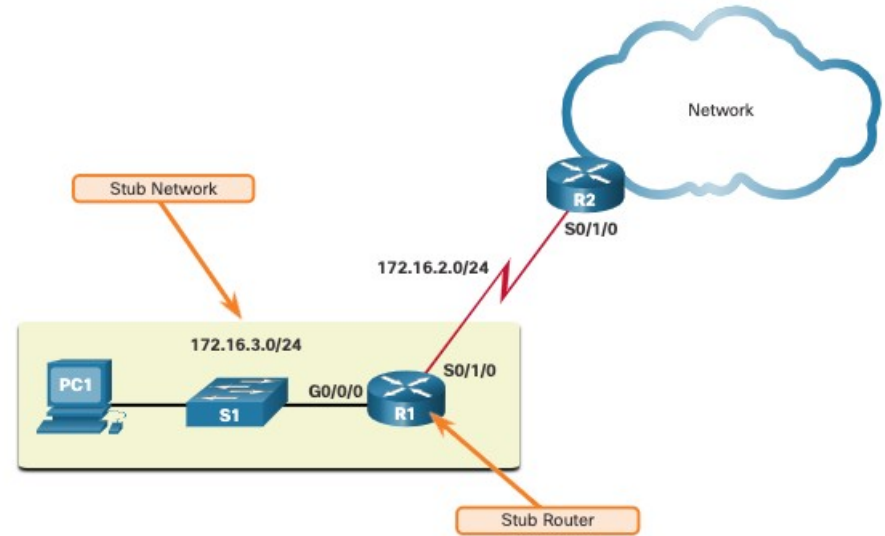
Replace **ip** with **ipv6** for the IPv6 versions of the command.

15.3 Configure IP Default Static Routes

Configure IP Default Static Routes

Default Static Route

- A default route is a static route that **matches all packets**. A single default route represents any network that is not in the routing table.
- Routers commonly use default routes that are either configured locally or learned from another router. The default route is used as the **Gateway of Last Resort**.
- Default static routes are **commonly used when connecting an edge router to a service provider network**, or a stub router (a router with only one upstream neighbor router).
- The figure shows a typical default static route scenario.



Configure IP Default Static Routes

Default Static Route (Cont.)

IPv4 Default Static Route: The command syntax for an IPv4 default static route is similar to any other IPv4 static route, except that the network address is **0.0.0.0** and the subnet mask is **0.0.0.0**. The 0.0.0.0 0.0.0.0 in the route will match any network address.

Note: An IPv4 default static route is commonly referred to as a quad-zero route.

The basic command syntax for an IPv4 default static route is as follows:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

IPv6 Default Static Route: The command syntax for an IPv6 default static route is similar to any other IPv6 static route, except that the ipv6-prefix/prefix-length is **::/0**, which matches all routes.

The basic command syntax for an IPv6 default static route is as follows:

```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```

Configure IP Default Static Routes

Verify a Default Static Route

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

```
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
```

The **show ip route static** command output from R1 displays the contents of the static routes in the routing table. Note the asterisk (*) next to the route with code 'S'. The asterisk indicates that this static route is a candidate default route, which is why it is selected as the Gateway of Last Resort.

```
R1# show ip route static
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
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
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
```

```
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 172.16.2.2
```

```
R1# show ipv6 route static
```

```
IPv6 Routing Table - default - 8 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
Ndr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
ld - LISP dyn-eid, la - LISP away, le - LISP extranet-policy
a - Application
S ::/0 [1/0]
via 2001:DB8:ACAD:2::2
```

15.4 Configure Floating Static Routes

Configure Floating Static Routes

Floating Static Routes

- Another type of static route is a floating static route. Floating static routes are static routes that are used to provide a **backup path to a primary static or dynamic route**. The floating static route is only used when the primary route is not available.
- To accomplish this, the floating static route is configured with a **higher administrative distance than the primary route**. The administrative distance represents the trustworthiness of a route. If multiple paths to the destination exist, the router will choose the path with the lowest administrative distance.
- By default, **static routes have an administrative distance of 1**, making them preferable to routes learned from dynamic routing protocols.
- The administrative distance of a static route can be increased to make the route **less desirable than that of another static route or a route learned through a dynamic routing** protocol. In this way, the static route “floats” and is not used when the route with the better administrative distance is active.

Configure IPv4 and IPv6 Floating Static Routes

The commands to configure default and floating IP default routes are as follows:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
R1(config)# ipv6 route ::/0 2001:db8:feed:10::2 5
```

The **show ip route** and **show ipv6 route** output verifies that the default routes to R2 are installed in the routing table. Note that the IPv4 **floating static route to R3 is not present in the routing table**.

```
R1# show ip route static | begin Gateway
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.2.2
R1# show ipv6 route static | begin S :
S    ::/0 [1/0]
      via 2001:DB8:ACAD:2::2
R1#
```

15.5 Configure Static Host Routes

Configure Static Host Routes

Host Routes

A host route is an **IPv4 address with a 32-bit mask, or an IPv6 address with a 128-bit mask**. The following shows the three ways a host route can be added to the routing table:

- Automatically installed when an IP address is configured on the router
- Configured as a static host route
- Host route automatically obtained through other methods (discussed in later courses)

Configure Static Host Routes

Automatically Installed Host Routes

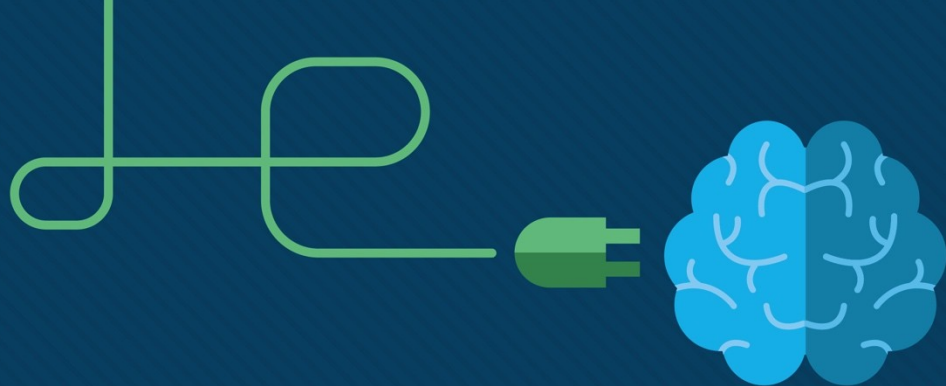
- Cisco IOS automatically installs a host route, also known as a local host route, when an interface address is configured on the router. A host route allows for a more efficient process for packets that are directed to the router itself, rather than for packet forwarding.
- This is in addition to the connected route, designated with a **C** in the routing table for the network address of the interface.
- The local routes are marked with **L** in the output of the routing table.

Configure Static Host Routes

Configure Static Host Routes

The example shows the IPv4 and IPv6 static host route configuration on the Branch router to access the server.

```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2  
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2  
Branch(config)# exit  
Branch#
```



Module 16: Troubleshoot Static and Default Routes

Switching, Routing and
Wireless Essentials v7.0
(SRWE)



Module Objectives

Module Title: Troubleshoot Static and Default Routes

Module Objective: Troubleshoot static and default route configurations.

Topic Title	Topic Objective
Packet Processing with Static Routes ✓	Explain how a router processes packets when a static route is configured.
Troubleshoot IPv4 Static and Default Route Configuration	Troubleshoot common static and default route configuration issues.

16.2 Troubleshoot IPv4 Static and Default Route Configuration

Troubleshoot IPv4 Static and Default Route Configuration

Network Changes

Networks fail for a number of reasons:

- An **interface can fail**
- **A service provider drops a connection**
- Links can become **oversaturated**
- An administrator may enter a **wrong configuration**.

Network administrators are responsible for pinpointing and **solving the problem**.

To efficiently find and solve these issues, it is advantageous to be intimately **familiar with tools** to help isolate routing problems quickly.

Troubleshoot IPv4 Static and Default Route Configuration

Common Troubleshooting Commands

Command	Description
ping	<ul style="list-style-type: none">• Verify Layer 3 connectivity to destination.• Extended pings provide additional options.
tracert	<ul style="list-style-type: none">• Verify path to destination network.• It uses ICMP echo reply messages to determine the hops to the destination.
show ip route	<ul style="list-style-type: none">• Displays the routing table.• Used to verify route entries for destination IP addresses.
show ip interface brief	<ul style="list-style-type: none">• Displays the status of device interfaces.• Used to verify the operational status and IP address of an interface.
show cdp neighbors	<ul style="list-style-type: none">• Displays a list of directly connected Cisco devices.• Also used to validate Layer 1 and 2 connectivity.

