IP protocol & IP addressing

Lecture 3.3

Module 3. Networking Fundamentals

Serhii Zakharchenko

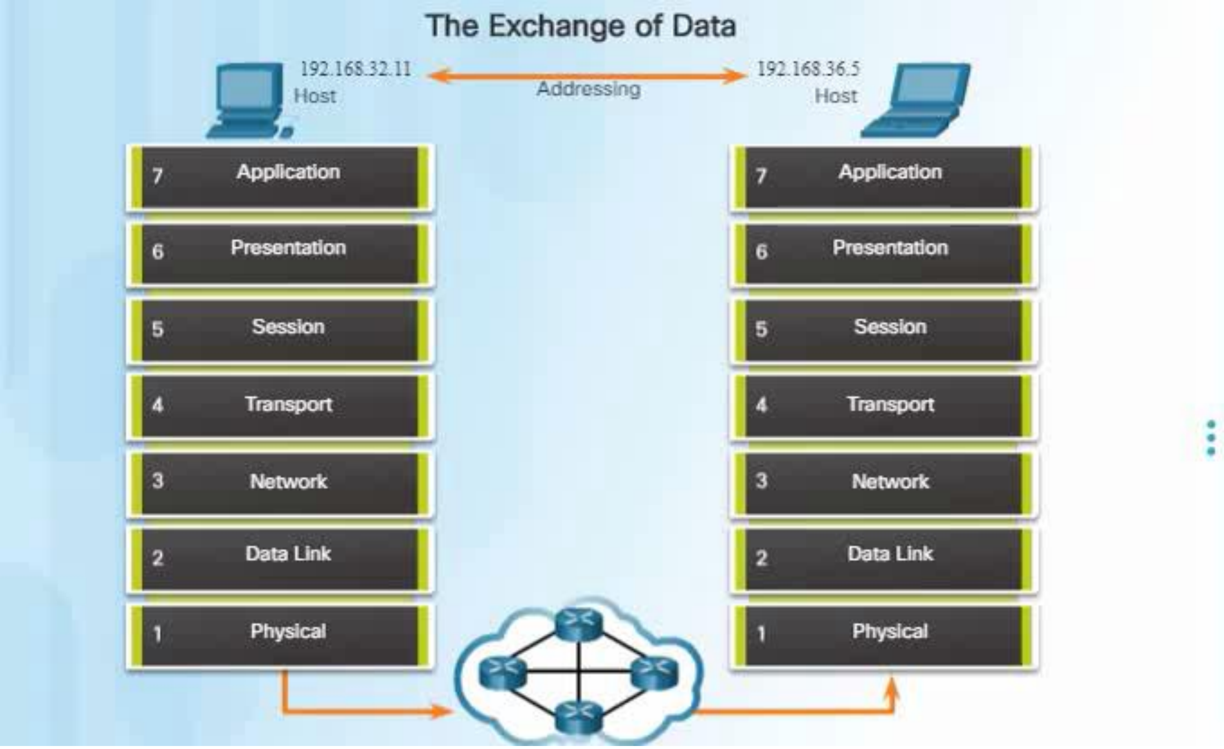
Agenda

- Internet Protocol
- IPv4 address subnetting
- IP routing
- Q&A

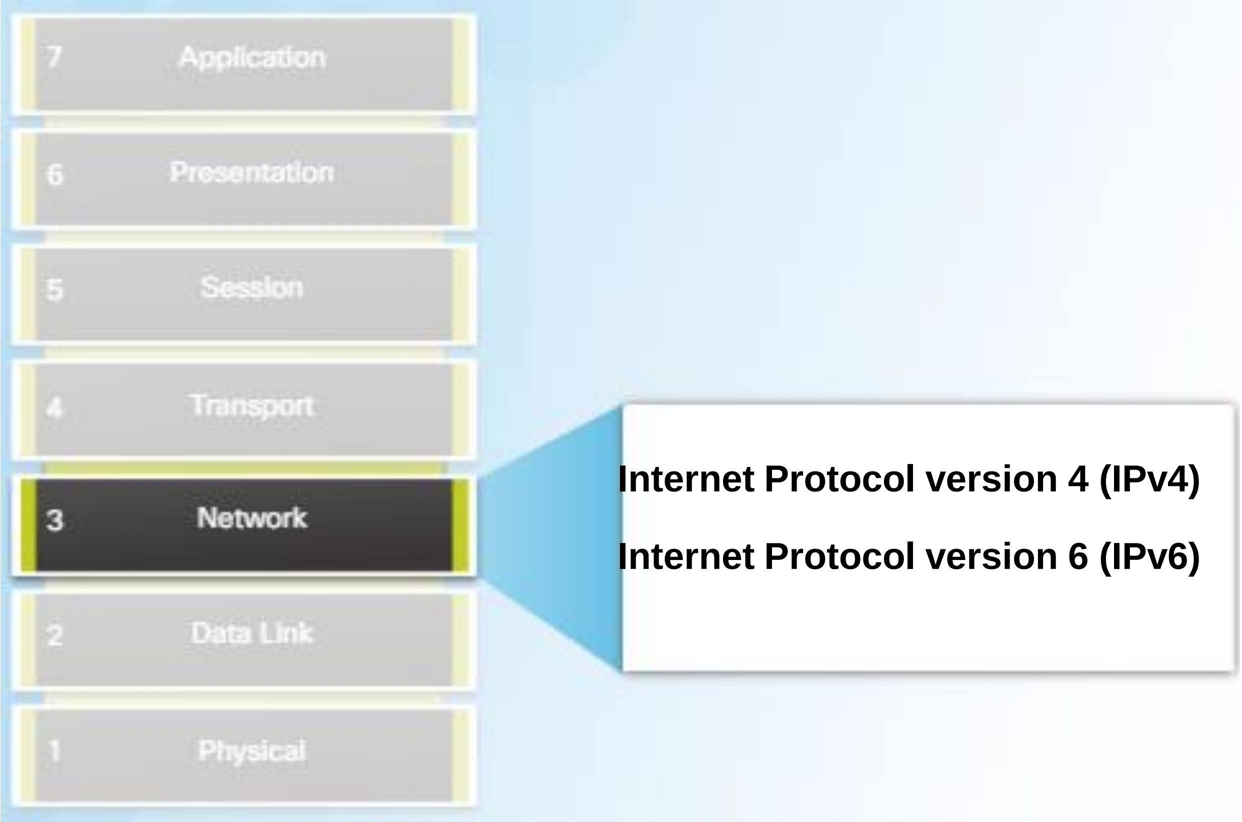
Internet Protocol

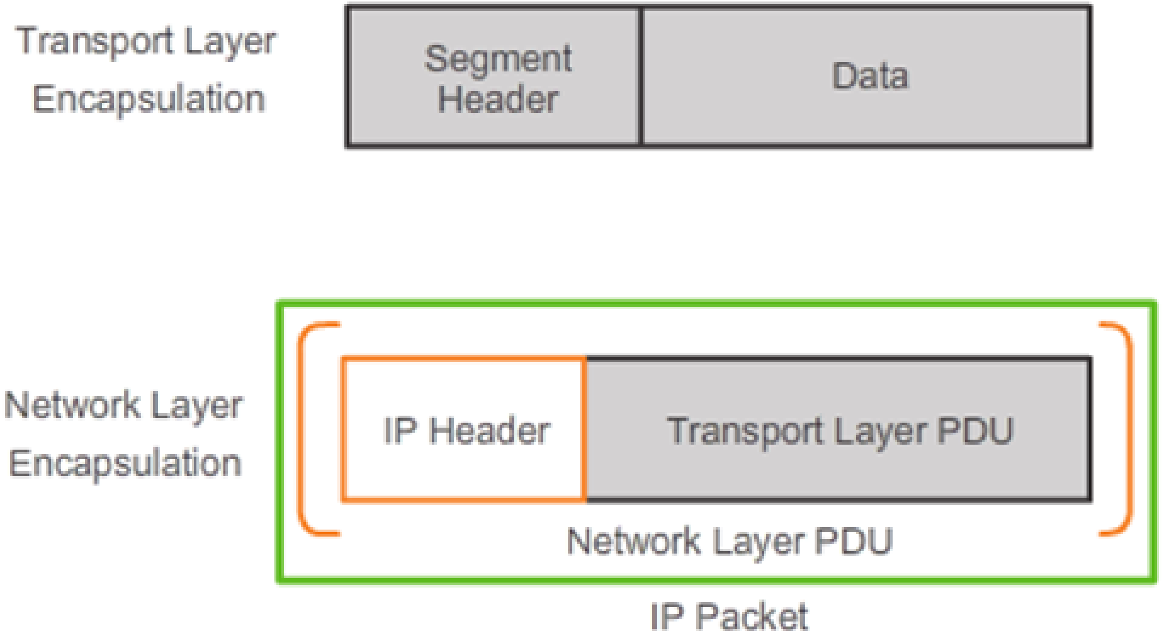
The Network Layer basic processes

- **Addressing end devices** - end devices must be configured with a unique IP address for identification on the network.
- **Encapsulation** - The network layer receives a protocol data unit (PDU) from the transport layer. In a process called encapsulation, the network layer adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts.
- **Routing** - The role of the router is to select paths for and direct packets toward the destination host in a process known as routing.
- **De-encapsulating** - If the destination IP address within the header matches host IP address, the IP header is removed from the packet. This process is known as de-encapsulation



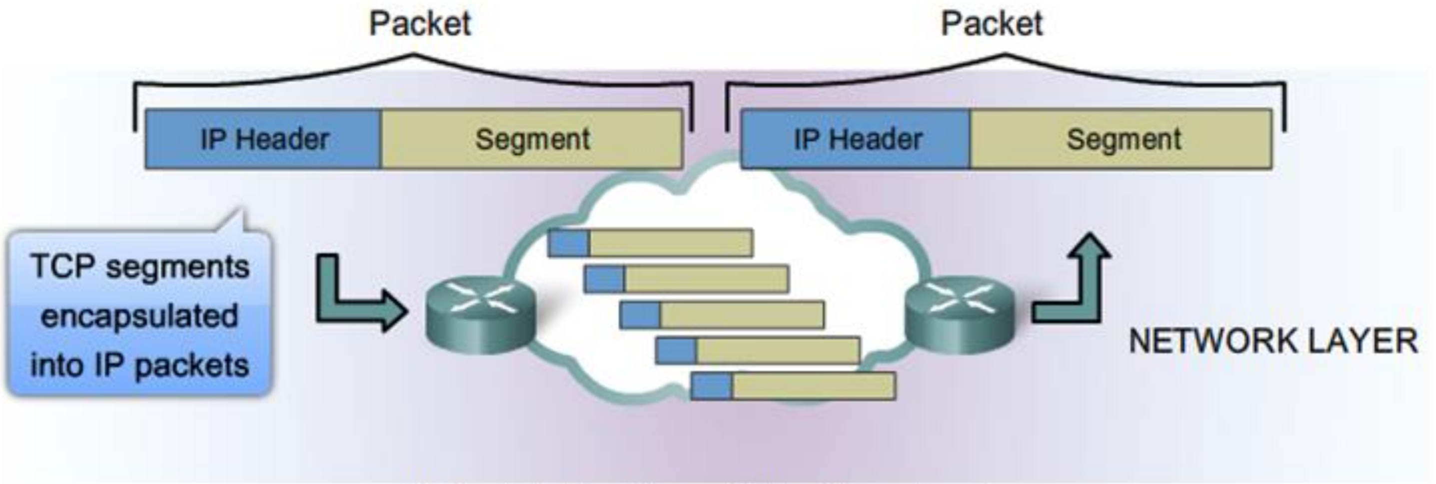
Network Layer Protocols





Characteristics of IP

- IP was designed as a protocol with **low overhead**. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.
- The basic characteristics of IP are:
  - **Connectionless -** No connection with the destination is established before sending data packets.
  - **Best Effort (unreliable) -** Packet delivery is not guaranteed.
  - **Media Independent -** Operation is independent of the medium carrying the data.



IP Packets flow through the internetwork.

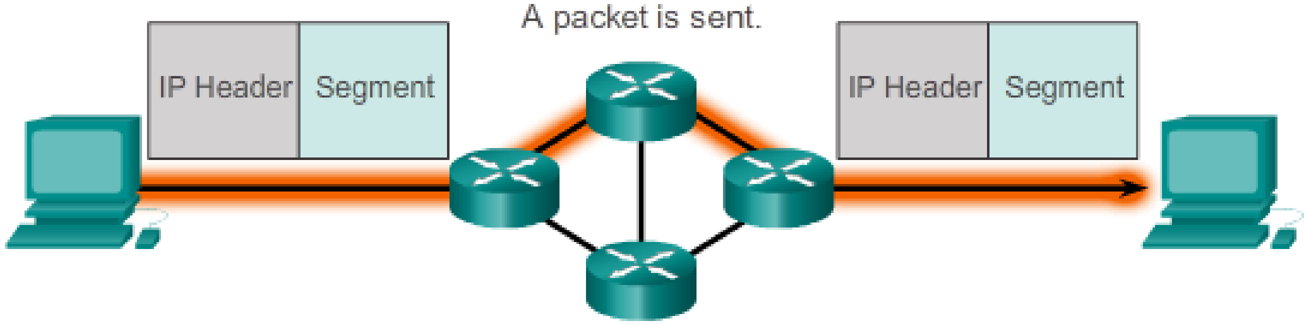
IP - Connectionless

The sender doesn't know:

- If the receiver is present
- If the letter arrived
- If the receiver can read the letter

The receiver doesn't know:

- When it is coming



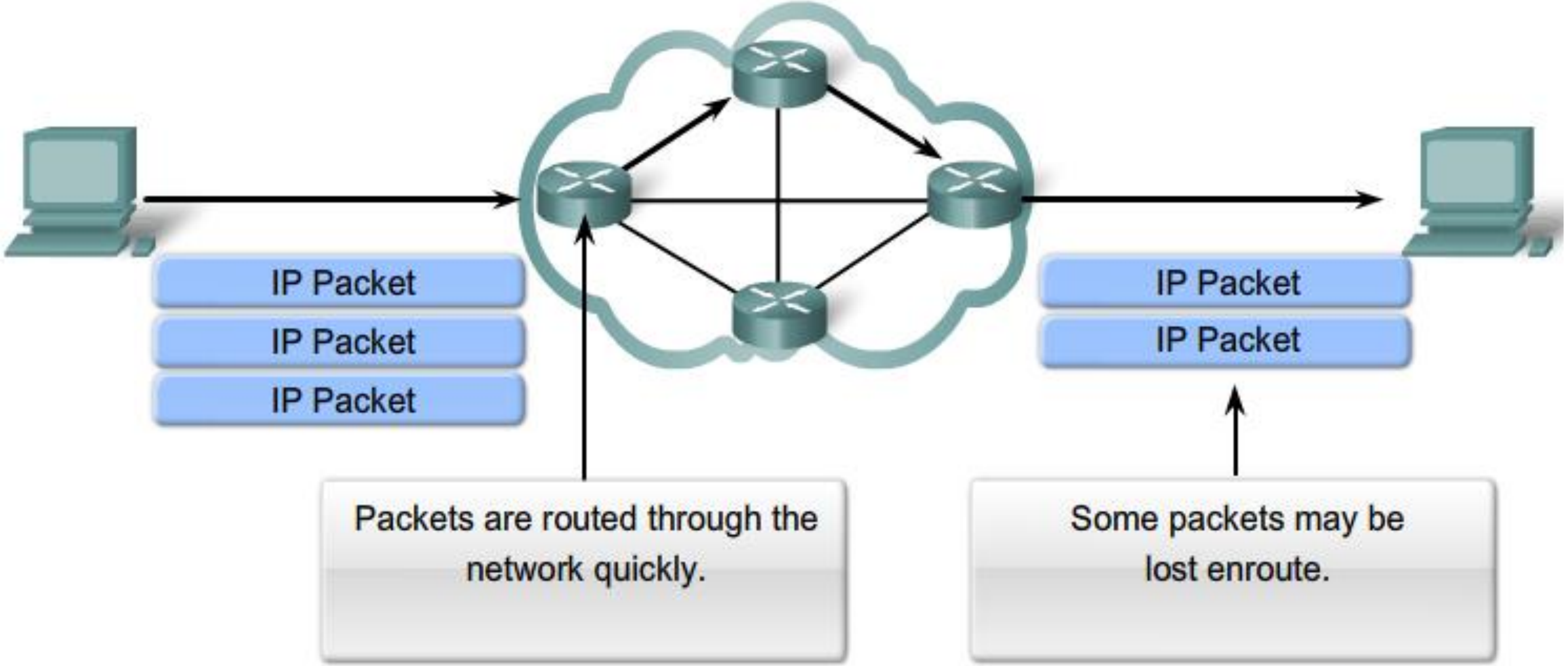
The sender doesn't know:

- If the packet arrived
- If the receiver can read the packet

The receiver doesn't know:

- When it is coming

IP – Best Effort Delivery

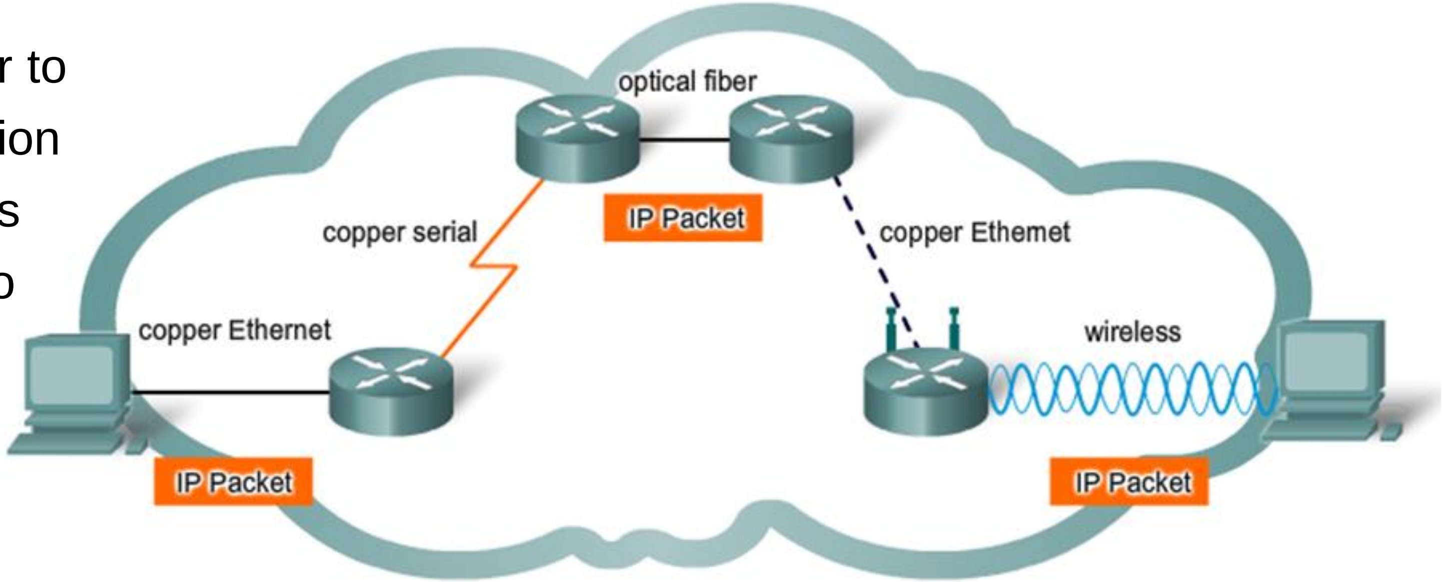


As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Other protocols manage the process of tracking packets and ensuring their delivery.

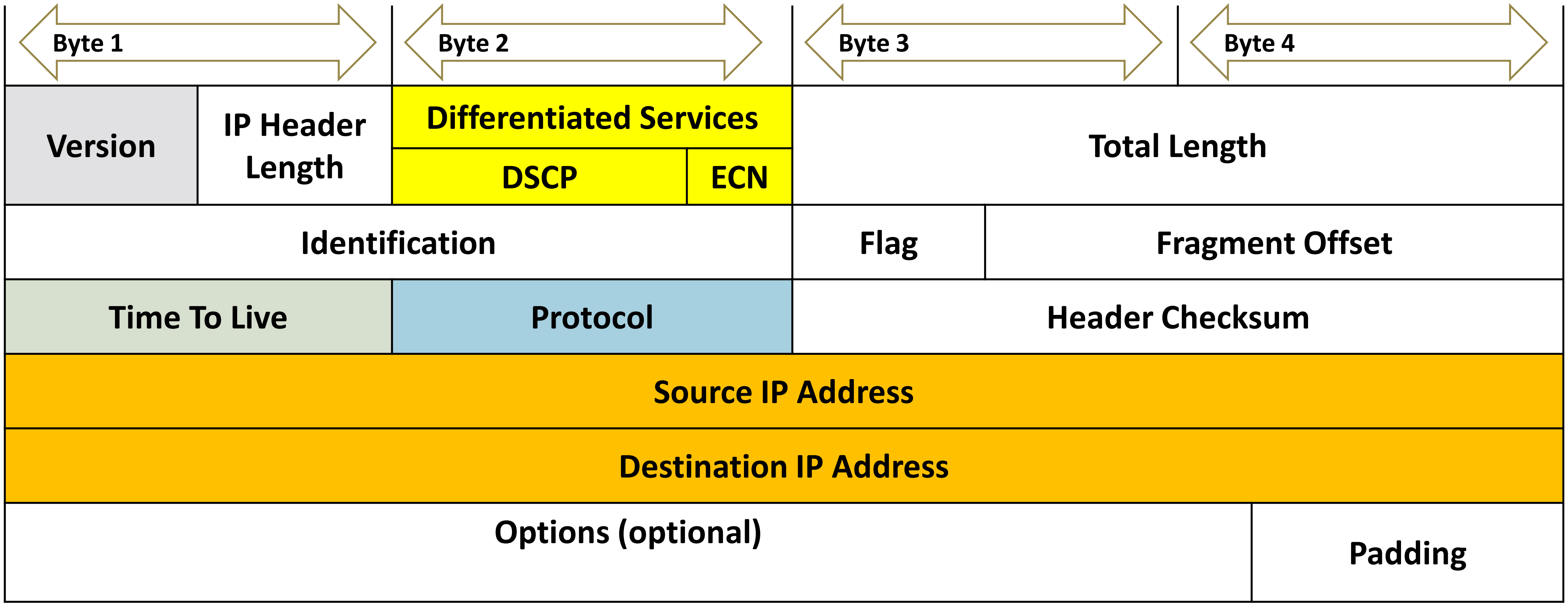
IP – Media Independent

It is the responsibility of the OSI data link layer to take an IP packet and prepare it for transmission over the communications medium. This means that the transport of IP packets is not limited to any particular medium.

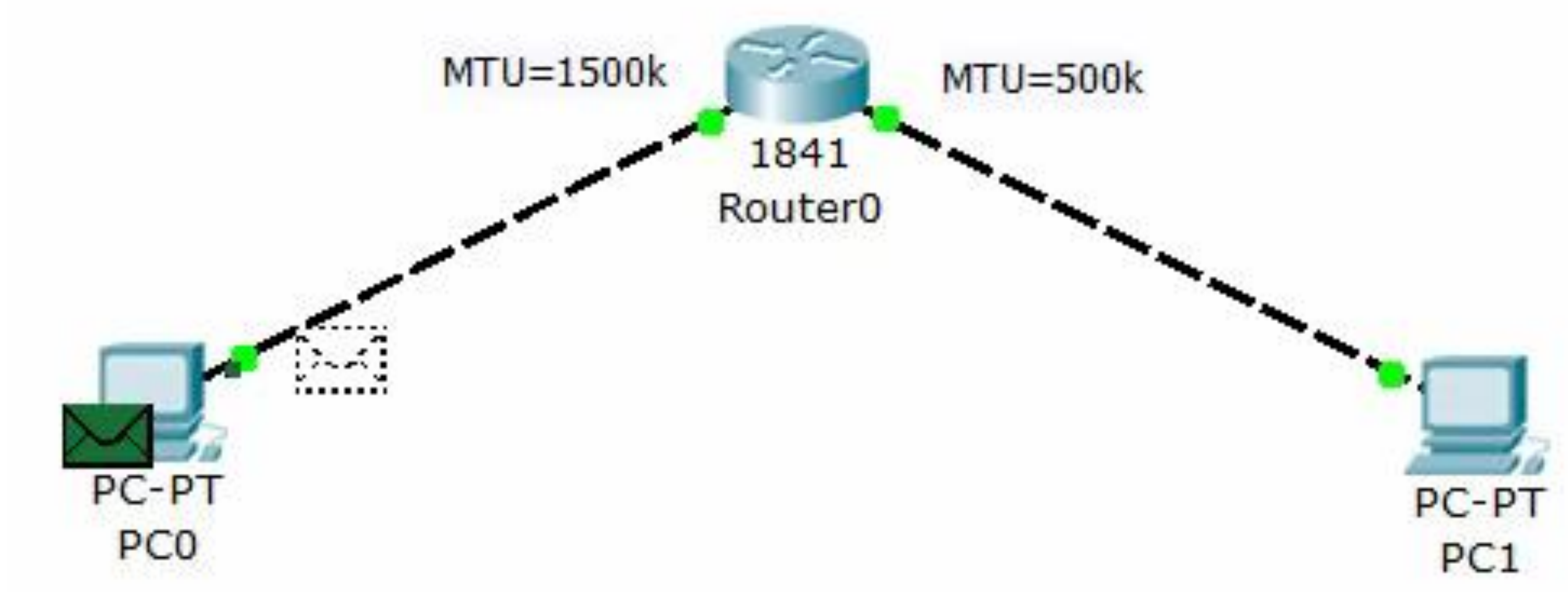


- There is, however, one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the **maximum transmission unit** (MTU). The data link layer passes the MTU value up to the network layer. The network layer then determines how large packets should be.
- In some cases, an intermediate device, usually a router, must split up a packet when forwarding it from one medium to a medium with a smaller MTU. This process is called fragmenting the packet or **fragmentation**.

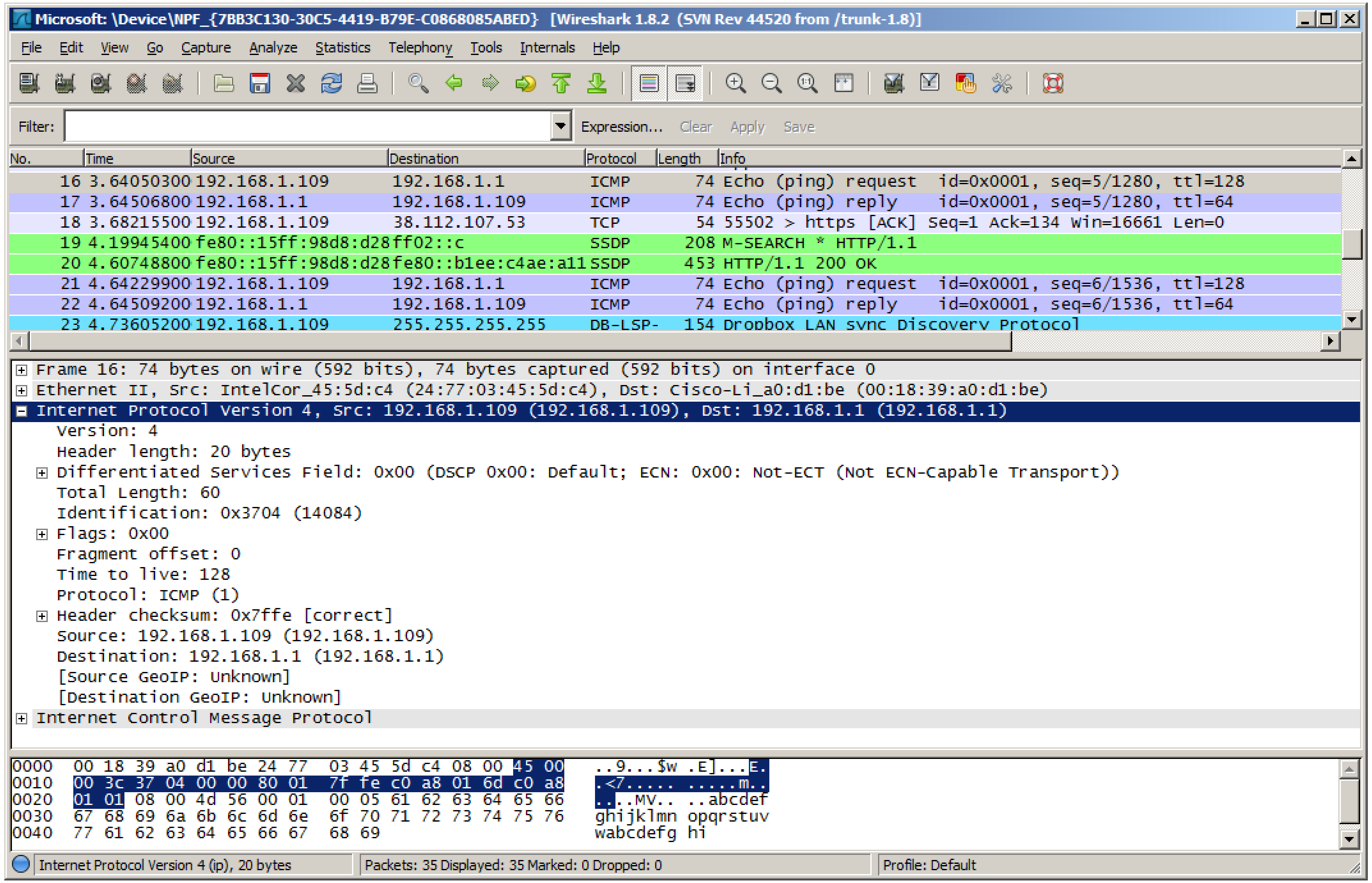
IPv4 Packet Header



IPv4 Packet Fragmentation



Sample IPv4 Headers



Network Troubleshooting utilities (ICMP Ping)

- The ICMP echo request and the ICMP echo reply messages are commonly known as ping messages.
- Ping is a troubleshooting tool used by system administrators to manually test for connectivity between network devices, and also to test for network delay and packet loss.
- The ping command sends an ICMP echo request to a device on the network, and the device immediately responds with an ICMP echo reply.

```
C:\Users\Сер3а>ping 8.8.8.8

Обмен пакетами с 8.8.8.8 по с 32 байтами данных:
Ответ от 8.8.8.8: число байт=32 время=22мс TTL=118
Ответ от 8.8.8.8: число байт=32 время=19мс TTL=118
Ответ от 8.8.8.8: число байт=32 время=21мс TTL=118
Ответ от 8.8.8.8: число байт=32 время=22мс TTL=118

Статистика Ping для 8.8.8.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 19мсек, Максимальное = 22 мсек, Среднее = 21 мсек
```

Network Troubleshooting utilities (Traceroute)

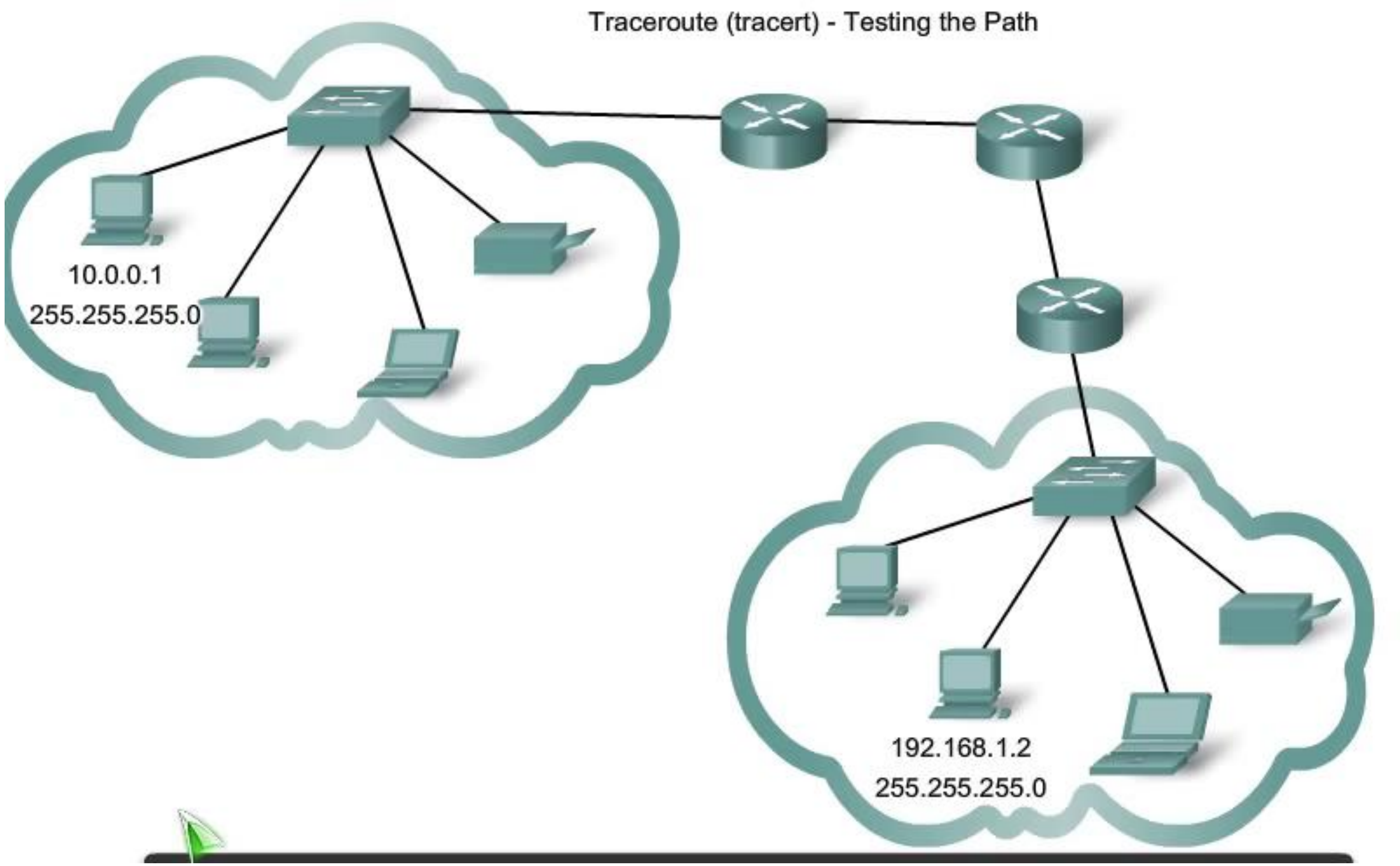
- **Traceroute**, also called tracert, is a utility that uses ICMP packets to record the route through the internet from one computer to another.
- It calculates the time taken for each hop as the packet is routed to the destination.
- To guarantee accuracy, each hop is queried multiple times (in this case three times) to better measure the response of that particular hop.

```
C:\Users\Сер3а>tracert 8.8.8.8

Трассировка маршрута к dns.google [8.8.8.8]
с максимальным числом прыжков 30:

  1     8 ms     1 ms     1 ms  192.168.1.1
  2     2 ms     1 ms     1 ms  10.128.16.1
  3    18 ms    21 ms    20 ms  vl-21.sw-vn-1-1.enet.vn.ua [217.30.200.62]
  4     4 ms     2 ms     2 ms  et-0-0-0.boar.enet.vn.ua [217.30.200.189]
  5     8 ms     6 ms     7 ms  vl-32.sw-kyiv-nt-1.enet.vn.ua [217.30.200.218]
  6     6 ms     8 ms     6 ms  google-gw.ix.net.ua [185.1.50.166]
  7    32 ms     7 ms     9 ms  108.170.248.155
  8    20 ms    20 ms    19 ms  142.251.67.218
  9    19 ms    27 ms    29 ms  142.251.77.181
 10    20 ms    27 ms    22 ms  74.125.242.241
 11    22 ms    18 ms    19 ms  142.251.65.227
 12    23 ms    19 ms    26 ms  dns.google [8.8.8.8]
```

Traceroute deep look



Limitations of IPv4

- **IP Address depletion** - IPv4 has a limited number of unique public IP addresses available.
- **Internet routing table expansion** - A routing table is used by routers to make best path determinations. These IPv4 routes consume a great deal of memory and processor resources on Internet routers.
- **Lack of end-to-end connectivity** - Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IP address. However, because the public IP address is shared, the IP address of an internal network host is hidden. This can be problematic for technologies that require end-to-end connectivity.

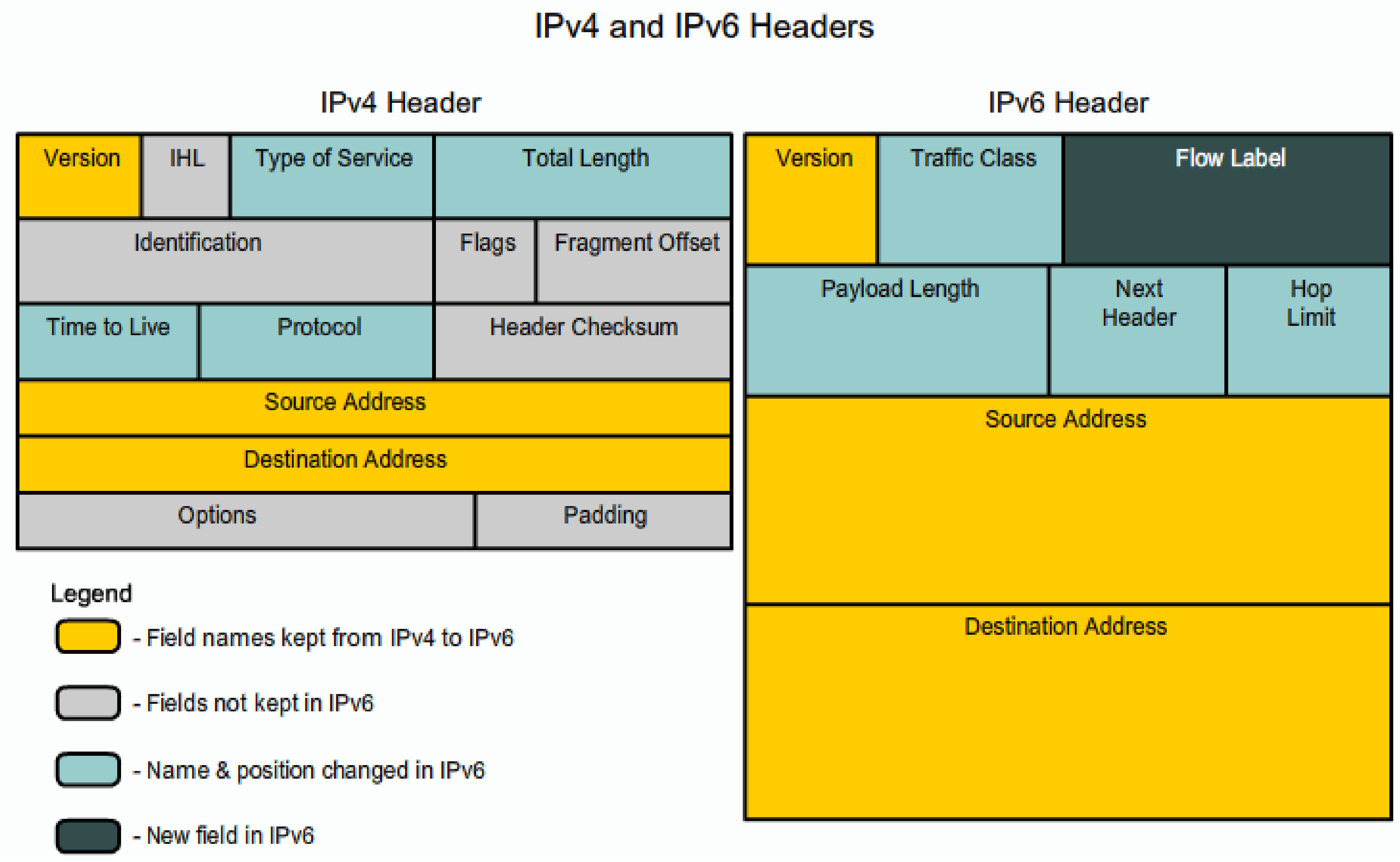
Introducing IPv6

- **Increased address space**:
  - **4 billion** IPv4 addresses - **4,000,000,000**;
  - **340 undecillion** IPv6 addresses **340,000,000,000,000,000,000,000,000,000,000,000,000**
- **Improved packet handling** - The IPv6 header has been simplified with fewer fields.
- **Eliminates the need for NAT** - With such a large number of public IPv6 addresses, Network Address Translation (NAT) is not needed. This avoids some of the NAT-induced application problems experienced by applications requiring end-to-end connectivity.
- Ipv6 popularity

Encapsulating IPv6

The IPv6 simplified header offers several advantages over IPv4:

- Better routing efficiency for performance and forwarding-rate scalability
- No requirement for processing checksums
- Simplified and more efficient extension header mechanisms (as opposed to the IPv4 Options field)
- A Flow Label field for per-flow processing with no need to open the transport inner packet to identify the various traffic flows

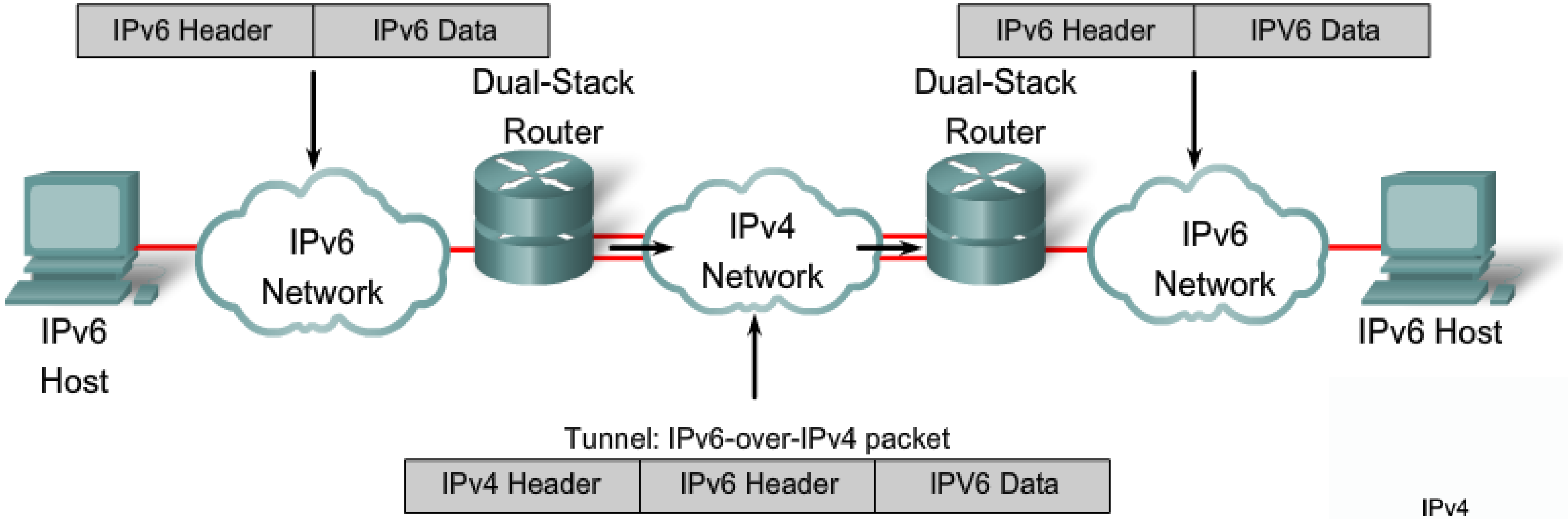


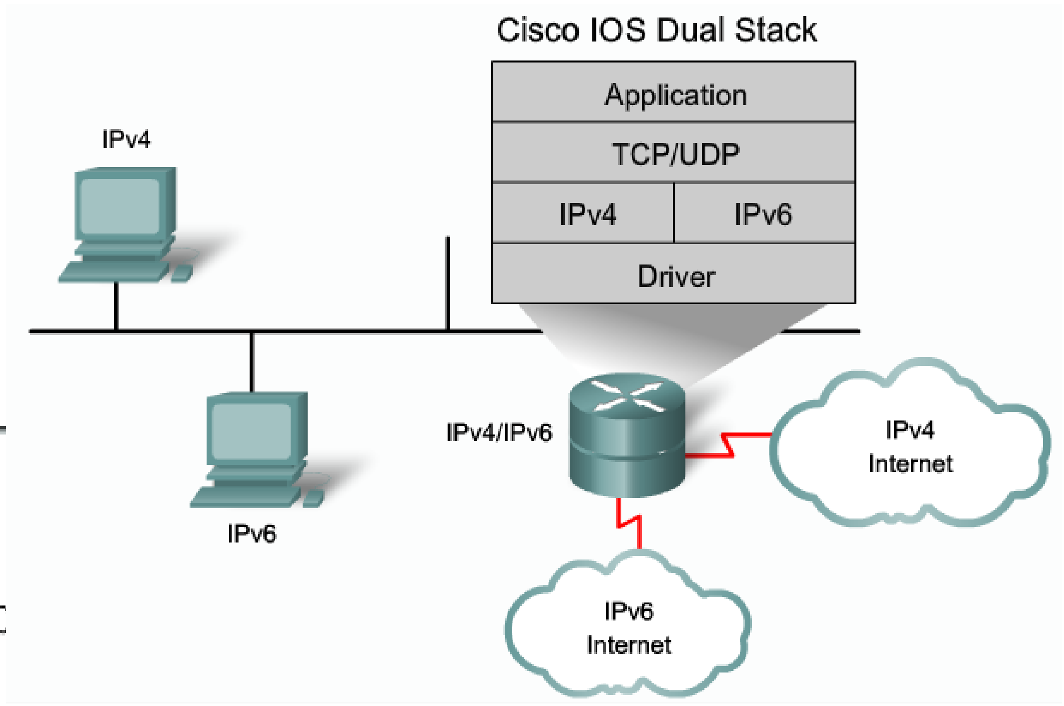
IPv6 extension header mechanisms

IPv6 Header Next Header - Routing	Header Routing Next Header - Fragment	Header Fragment Next Header - TCP (UDP) Header	Header TCP (UDP)	Data

Next Header title	Next Header field value
Hop-by-Hop	**0**
Routing	**43**
Fragmentation	**44**
Encapsulating Security Paiload (ESP)	**50**
Autentication Header (AH)	**51**

IPv4 and IPv6 Coexistence

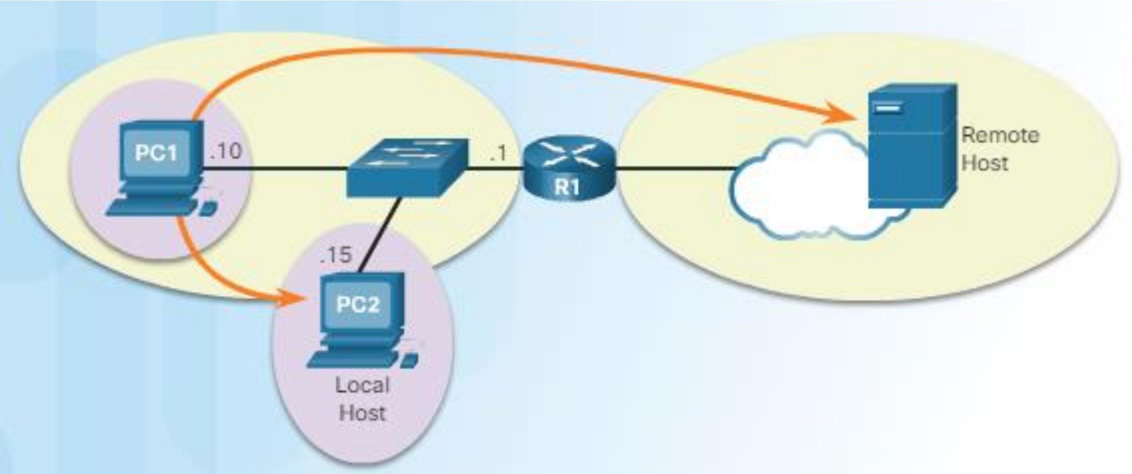





```
conf t
ipv6 unicast-routing

interface ethernet0
  ip address 192.168.99.1 255.255.255.0
  ipv6 address 3ffe:b00:c18:1::3/127
```

Host Forwarding Decision



A host can send a packet to:

- **Itself** - This is a special IP address of 127.0.0.1 which is referred to as the loopback interface. This loopback address is automatically assigned to a host when TCP/IP is running. The ability for a host to send a packet to itself using network functionality is useful for testing purposes. Any IP within the network 127.0.0.0/8 refers to the local host.
- **Local host** - This is a host on the same network as the sending host. The hosts share the same network address.
- **Remote host** - This is a host on a remote network. The hosts do not share the same network address

Host Routing Tables

The local table of the host typically contains :

- **Direct connection** - This is a route to the loopback interface (127.0.0.1).
- **Local network route** - The network which the host is connected to is automatically populated in the host routing table.
- **Local default route** - The default route represents the route that packets must take to reach all remote network addresses. The default route is created when a default gateway address is present on the host. The default gateway address is the IP address of the network interface of the router that is connected to the local network.

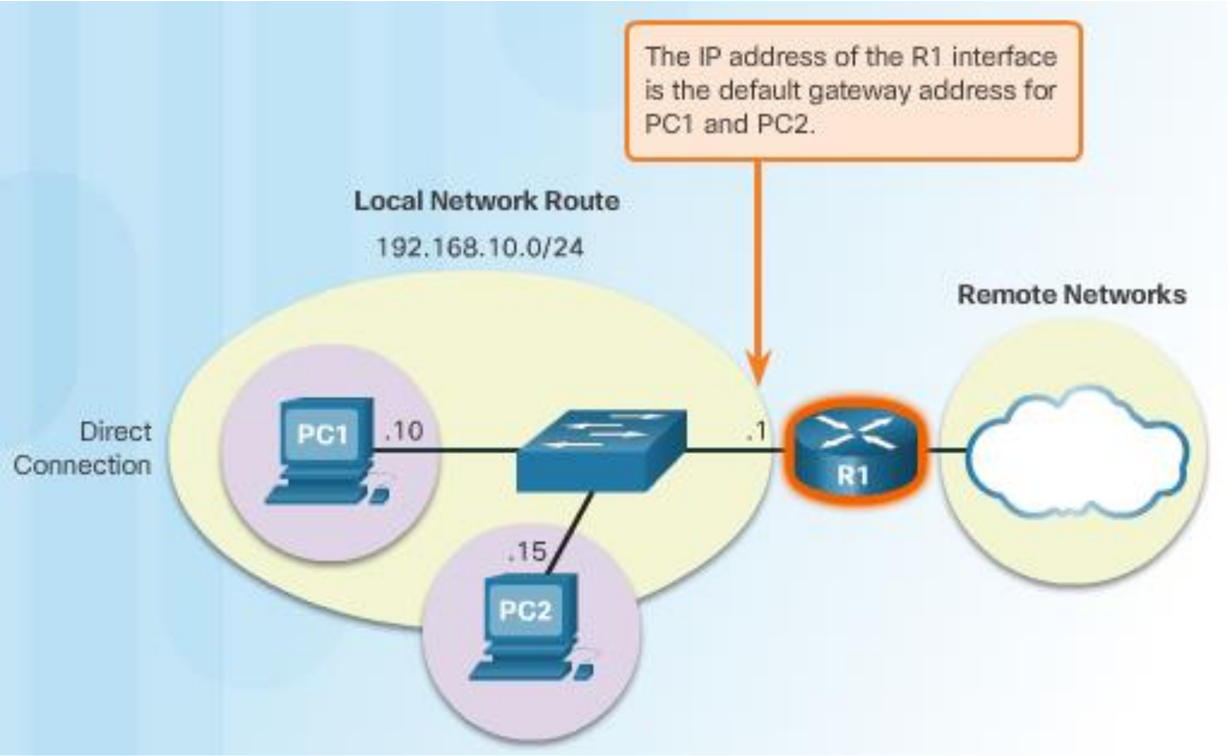
route print

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.103	40
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
192.168.1.0	255.255.255.0	On-link	192.168.1.103	296
192.168.1.103	255.255.255.255	On-link	192.168.1.103	296
192.168.1.255	255.255.255.255	On-link	192.168.1.103	296
192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	On-link	192.168.56.1	281
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	192.168.56.1	281
224.0.0.0	240.0.0.0	On-link	192.168.1.103	296
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
255.255.255.255	255.255.255.255	On-link	192.168.1.103	296

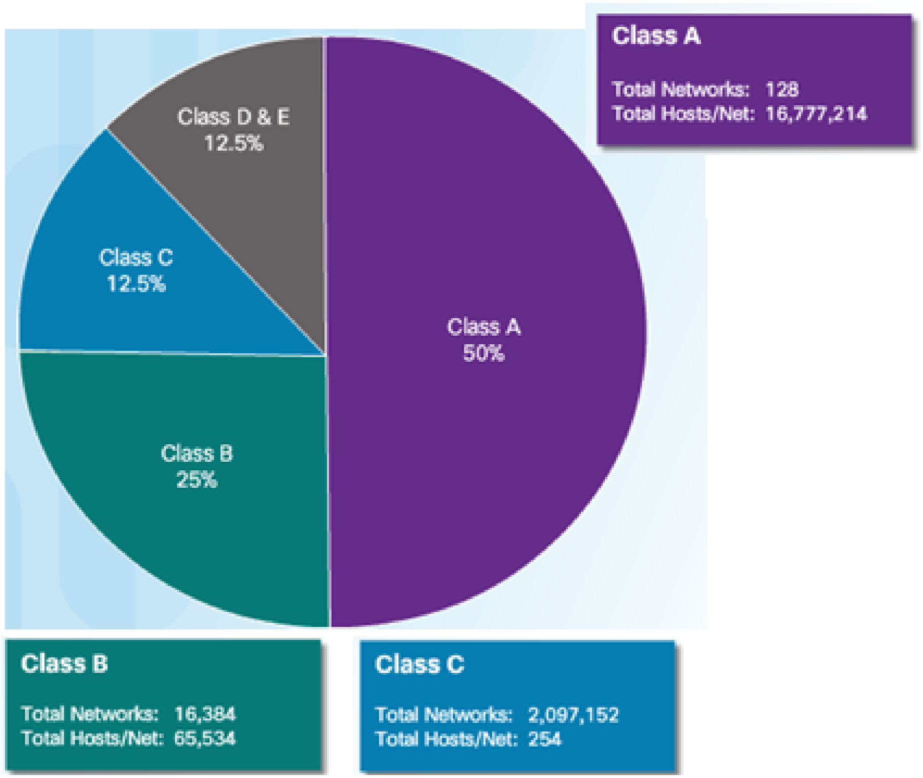
Default Gateway

- The default gateway is the network device that can route traffic to other networks. It is the router that can route traffic out of the local network.
- If you use the analogy that a network is like a room, then the default gateway is like a doorway. If you want to get to another room or network, you need to find the doorway.
- Alternatively, a PC or computer that does not know the IP address of the default gateway is like a person, in a room, that does not know where the doorway is.



Legacy Classful Addressing

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

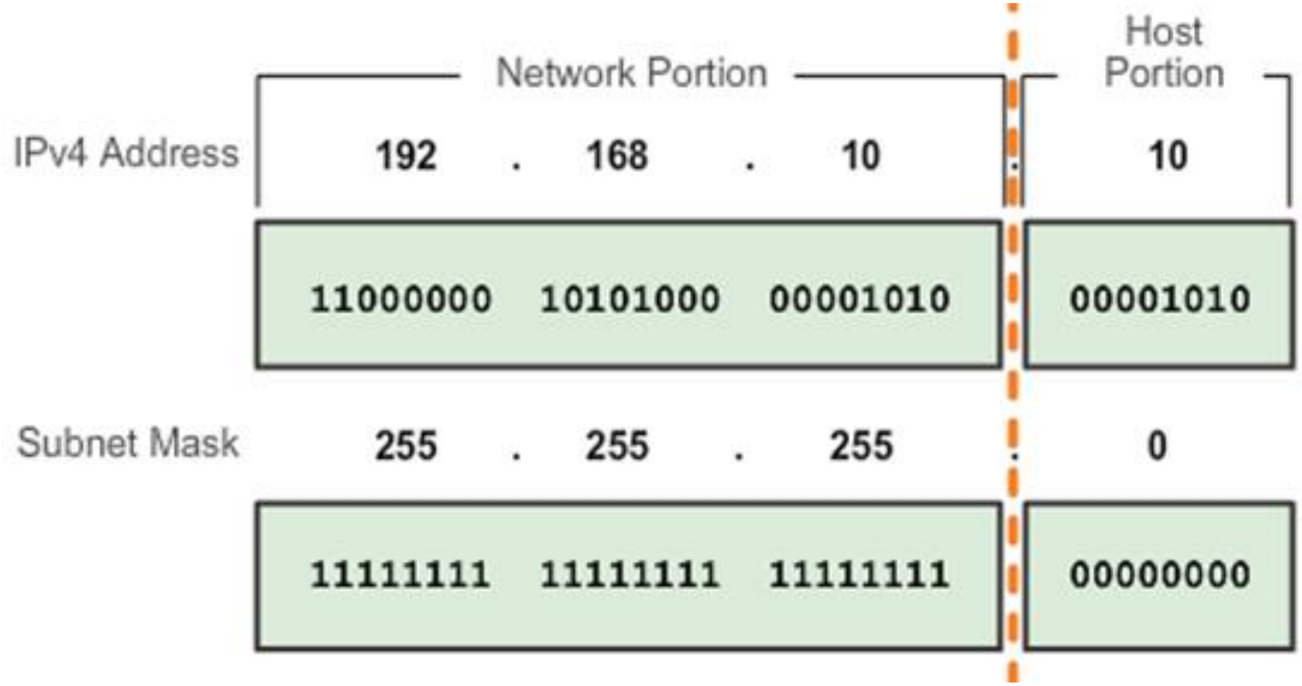


Класс A	0	7-разрядный адрес сети	24-разрядный адрес интерфейса
Класс B	10	14-разрядный адрес сети	16-разрядный адрес интерфейса
Класс C	110	21-разрядный адрес сети	8-разрядный адрес интерфейса
Класс D	1110	Адрес многоадресной рассылки	
Класс E	1111	Зарезервировано	

Classless Addressing

- The system in use today is referred to as **classless addressing**. The formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”).
- In 1993, the IETF created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address.
- The IETF knew that CIDR was only a temporary solution and that a new IP protocol would have to be developed to accommodate the rapid growth in the number of Internet users. In 1994, the IETF began its work to find a successor to IPv4, which eventually became IPv6.

Network Portion and Host Portion of an IPv4 Address



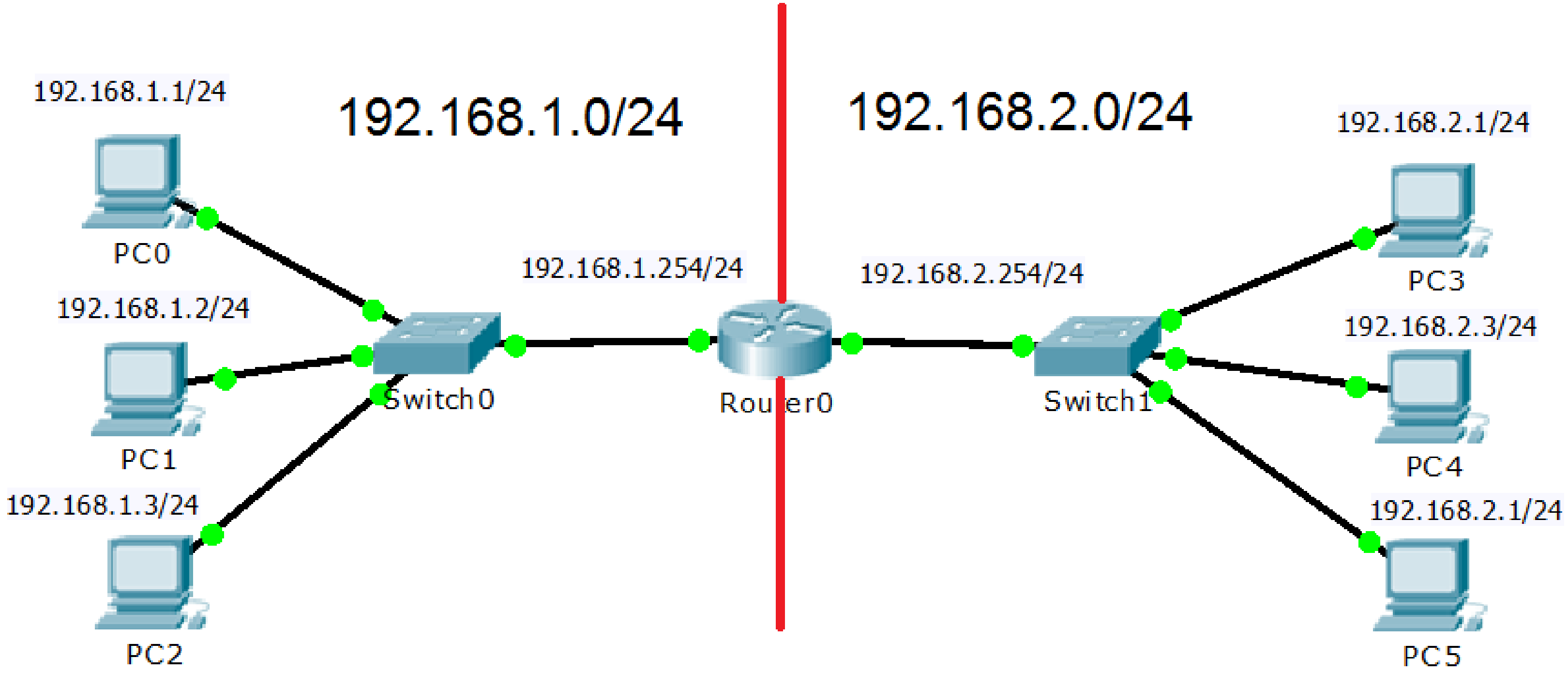
Valid Subnet Masks

Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

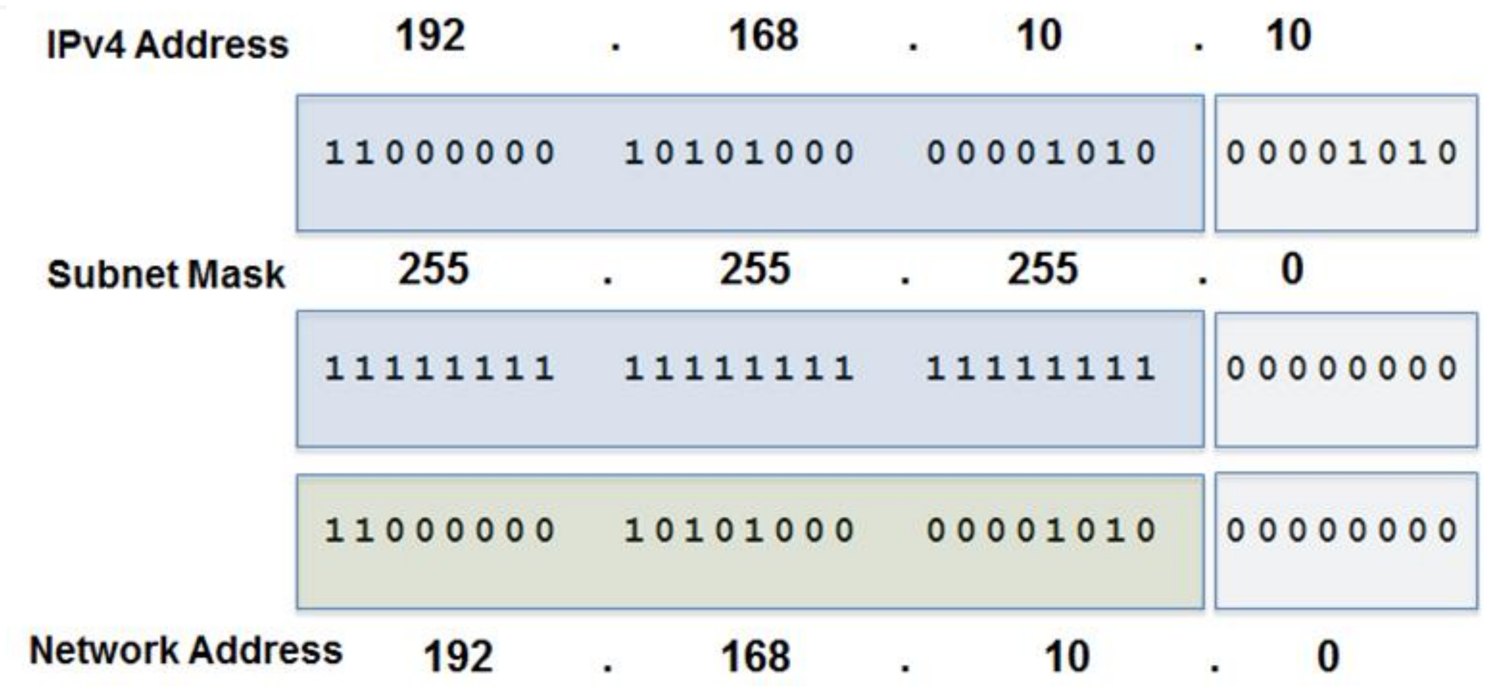
- To define the network and host portions of an address, a devices use a separate 32-bit pattern called a **subnet mask**
- The subnet mask signifies which part of the IP address is network and which part is host.

IP-address requirement

- The bits within the network portion of the address must be **identical** for all devices that reside in the same network.
- The bits within the host portion of the address must be **unique** to identify a specific host within a network.



Bitwise AND Operation



1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

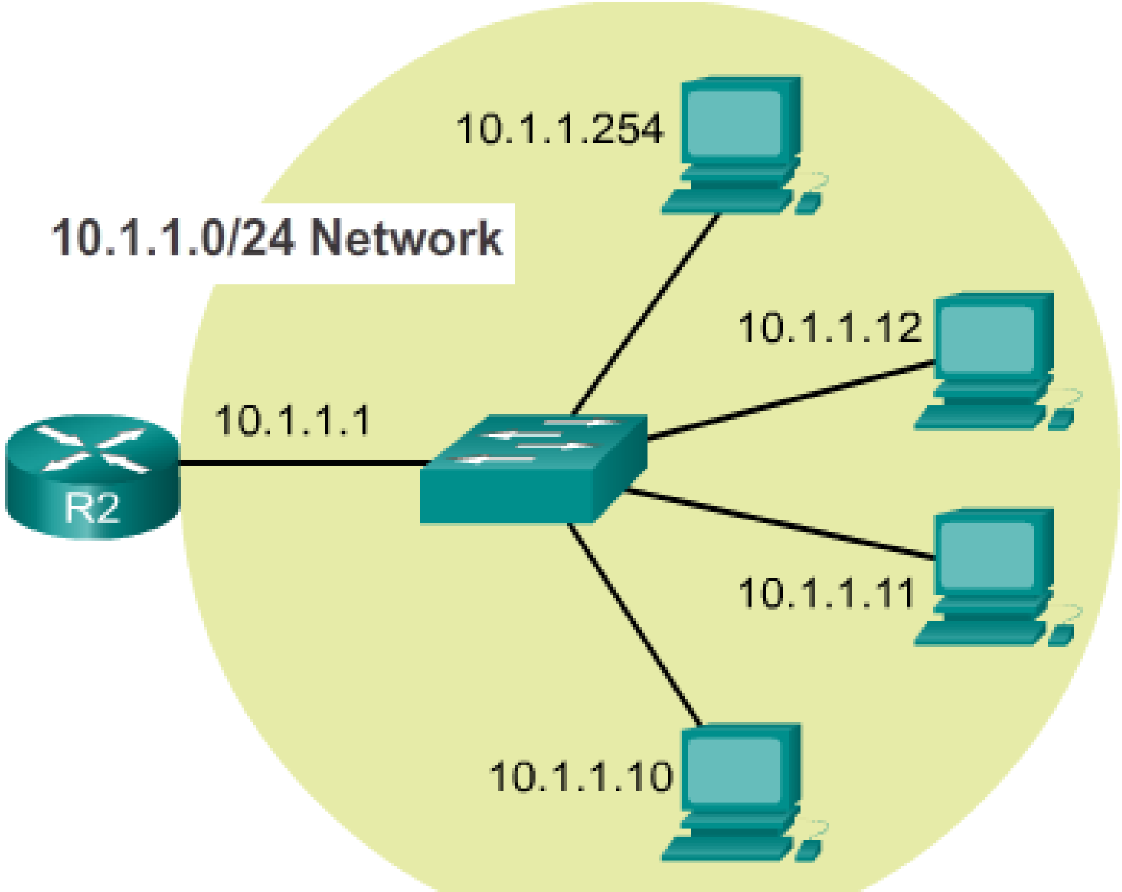
Host address	10111000 184	00100011 35	01001000 64+8=72	01011111 95
Subnet mask	11111111 255	11111111 255	11110000 240	00000000 0
Network address	10111000 184	00100011 35	01000000 64	00000000 0

Network Prefixes

- The prefix length is another way of expressing the subnet mask.
- The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, a “/” followed by the number of bits set to 1.
- For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24.
    - subnet mask : **255.255.0.0** prefix length : **16**
    - subnet mask : **255.255.240.0** prefix length : **20**

The types of addresses within the address range

- **Network address** - has a 0 for each host bit in the host portion of the address. Example: **10.1.1.0/24**
- **Host addresses** - has any combination of 0 and 1 bits in the host portion of the address but cannot contain all 0 bits or all 1 bits. Example: **10.1.1.10/24**
- **Broadcast address** - This is the address in which the bits in the host portion are all 1s. Example: **10.1.1.255/24**



AWS VPC specific addresses

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following **five** IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is in the primary CIDR.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC; therefore, we reserve this address.

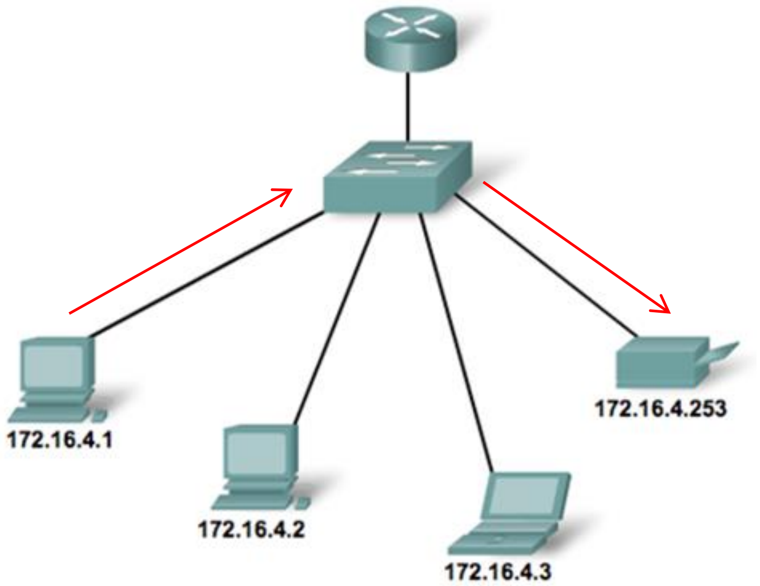
IPv4 Network, Host, and Broadcast Address samples

Network Address	10.1.1.0/24	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: 2^8 – 2 = 254 hosts		

Network Address	10.1.1.0/25	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: 2^7 – 2 = 126 hosts		

IPv4 Unicast, Broadcast, and Multicast

Unicast - the process of sending a packet from one host to an individual .

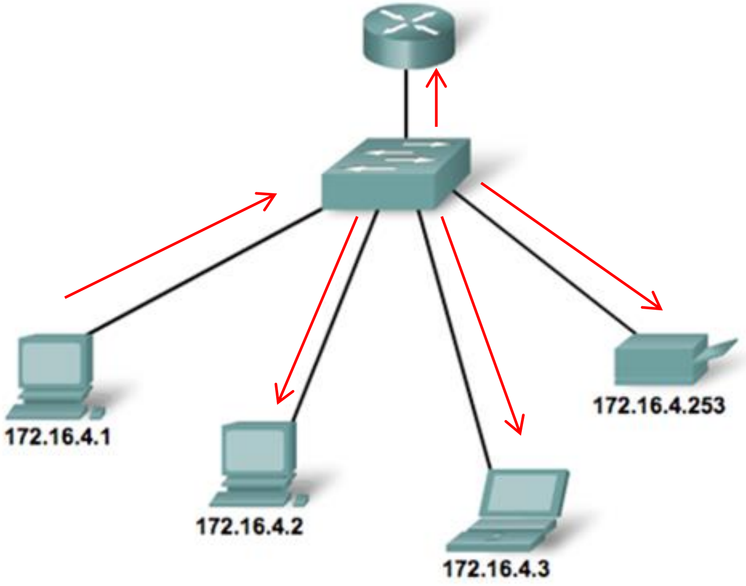


Multicast - the process of sending a packet from one host to a selected group of hosts, possibly in different networks

- Reduces traffic
- Reserved for addressing multicast groups - 224.0.0.0 to 239.255.255.255.
- Link local - 224.0.0.0 to 224.0.0.255 (Example: routing information exchanged by routing protocols)
- Globally scoped addresses - 224.0.1.0 to 238.255.255.255 (Example: 224.0.1.1 has been reserved for Network Time Protocol)

Broadcast - the process of sending a packet from one host to all hosts in the network

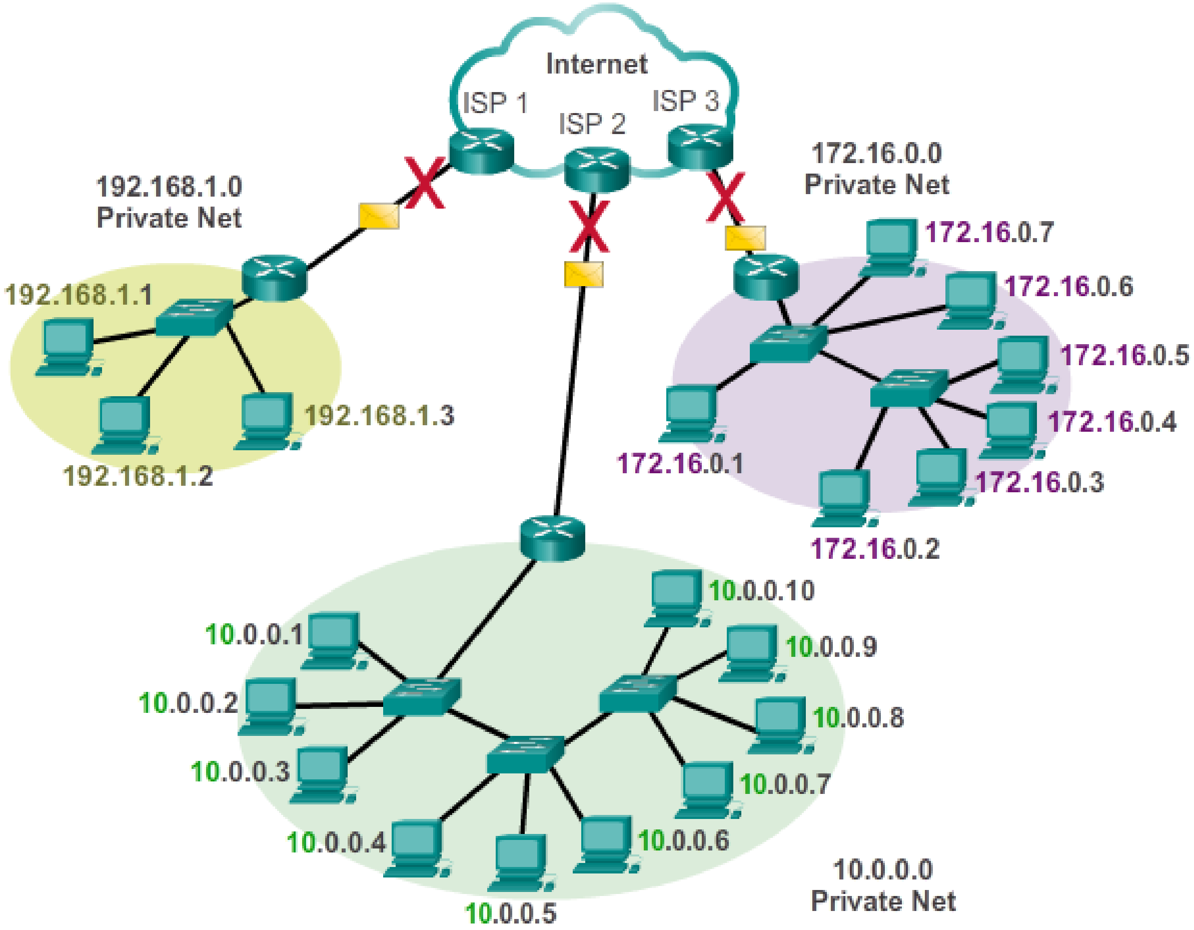
- Directed broadcast Destination **172.16.4.255**
- Limited broadcast Destination **255.255.255.255**
- Routers do not forward a limited broadcast!



Public and Private IPv4 Addresses

Private address blocks are:

- 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)



Assignment of Public IP Addresses
Regional Internet Registries (RIRs)

Special Use IPv4 Addresses

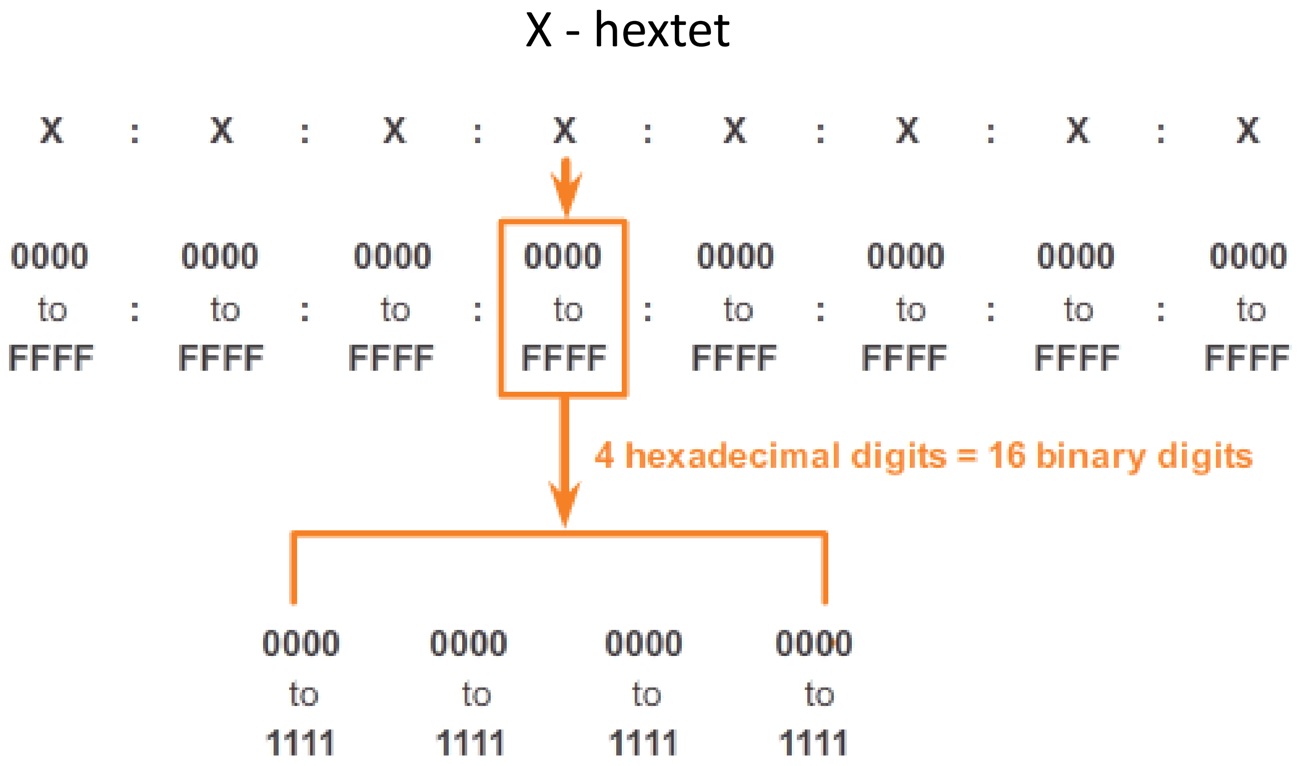
- **Network and Broadcast addresses** - within each network the first and last addresses cannot be assigned to hosts
- **Loopback address -** 127.0.0.1 a special address that hosts use to direct traffic to themselves (addresses 127.0.0.0 to 127.255.255.255 are reserved)
- **Link-Local address -** 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) addresses can be automatically assigned to the local host
- **TEST-NET addresses** - 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) set aside for teaching and learning purposes, used in documentation and network examples
- **Experimental addresses -** 240.0.0.0 to 255.255.255.254 are listed as reserved

IPv6 Address Representation

- 128 bits in length and written as a string of hexadecimal values
- In IPv6, 4 bits represents a single hexadecimal digit, 32 hexadecimal values = IPv6 address
- **Hextet** used to refer to a segment of **16 bits** or **four hexadecimals**
- Can be written in either lowercase or uppercase
- Samples:

  2001:0DB8:0000:1111:0000:0000:0000:0200

  FE80:0000:0000:0000:0123:4567:89AB:CDEF



IPv6 compact presentation form

Rule 1- Omitting Leading 0s

Rule 2- Omitting All 0 Segments:

- A double colon (::) can replace any **single**, contiguous string of one or more 16-bit segments (hextets) consisting of all 0's
- Double colon (::) can only be used **once** within an address otherwise the address will be ambiguous
- Known as the *compressed format*

Preferred	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Omit leading 0s	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressed	2001:DB8::ABCD:0:0:100
OR	
Compressed	2001:DB8:0:0:ABCD::100

Only one :: may be used.

IPv6 Address Types

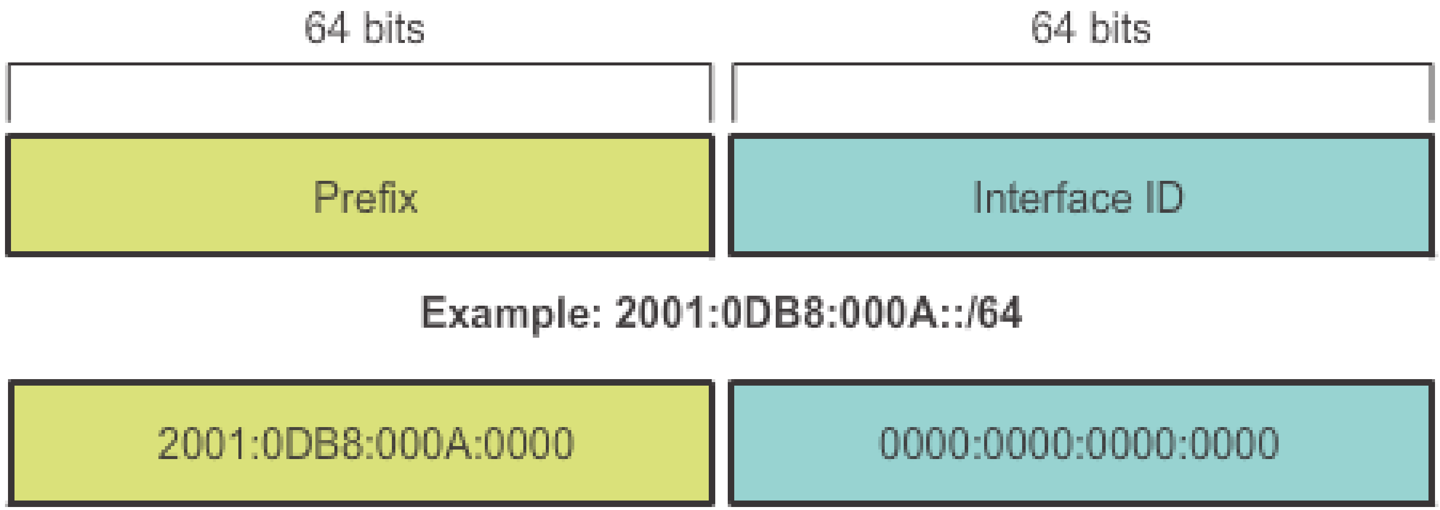
There are three types of IPv6 addresses:

- **Unicast** - an IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device.
- **Multicast** - an IPv6 multicast address is used to send a single IPv6 packet to multiple destinations
- **Anycast** - an IPv6 anycast address 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.

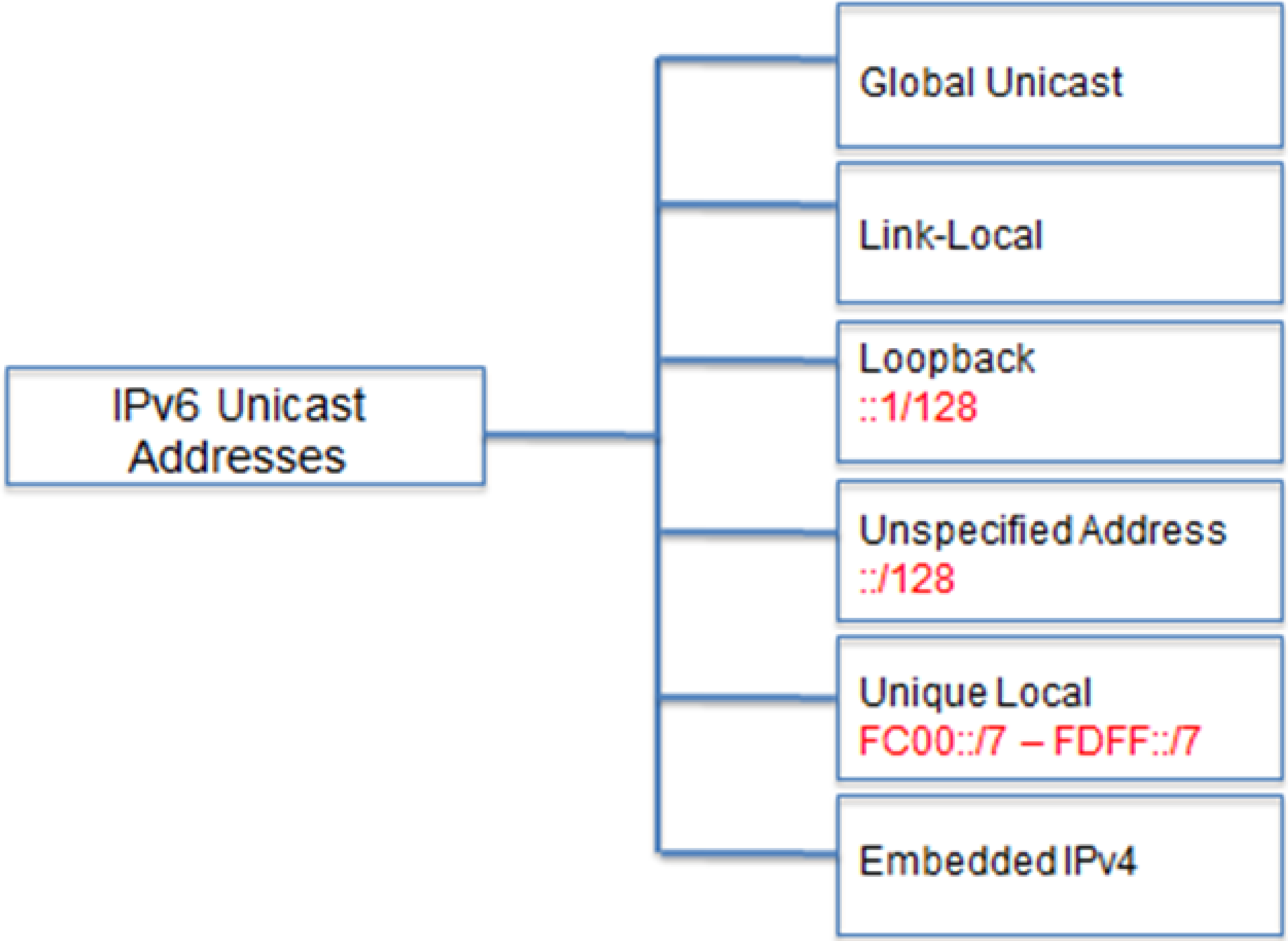
Note: **IPv6 does not have broadcast addresses**.

IPv6 Prefix Length

- IPv6 **does not use** the dotted-decimal subnet mask notation
- Prefix length indicates the network portion of an IPv6 address using the following format:
  - IPv6 address/prefix length
  - Prefix length can range from 0 to 128
  - Typical prefix length is /64

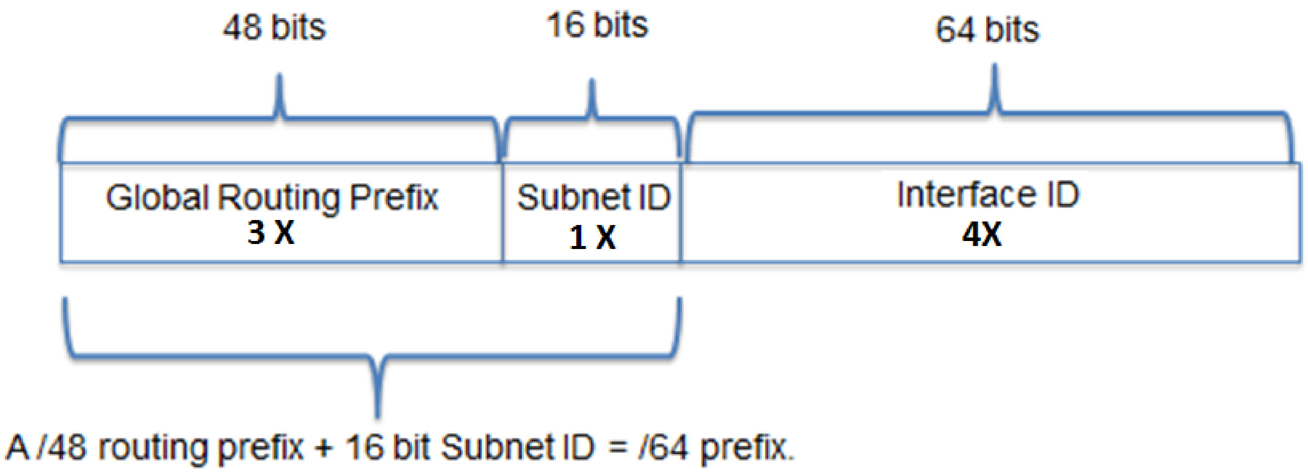


Unicast Address types



Structure of an IPv6 Global Unicast Address

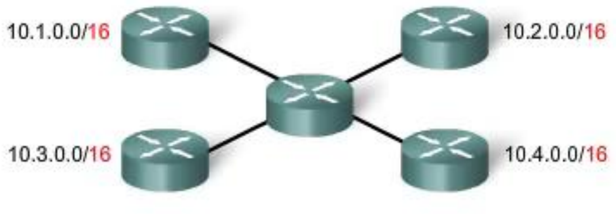
- **Global Routing Prefix**- prefix or network portion of the address assigned by the provider, such as an ISP, to a customer or site, currently, RIR's assign a /48 global routing prefix to customers. This includes **everyone** from **enterprise business networks** to individual **households**. Example: 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (2001:0DB8:ACAD) is the prefix or network portion
- **Subnet ID -** used by an organization to identify subnets within its site
- **Interface ID - e**quivalent to the host portion of an IPv4 address



IPv4 address subnetting

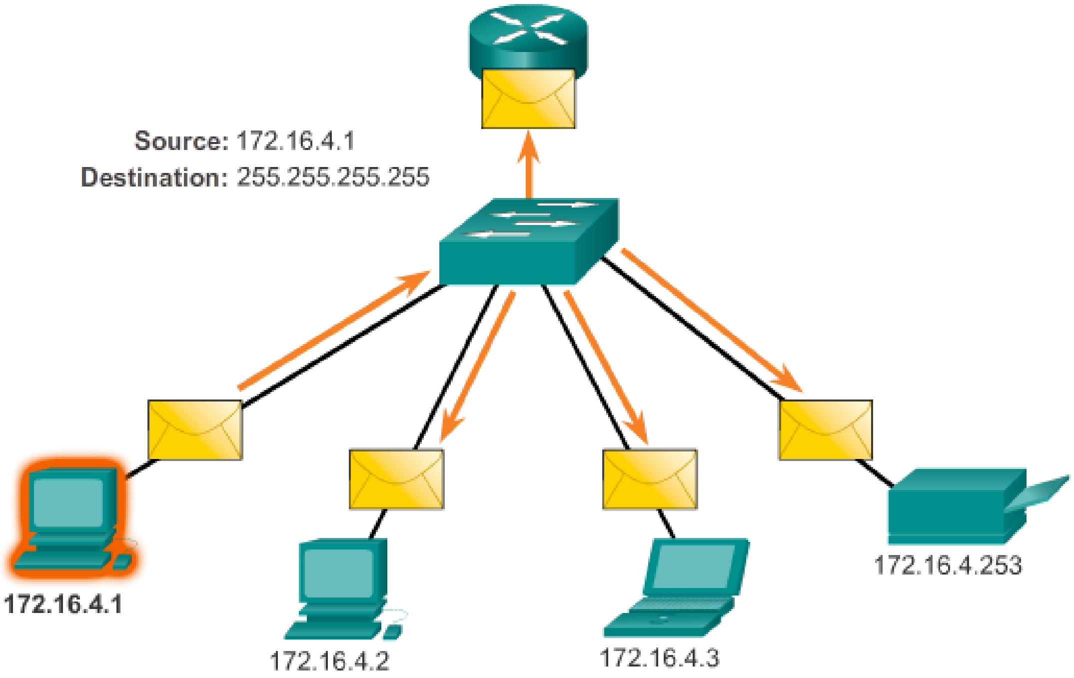
Subnetting

Subnetting - process of segmenting a network into multiple smaller network spaces called subnetworks or **Subnets.**



Reasons for Subnetting

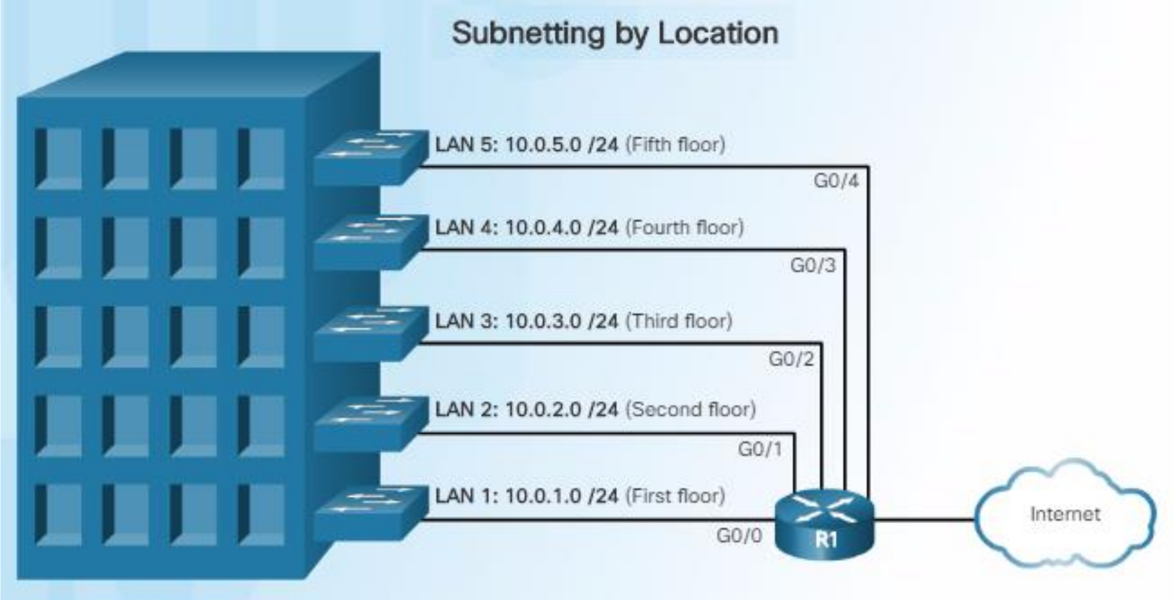
- Control traffic by containing broadcast traffic within subnetwork
- Reduce overall network traffic and improve network performance
- Reduce security risks

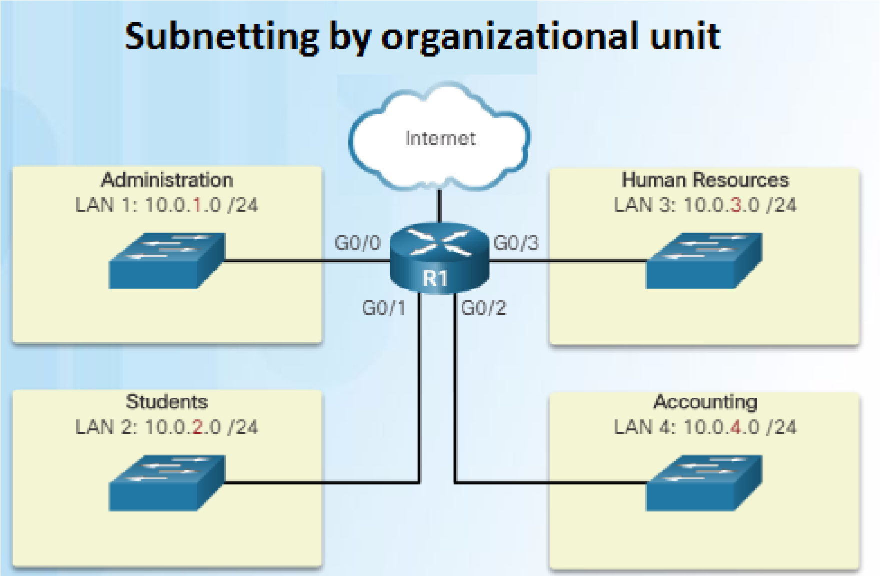


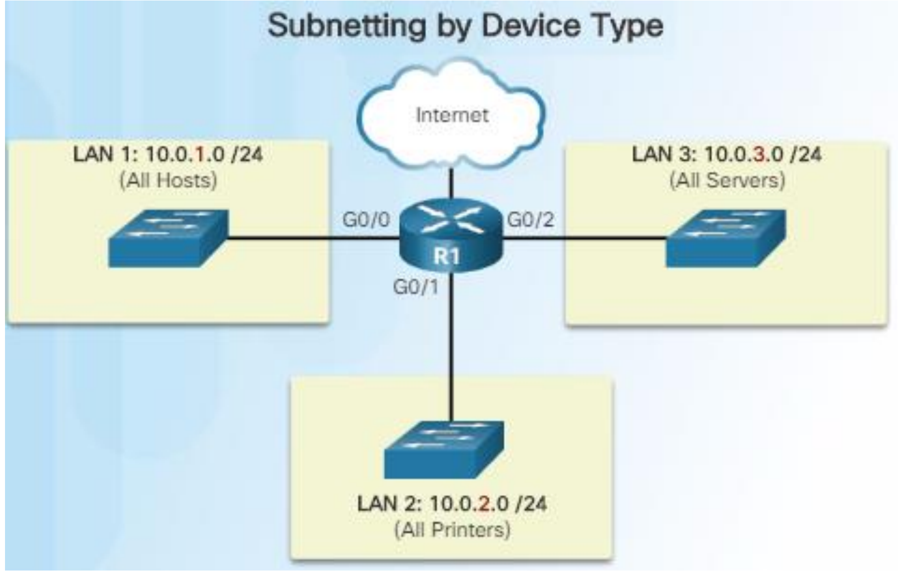
Subnetting ways

There are various ways of using subnets to help manage network devices. Network administrators can group devices and services into subnets that are determined by:

- Location, such as floors in a building.
- Organizational unit.
- Device type.
- Any other division that makes sense for the network.







Subnetting types

- Same Length Subnet Masks (SLSM) – all subnets have the **same** subnetting mask
- Variable Length Subnet Masks (VLSM) - allows a network space to be divided in **unequal** parts
- Subnetting based on **host requirements**
- Subnetting based on **networks requirements**

Subnetting networks on the octet boundary

- IPv4 subnets are created by using **one or more of the host bits as network bits**.
- This is done by **extending the subnet mask** to borrow some of the bits from the host portion of the address to create additional network bits.
- Networks are most easily subnetted at the octet boundary of **/8**, **/16**, and **/24**.

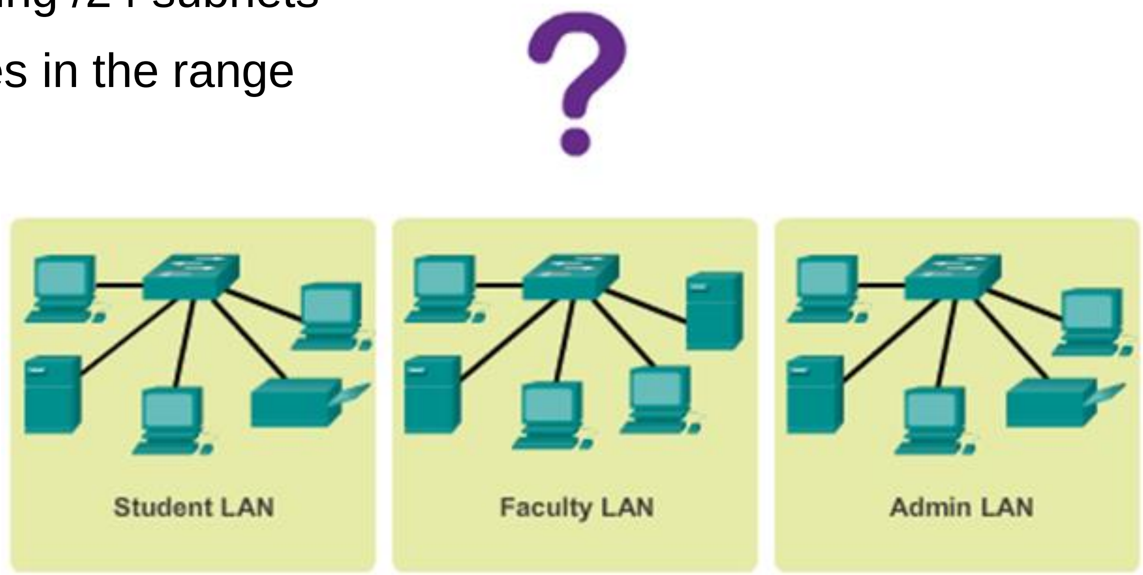
Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Subnetting Network 10.x.x.0/24

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	10.0.1.255
...	...	...
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	1.1.1.0.255
10.1.2.0/24	10.1.2.1 - 10.1.2.254	10.1.2.0.255
...	...	...
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

The subnetting plan

- The size of the subnet involves **planning the number of hosts** that will require IP host addresses in each subnet of the subdivided private network. For example, in a campus network design you might consider **how many hosts are needed** in the Administrative LAN, how many in the Faculty LAN and how many in the Student LAN.
- Create **standards for IP address assignments** within each subnet range. For example:
  - Printers and servers will be assigned static IP addresses
  - User will receive IP addresses from DHCP servers using /24 subnets
  - Routers are assigned the first available host addresses in the range



IP Subnetting principle

- IPv4 subnets are created by **using one or more of the host bits as network bits**.
- This is done by extending the mask to **borrow** some of the bits from the host portion of the address to create additional network bits.
- The more host bits borrowed, the more subnets that can be defined. For each bit borrowed, the number of subnetworks available is doubled. For example, if 1 bit is borrowed, 2 subnets can be created. If 2 bits, 4 subnets are created, if 3 bits are borrowed, 8 subnets are created, and so on.
- However, with each bit borrowed, fewer host addresses are available per subnet.

Subnetting a /24 Network

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	64	2

Subnetting

There are two considerations when planning subnets:

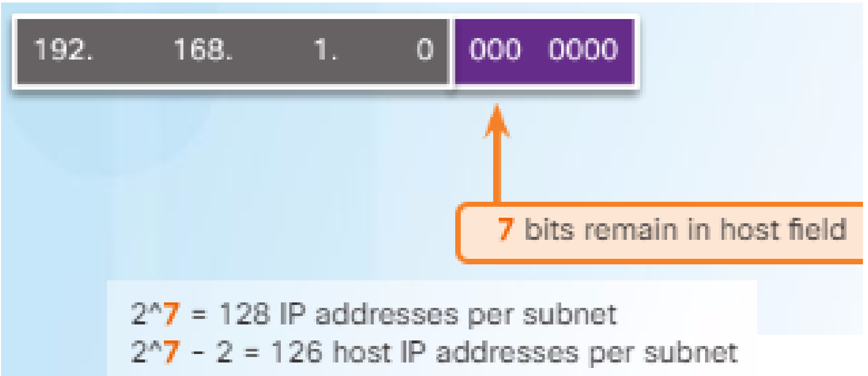
- Number of Subnets required: **2^n**

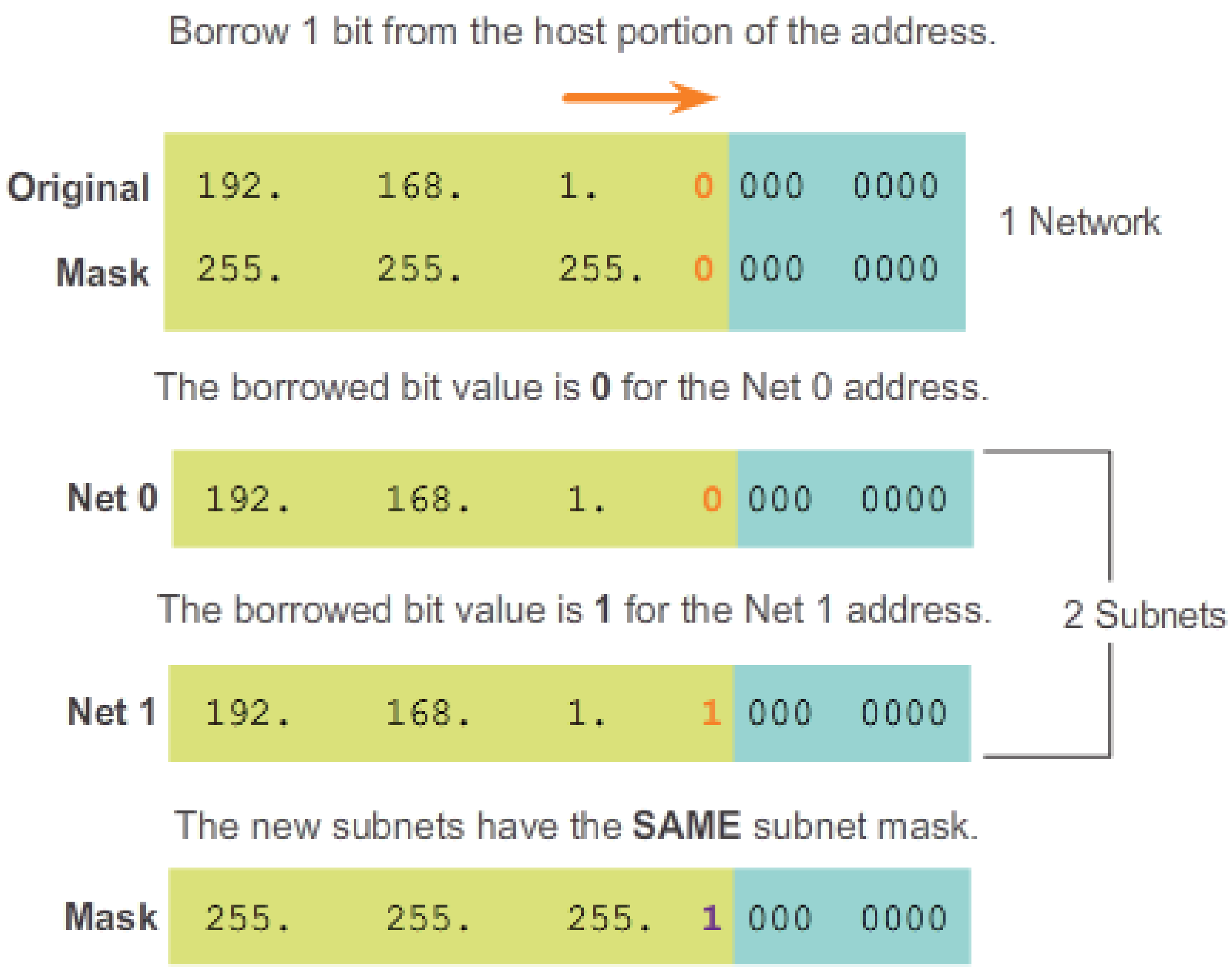
  n - is the number of host bits borrowed

- Number of Host addresses required: **2^m-2**

  m - is the number of host bits remaining

  2 - **subnetwork** and **broadcast** address cannot be used on each subnet

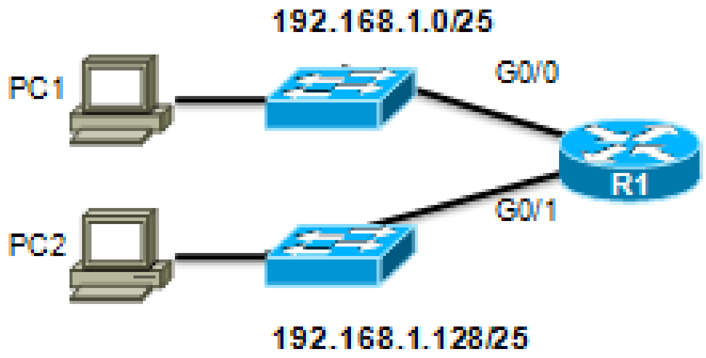




Subnetting in Use (2 subnets)

Subnet 0

Network 192.168.1.0-127/25



Subnet 1

Network 192.168.1.128-255/25

Address Range for 192.168.1.0/25 Subnet

Network Address	192. 168. 1. 0 000 0000	= 192.168.1.0
First Host Address	192. 168. 1. 0 000 0001	= 192.168.1.1
Last Host Address	192. 168. 1. 0 111 1110	= 192.168.1.126
Broadcast Address	192. 168. 1. 0 111 1111	= 192.168.1.127

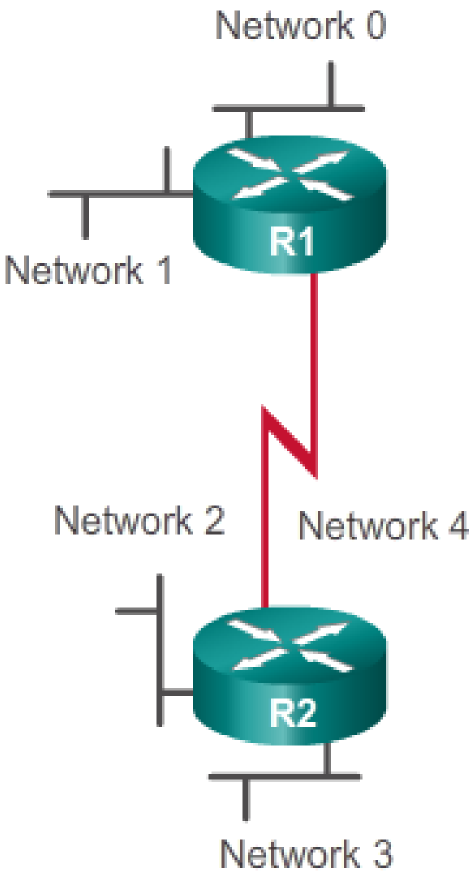
Address Range for 192.168.1.128/25 Subnet

Network Address	192. 168. 1. 1 000 0000	= 192.168.1.128
First Host Address	192. 168. 1. 1 000 0001	= 192.168.1.129
Last Host Address	192. 168. 1. 1 111 1110	= 192.168.1.254
Broadcast Address	192. 168. 1. 1 111 1111	= 192.168.1.255

Subnetting in Use (8 subnets)

Borrowing **3 bits** to create **8 subnets**.

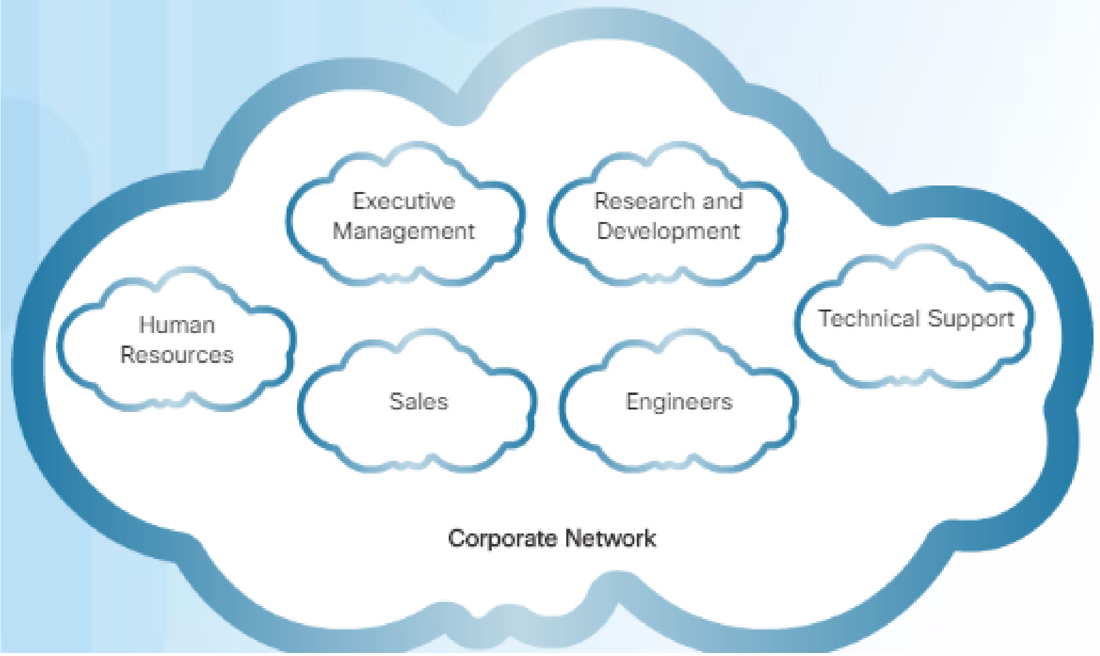
2^3 = 8 subnets



Net 0	Network	192.	168.	1.	000	0 0000	192.168.1.0
	First	192.	168.	1.	000	0 0001	192.168.1.1
	Last	192.	168.	1.	000	1 1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1 1111	192.168.1.31
Net 1	Network	192.	168.	1.	001	0 0000	192.168.1.32
	First	192.	168.	1.	001	0 0001	192.168.1.33
	Last	192.	168.	1.	001	1 1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1 1111	192.168.1.63
Net 2	Network	192.	168.	1.	010	0 0000	192.168.1.64
	First	192.	168.	1.	010	0 0001	192.168.1.65
	Last	192.	168.	1.	010	1 1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1 1111	192.168.1.95
Net 3	Network	192.	168.	1.	011	0 0000	192.168.1.96
	First	192.	168.	1.	011	0 0001	192.168.1.97
	Last	192.	168.	1.	011	1 1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1 1111	192.168.1.127

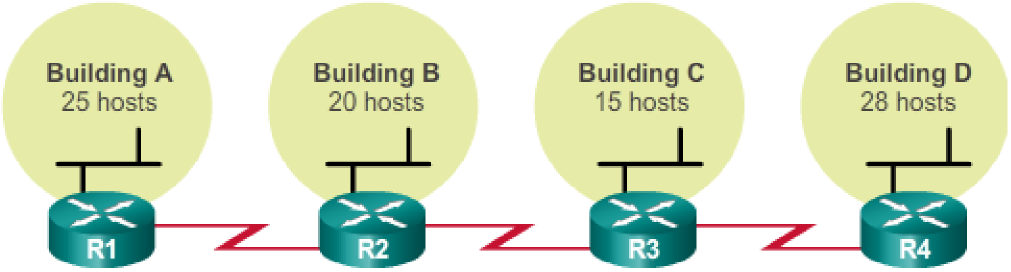
Subnetting Based on Host or Network Requirements

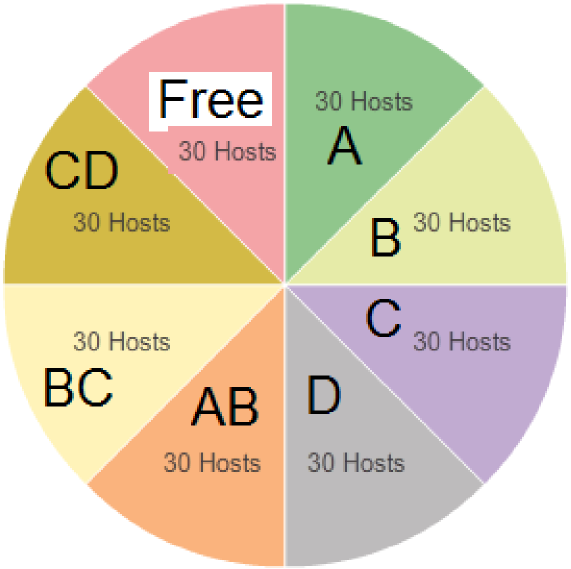
Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	16	14

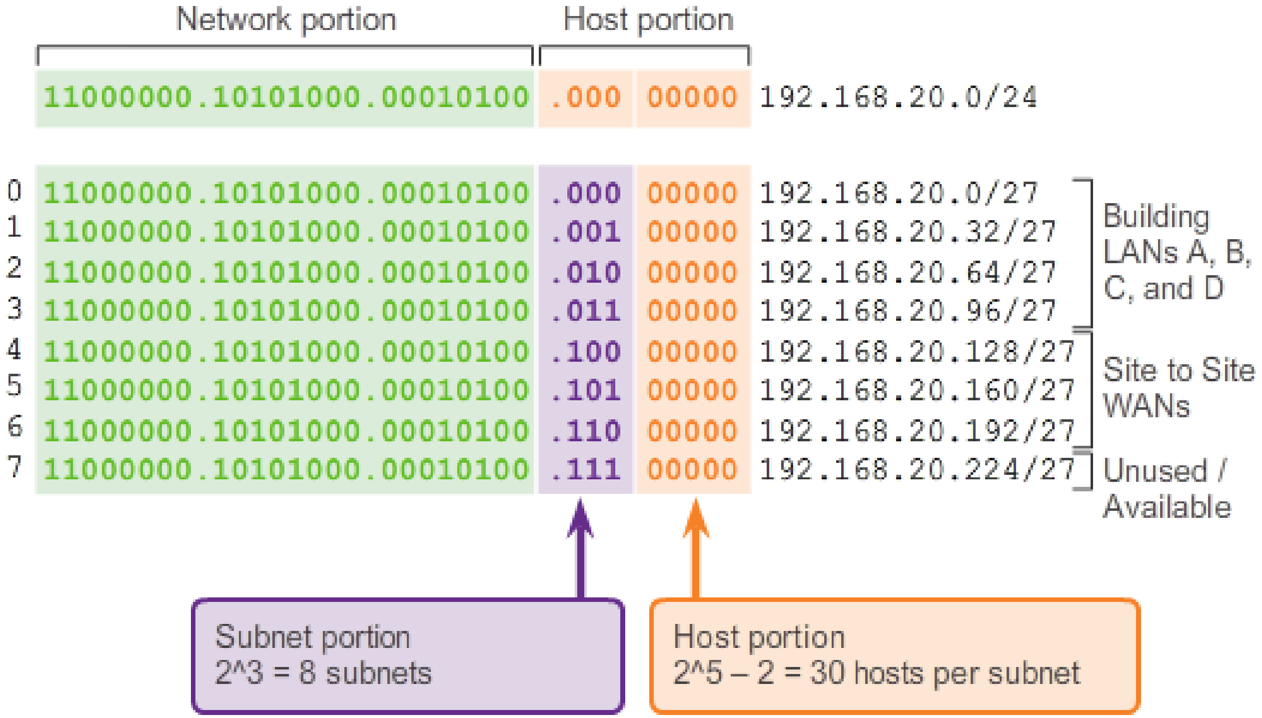


- Using traditional subnetting, the **same number** of addresses is allocated for each subnet.
- If all the subnets have the same requirements for the number of hosts, these fixed size address blocks would be efficient.
- However, most often that is not the case.

Subnetting To Meet Network Requirements



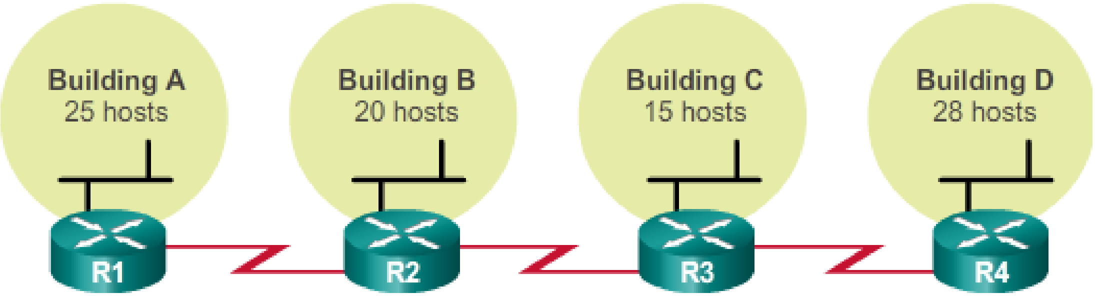


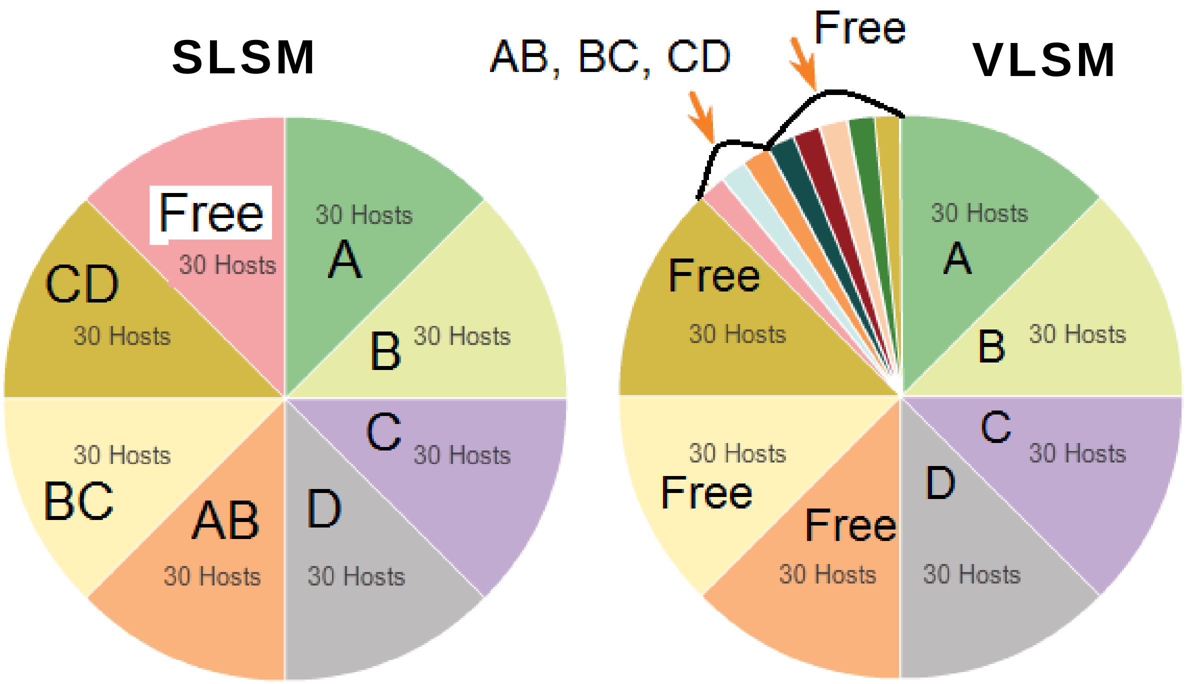


Variable Length Subnet Masks (VLSM)

- VLSM allows a network space to be divided in **unequal** parts.
- Subnet mask will vary depending on how many bits have been borrowed for a particular subnet.
- Network is first subnetted, and then the subnets are subnetted again.
- Process repeated as necessary to create subnets of various sizes.

VLSM Subnetting





	11000000.10101000.00010100	.000 00000	192.168.20.0/24

0	11000000.10101000.00010100	.000 00000	192.168.20.0/27	LANs A, B, C, D
1	11000000.10101000.00010100	.001 00000	192.168.20.32/27	
2	11000000.10101000.00010100	.010 00000	192.168.20.64/27	
3	11000000.10101000.00010100	.011 00000	192.168.20.96/27	
4	11000000.10101000.00010100	.100 00000	192.168.20.128/27	Unused / Available
5	11000000.10101000.00010100	.101 00000	192.168.20.160/27	
6	11000000.10101000.00010100	.110 00000	192.168.20.192/27	
7	11000000.10101000.00010100	.111 00000	192.168.20.224/27	

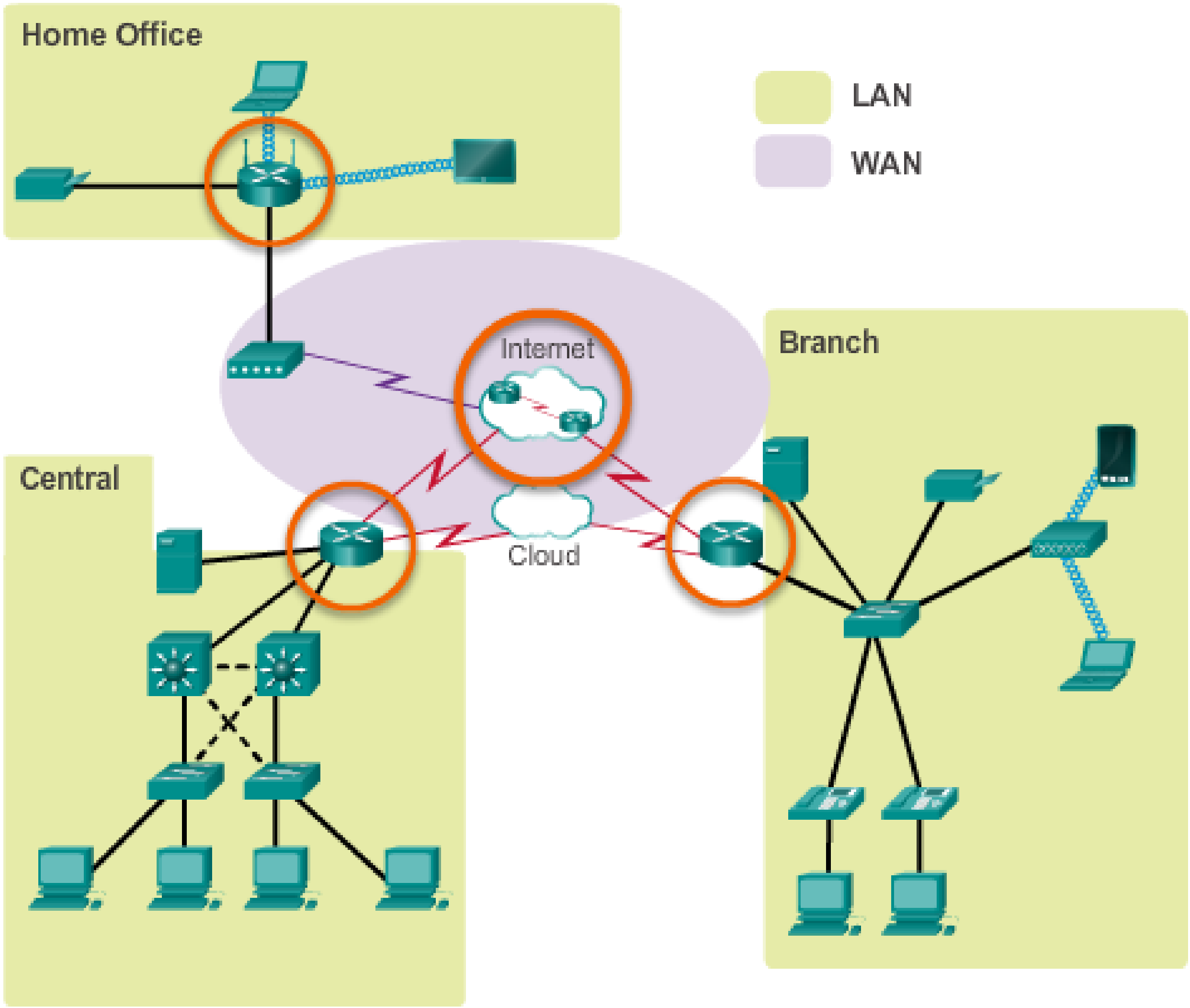
3 more bits borrowed from subnet 7:

7:0	11000000.10101000.00010100	.111000 00	192.168.20.224/30	WANs
7:1	11000000.10101000.00010100	.111001 00	192.168.20.228/30	
7:2	11000000.10101000.00010100	.111010 00	192.168.20.232/30	
7:3	11000000.10101000.00010100	.111011 00	192.168.20.236/30	Unused / Available
7:4	11000000.10101000.00010100	.111100 00	192.168.20.240/30	
7:5	11000000.10101000.00010100	.111101 00	192.168.20.244/30	
7:6	11000000.10101000.00010100	.111110 00	192.168.20.248/30	
7:7	11000000.10101000.00010100	.111111 00	192.168.20.252/30	

IP routing

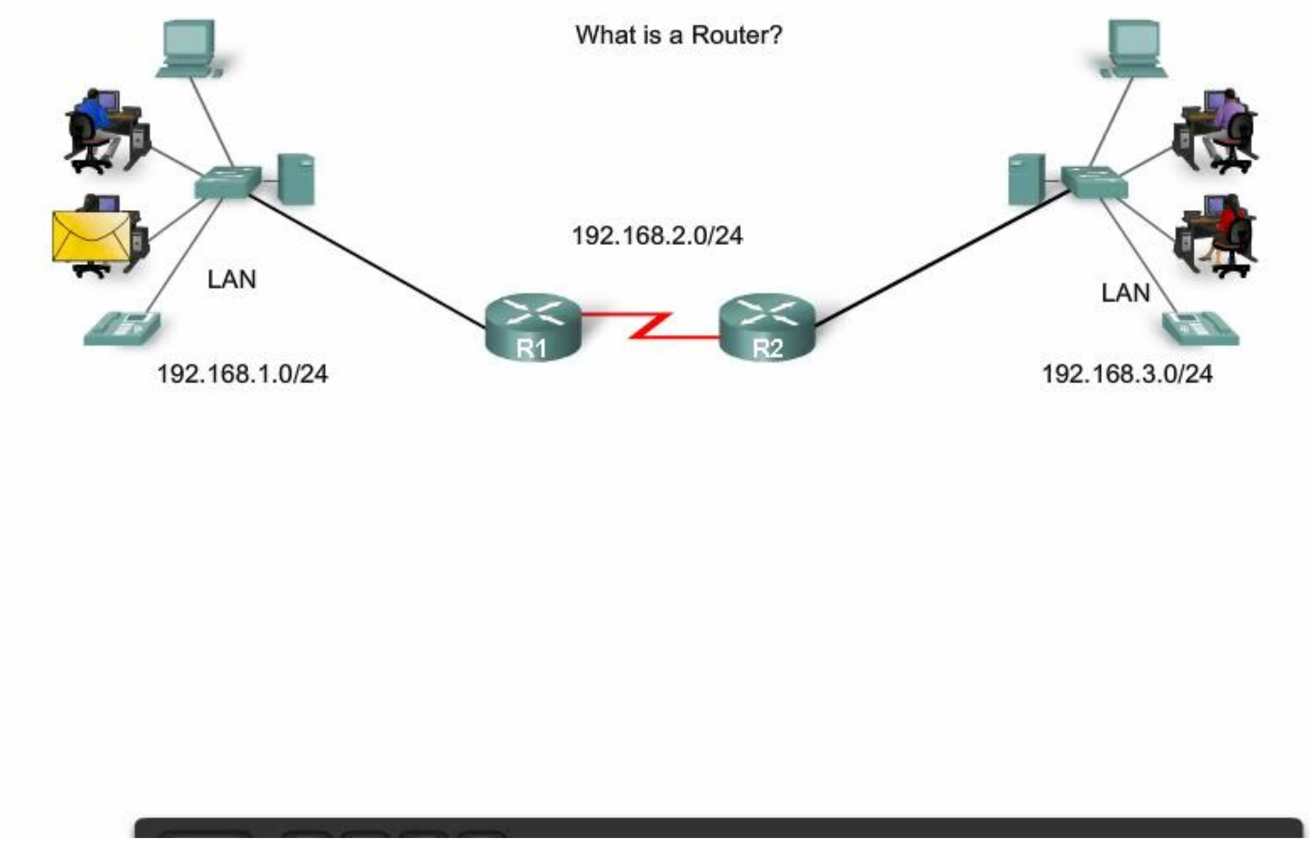
Why Routing?

- Communication between networks would not be possible without a router determining the best path to the destination and forwarding traffic to the next router along that path.
- The router is responsible for the routing of traffic between networks.



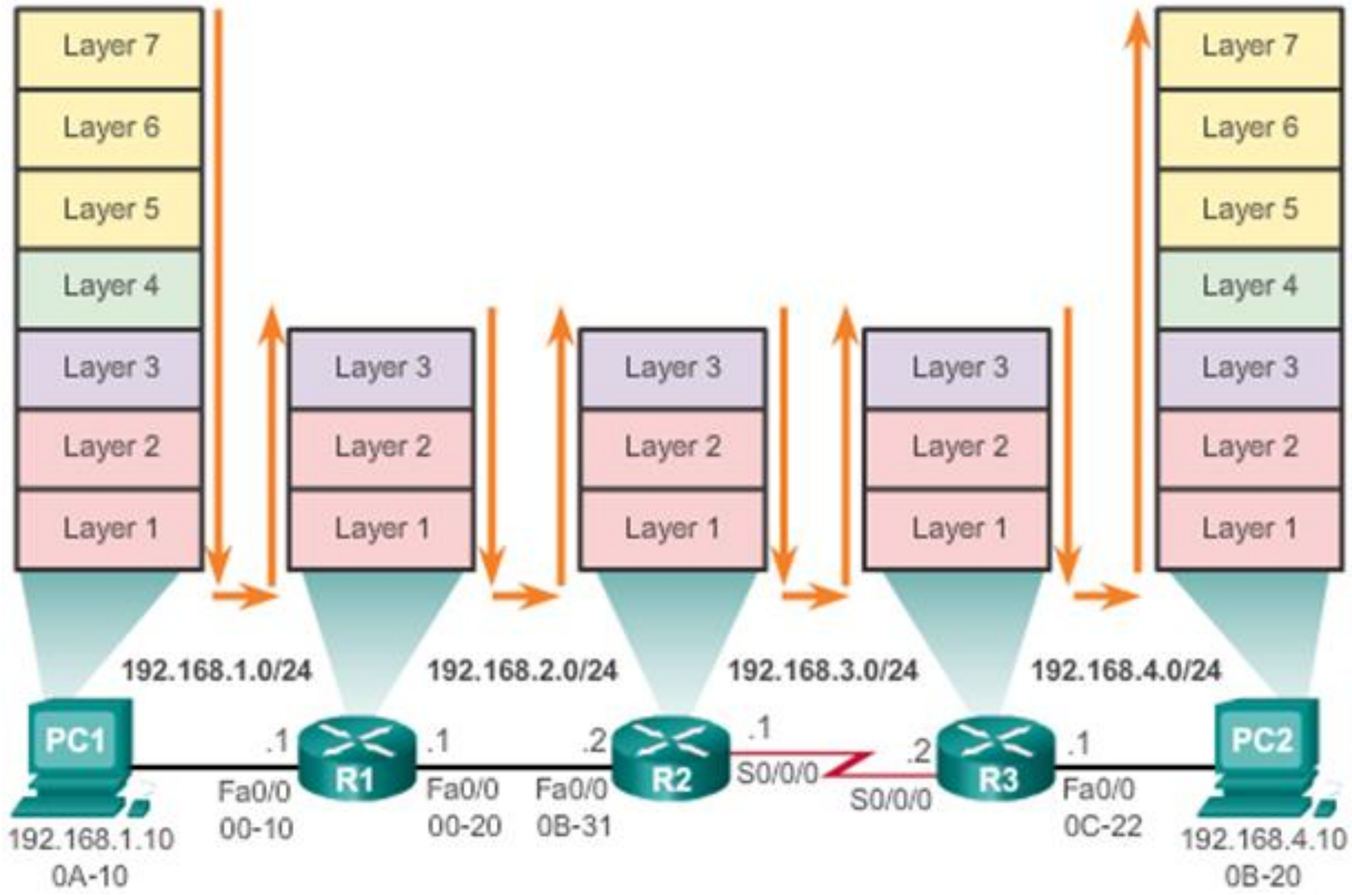
Functions of a router

- When the router receives a packet, it examines the **destination address** of the packet and uses the **routing table** to search for the best path to that network.
- The routing table also includes the **interface** to be used to **forward packets** for each known network.
- When a match is found, the router **encapsulates** the packet into the data link frame of the outgoing or **exit interface**, and the packet is forwarded toward its destination.
- It is possible for a router to receive a packet that is encapsulated in one type of data link frame, and to forward the packet out of an interface that uses a different type of data link frame.

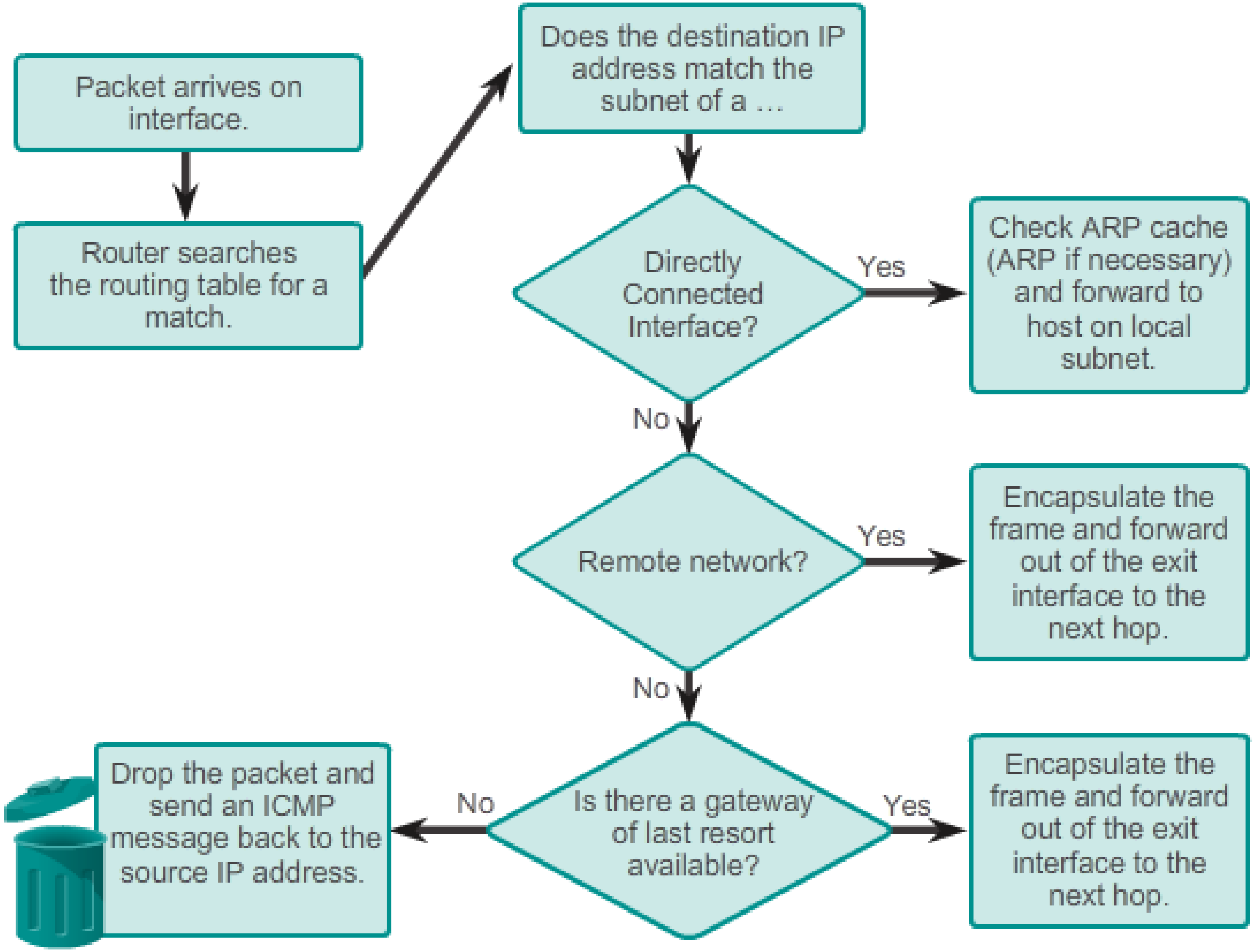


Router Switching Functions

- The router performs the following three major steps:
- **Step 1**. De-encapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer.
- **Step 2.** Examines the destination IP address of the IP packet to find the best path in the routing table.
- **Step 3.** If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface.
- **Note**: In this context, the term “switching” literally means moving packets from source to destination and should not be confused with the function of a Layer 2 switch.

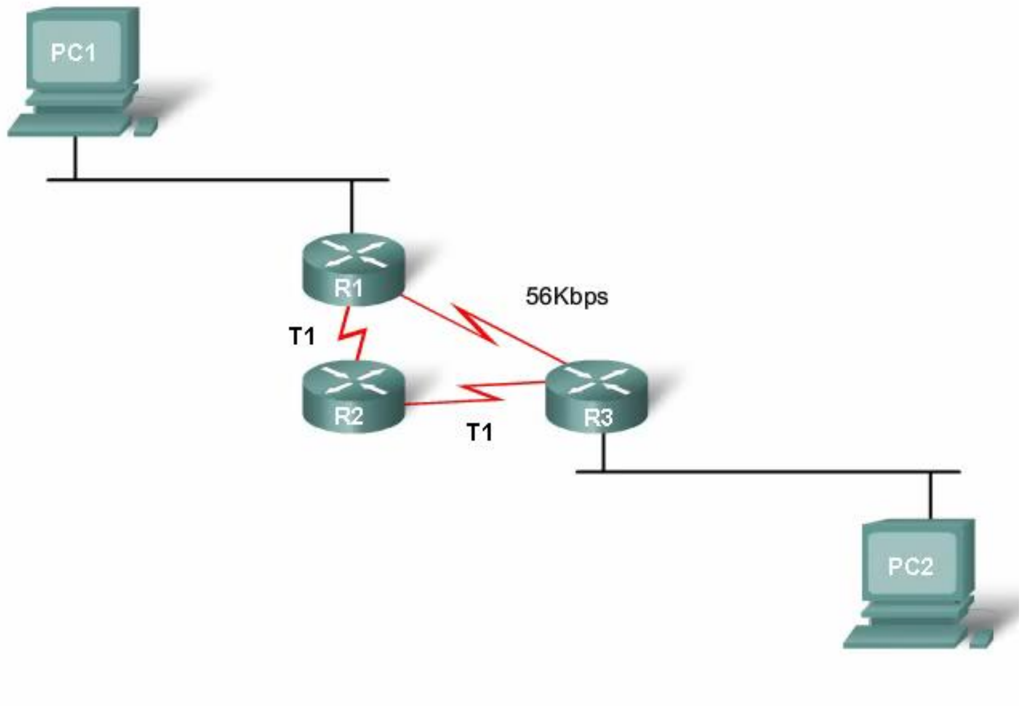


Packet Forwarding Decisions Process



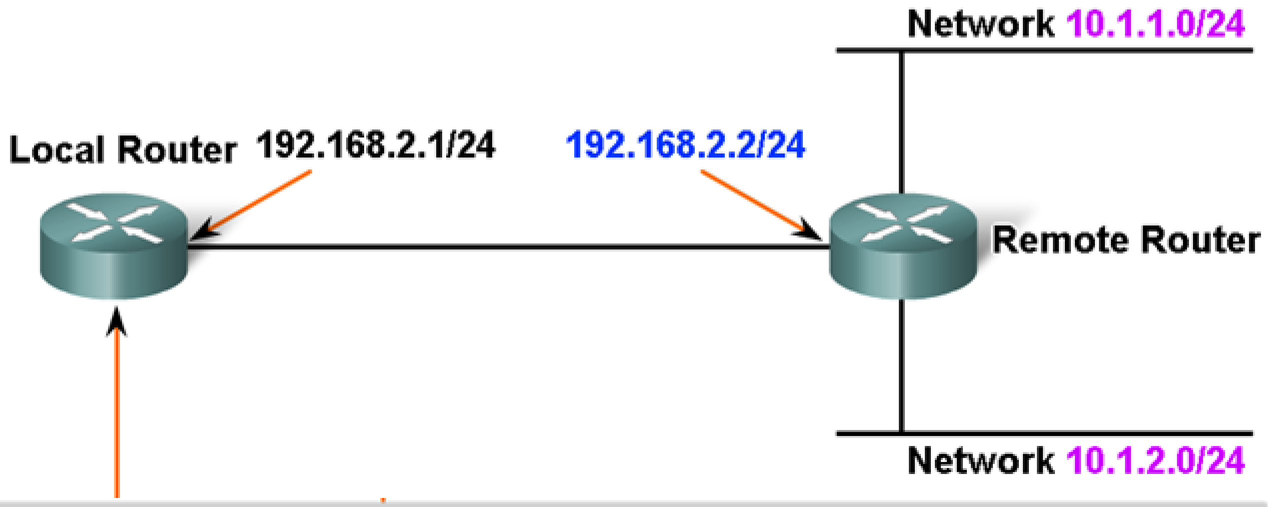
Best Path

- 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 value used to measure the distance to a given network.
- Best path to a network is the path with the **lowest metric**.
- Dynamic routing protocols use their own rules and metrics to build and update routing tables for example:
  - **Routing Information Protocol (RIP)** - Hop count
  - **Open Shortest Path First (OSPF)** - Cost based on cumulative bandwidth from source to destination
  - **Enhanced Interior Gateway Routing Protocol (EIGRP)** - Bandwidth, delay, load, reliability



Routing Table Records

- **Static** - created by the administrator, have unlimited validity
- **Dynamic** - created as a result of dynamic routing protocols, have a limited lifetime
- **Automatic** - records about directly connected networks, are created automatically upon completion of setup and inclusion of the router interface

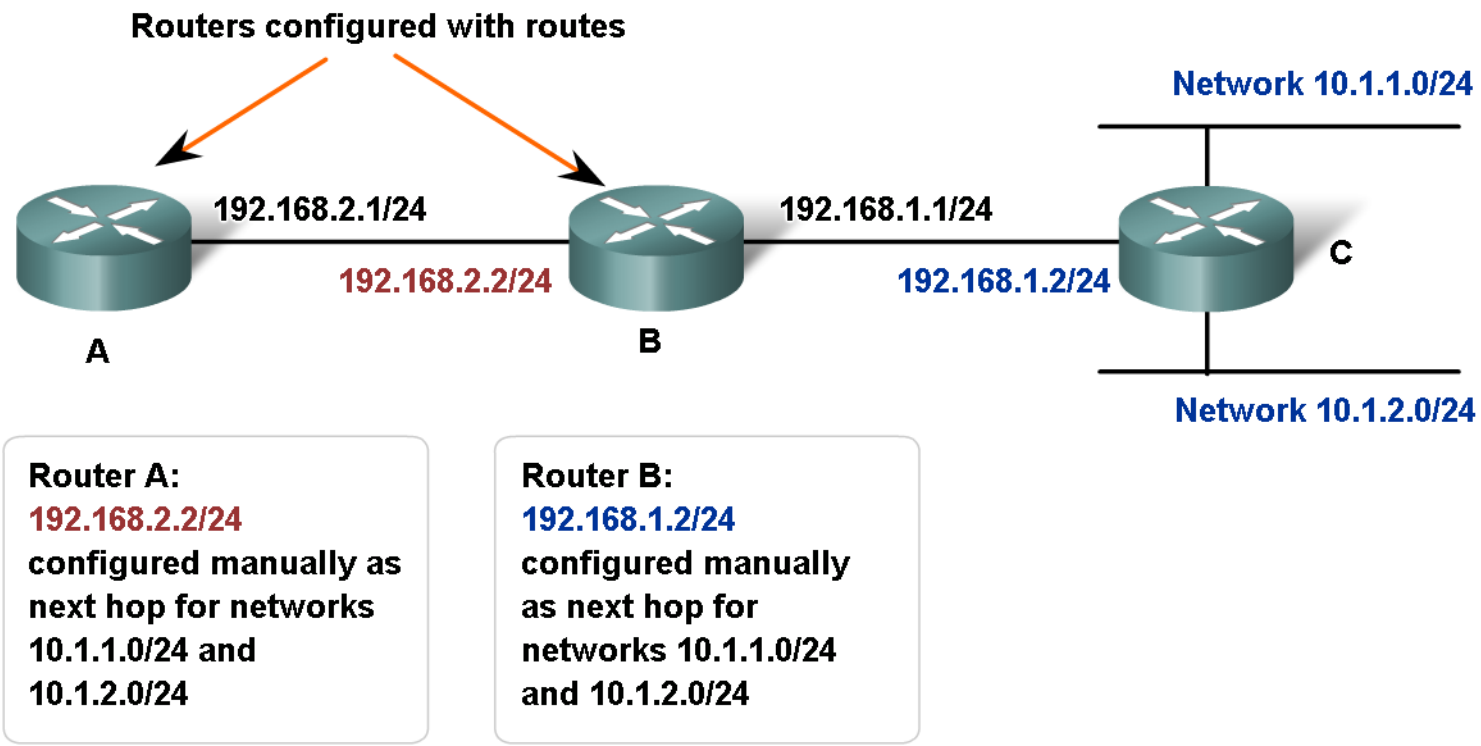



```
   10.0.0.0/24 is subnetted, 2 subnets
R       10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R       10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C   192.168.1.0/24 is directly connected, FastEthernet0/0
```

Static Routing

Static routing has three primary uses:

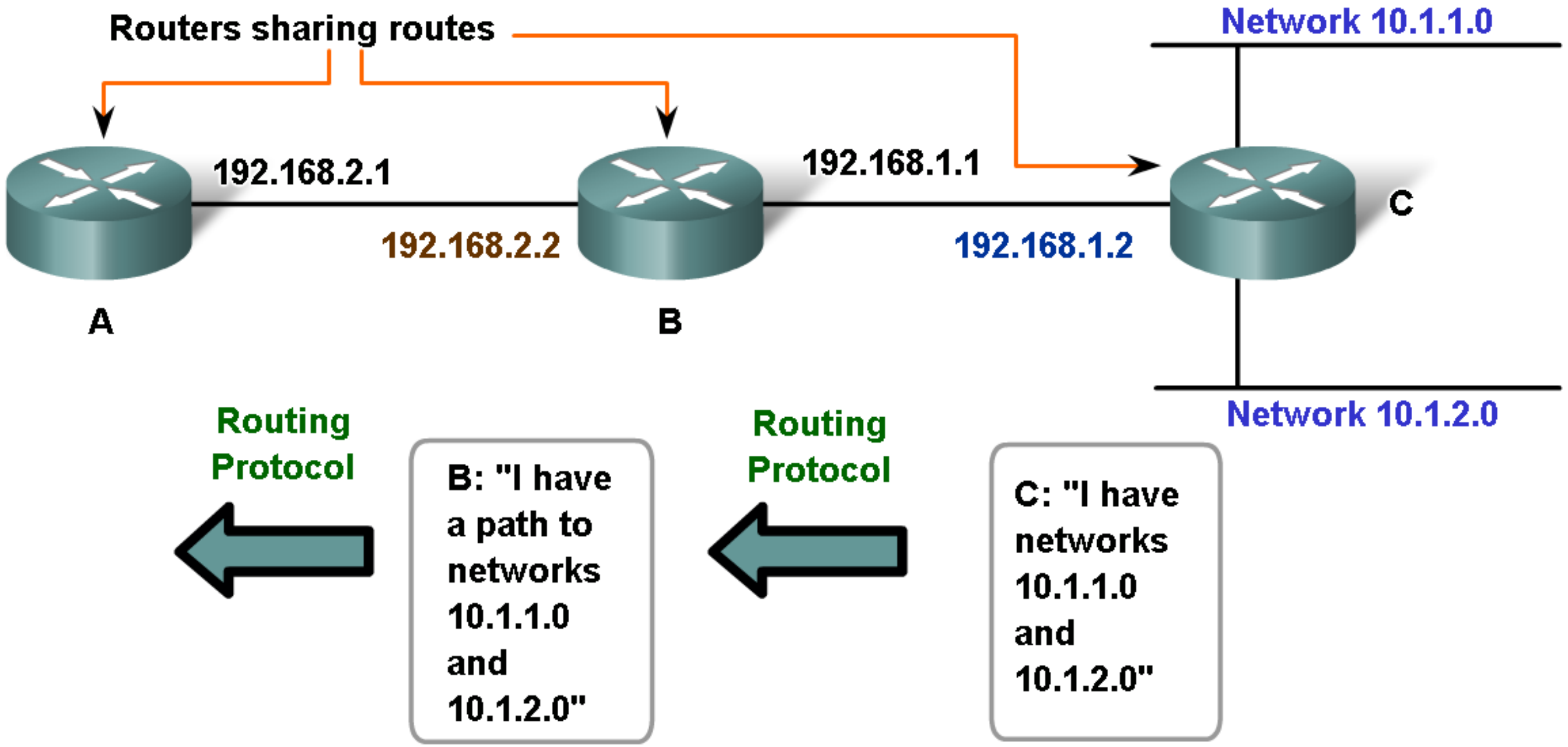
- Providing ease of routing table maintenance in **smaller networks** that are not expected to grow significantly.
- Routing to and from **stub networks**. A stub network is a network accessed by a single route, and the router has no other neighbors.
- Using a **single default route** to represent a 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.



Dynamic Routing

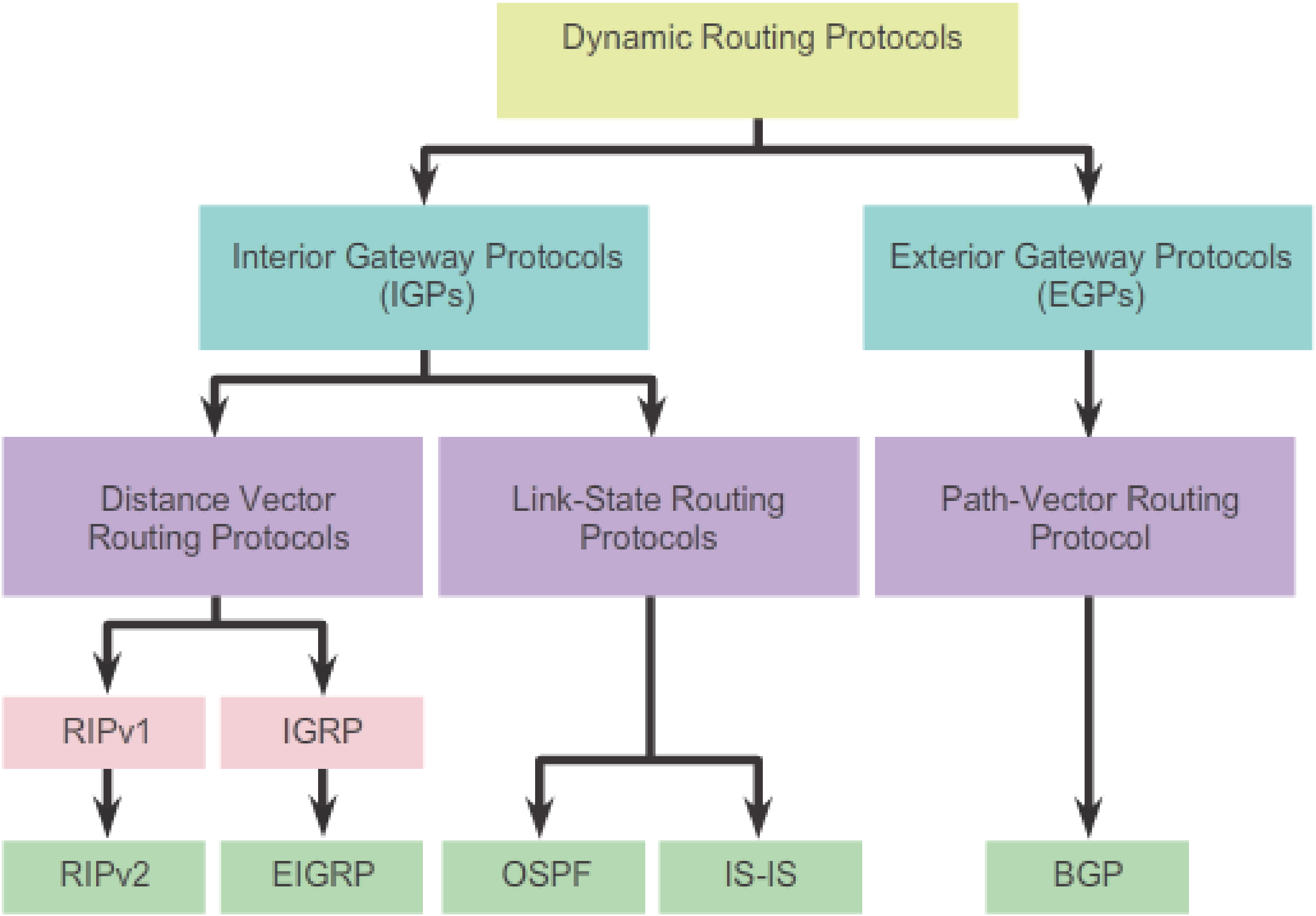
Dynamic routing protocols functions:

- Exchange of routing information between routers.
- Automatic update of the routing table when changing the route.
- Determining the best path to the destination.



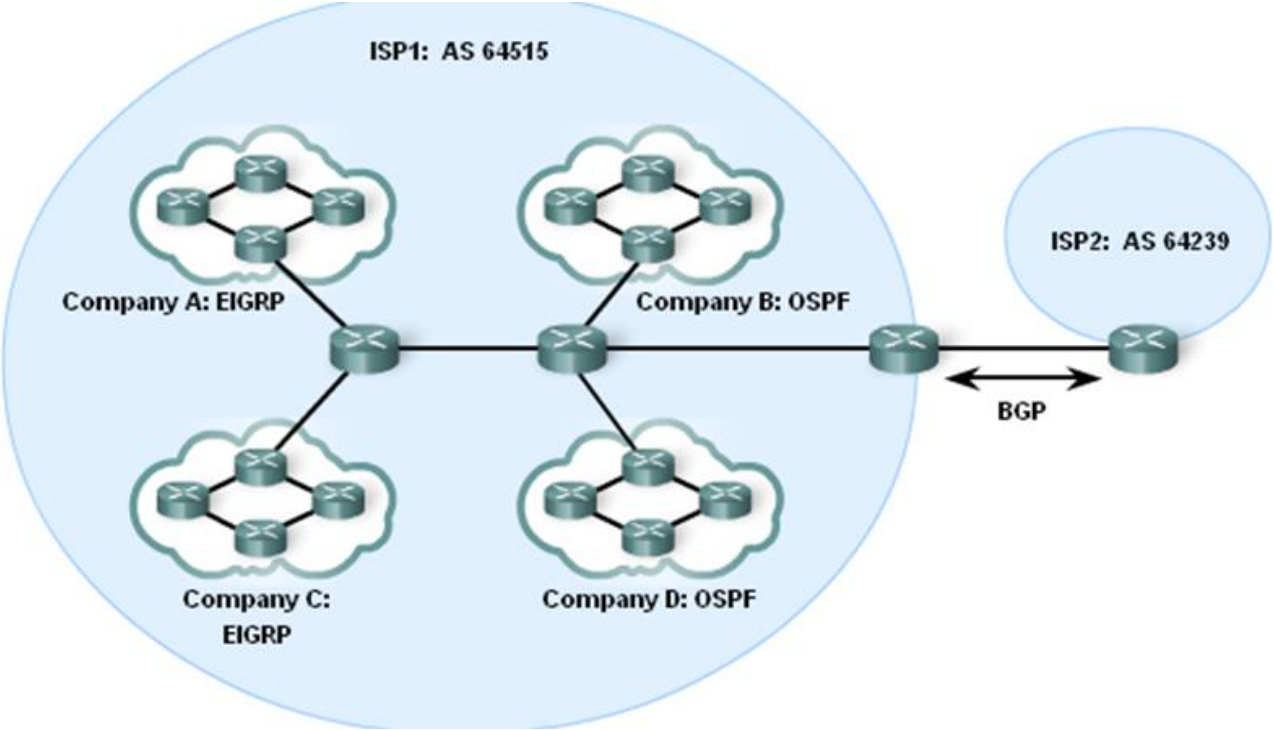
Router B learns about Router C's networks dynamically.
Router B's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.1.2 (Router C).
Router A learns about Router C's networks dynamically from Router B.
Router A's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.2.2 (Router B).

Dynamic routing protocol classification



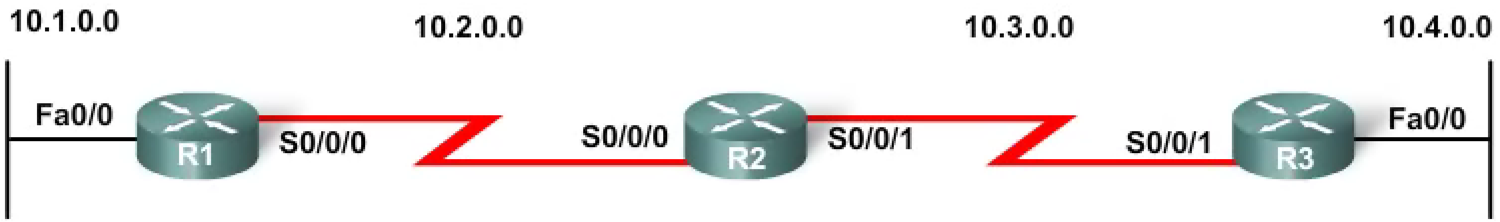
IGP and EGP

- An autonomous system (AS) is a collection of routers under a common administration such as a company or an organization. An AS is also known as a routing domain. Typical examples of an AS are a company's internal network and an ISP's network.
- The Internet is based on the AS concept; therefore, two types of routing protocols are required:
- **Interior Gateway Protocols (IGP)** - Used for routing **within** an AS. It is also referred to as intra-AS routing. Companies, organizations, and even service providers use an IGP on their internal networks.
- **Exterior Gateway Protocols (EGP)** - Used for routing **between** AS. It is also referred to as inter-AS routing. Service providers and large companies may interconnect using an EGP.



Distance Vector

- Routers do not have information about the topology of the all network
- Routers periodically send a routing table to neighbors
- Each router knows only the **distance** and direction (**vector**) to other networks
- Possibility of **routing loops**
- RIP, IGRP
- EIGRP loop free



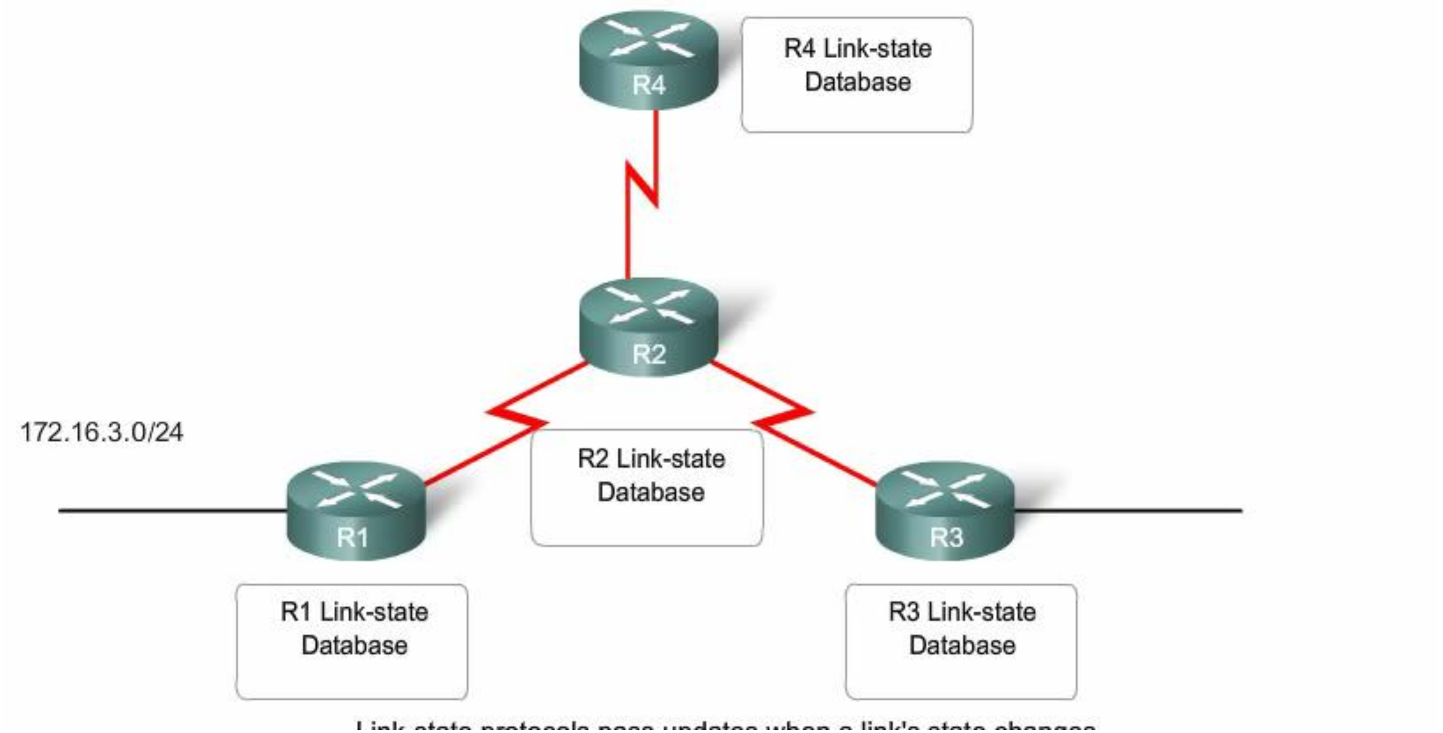
Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

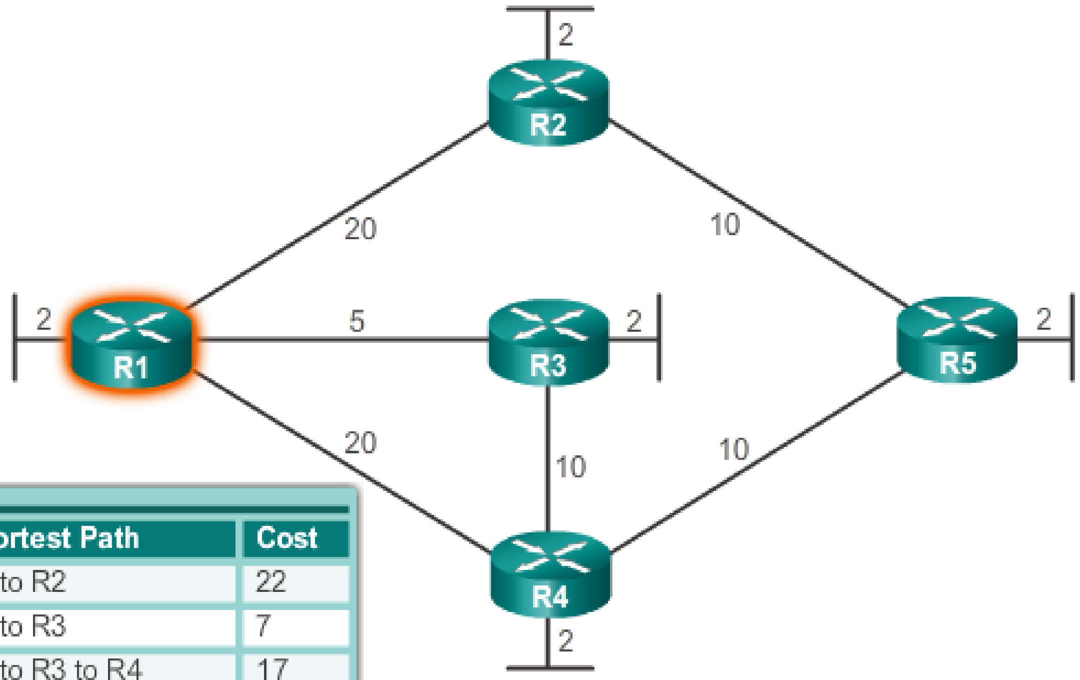
Link State

- Each router has complete information about the network topology
- Each router independently calculates the optimal routes, usually using the Dijkstra algorithm
- Updates are transmitted only when changes occur and contain information only about changes
- Loops are not formed
- OSPF, IS-IS



Shortest Path First Algorithm

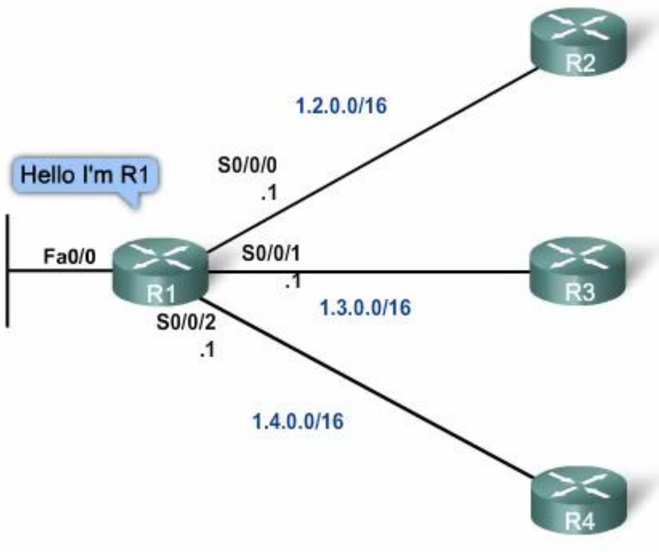
- All link-state routing protocols apply Dijkstra’s algorithm to calculate the best path route.
- The algorithm is commonly referred to as the shortest path first (SPF) algorithm.
- This algorithm uses accumulated costs along each path, from source to destination, to determine the total cost of a route.
- Link-state routing protocols have the reputation of being much more complex than their distance vector counterparts. However, the basic functionality and configuration of link-state routing protocols is equally straight-forward.

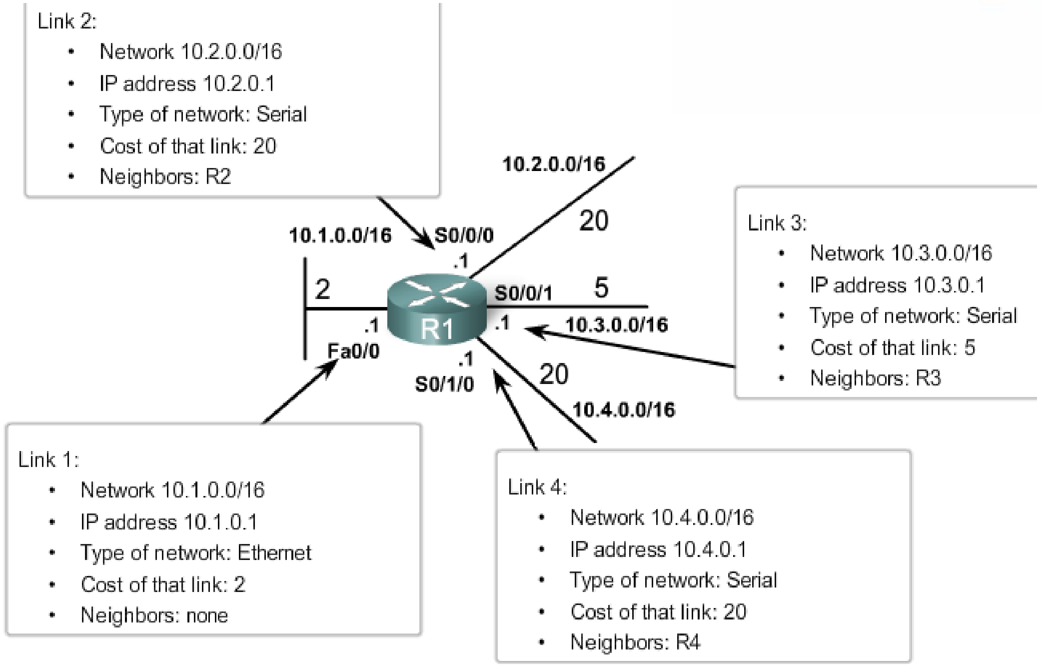


Destination	Shortest Path	Cost
R2 LAN	R1 to R2	22
R3 LAN	R1 to R3	7
R4 LAN	R1 to R3 to R4	17
R5 LAN	R1 to R3 to R4 to R5	27

Link-State Routing Process

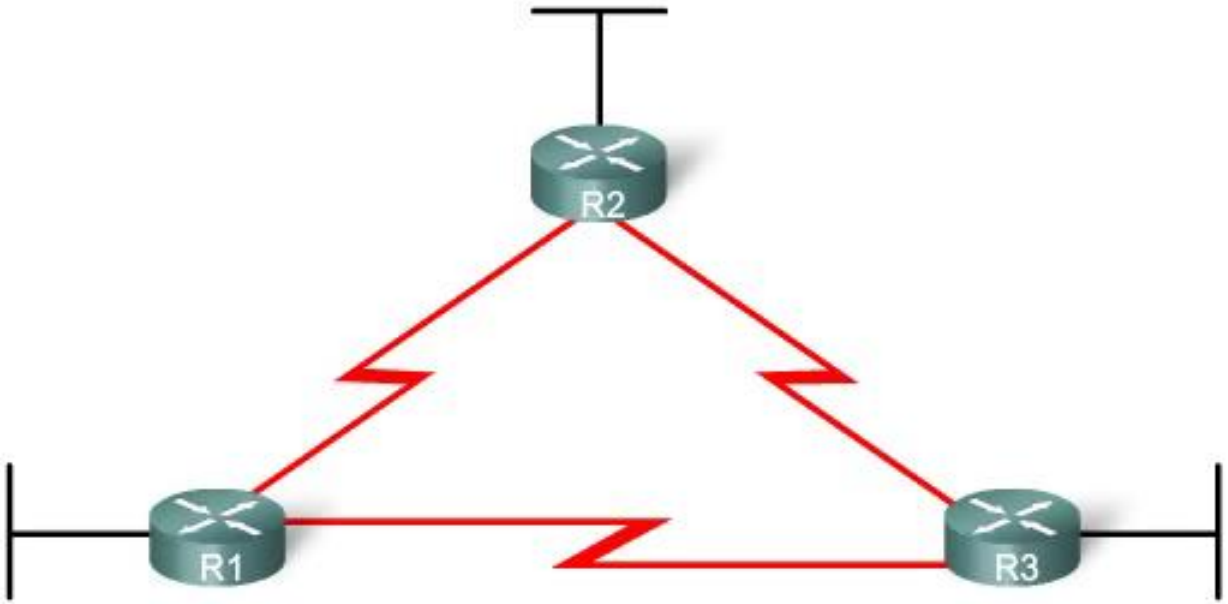
1. Each router learns about each of its own directly connected networks.
2. Each router is responsible for "saying hello" to its neighbors on directly connected networks.
3. Each router builds a Link-State Packet (LSP) containing the state of each directly connected link.
4. Each router floods the LSP to all neighbors who then store all LSP's received in a database.
5. Each router uses the database to construct a complete map of the topology and computes the best path to each destination network.





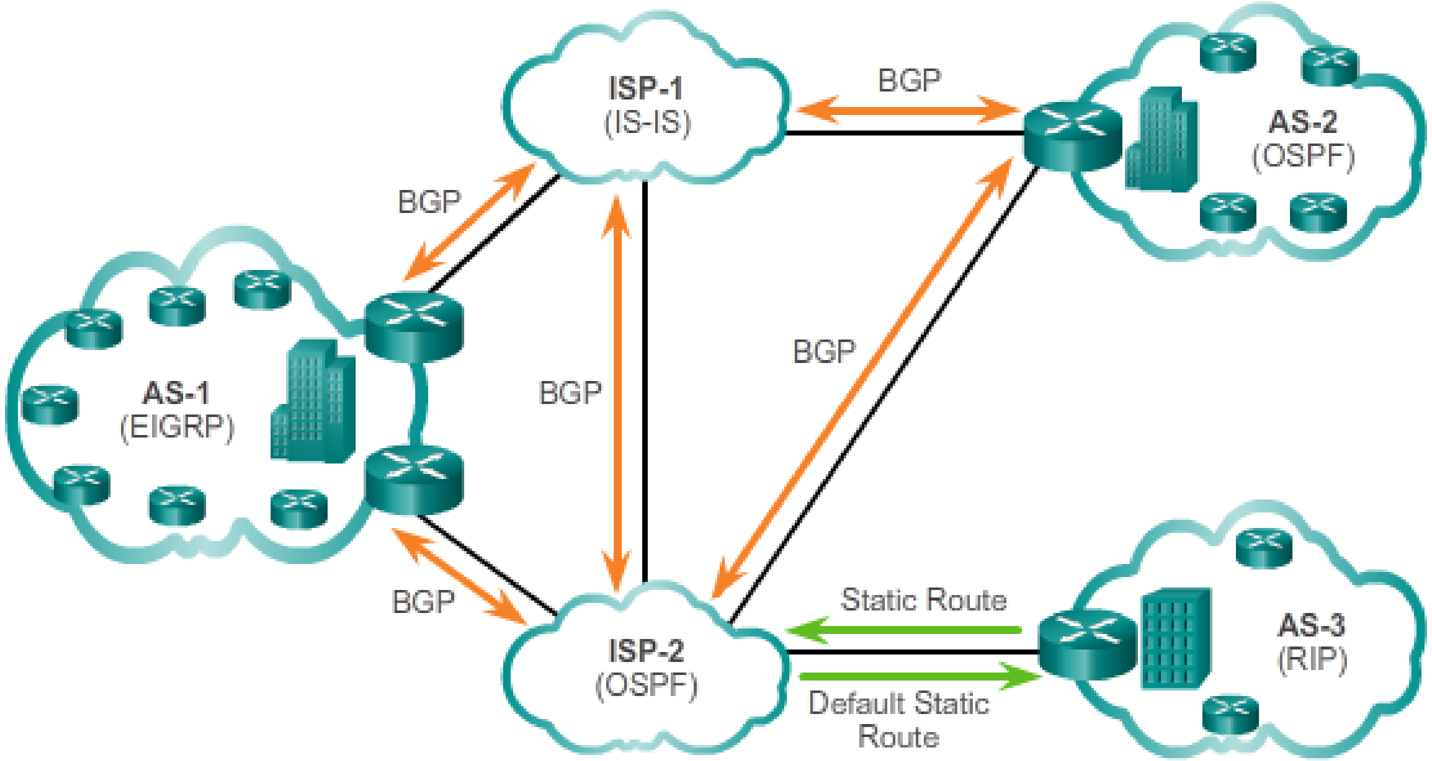
EIGRP

- Released in 1992 as a Cisco proprietary protocol.
- 2013 basic functionality of EIGRP released as an open standard.
- Advanced Distance Vector routing protocol.
- Uses the Diffusing Update Algorithm (DUAL) to calculate paths and back-up paths.
- Establishes Neighbor Adjacencies.
- Uses the Reliable Transport Protocol to provide delivery of EIGRP packets to neighbors.
- Partial and Bounded Updates. Send updates only when there is a change and only to the routers that need the information.
- Supports Equal and Unequal Cost Load Balancing.



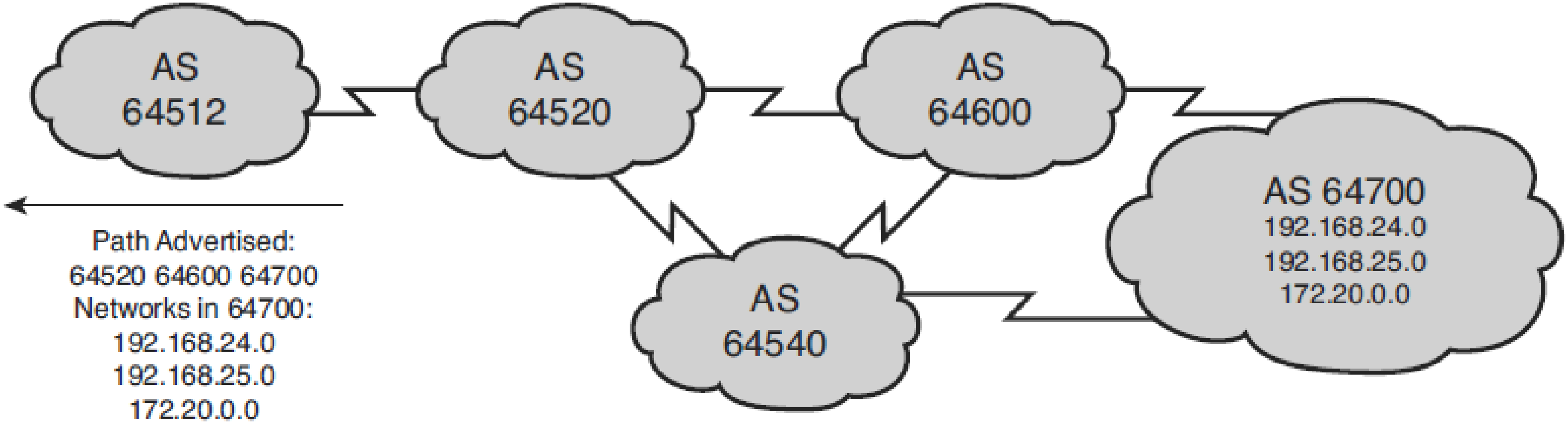
Border Gateway Protocol (BGP)

- Used to route between networks administered by two different organizations.
- In BGP, every AS is assigned a unique 16-bit or 32-bit AS number which uniquely identifies it on the Internet.
- BGP updates are encapsulated over TCP on port 179, inheriting the connection-oriented properties of TCP.



BGP – Path-Vector Protocol

The router passes to the neighbor a **list of the full AS path** (one by one) that must be traversed to reach the recipient's network.



Q&A

Thank you!