IPv4 Addressing

Dmytro Zubov, PhD
dmytro.zubov@ucentralasia.org

Naryn, 1:59pm, October 20, 2022

Lessons learnt last time

- **Configure Initial Router Settings:** Configure initial settings on an IOS Cisco router
- **Configure Interfaces:** Configure two active interfaces on a Cisco IOS router
- **Configure the Default Gateway:** Configure devices to use the default gateway

What we gonna discuss today?

- **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
- **VLSM:** Variable Length Subnet Mask
- **Route Summarization:** Route Summarization is basically advertising many routes into one route

IPv4 Address Structure

- IPv4 Address Structure

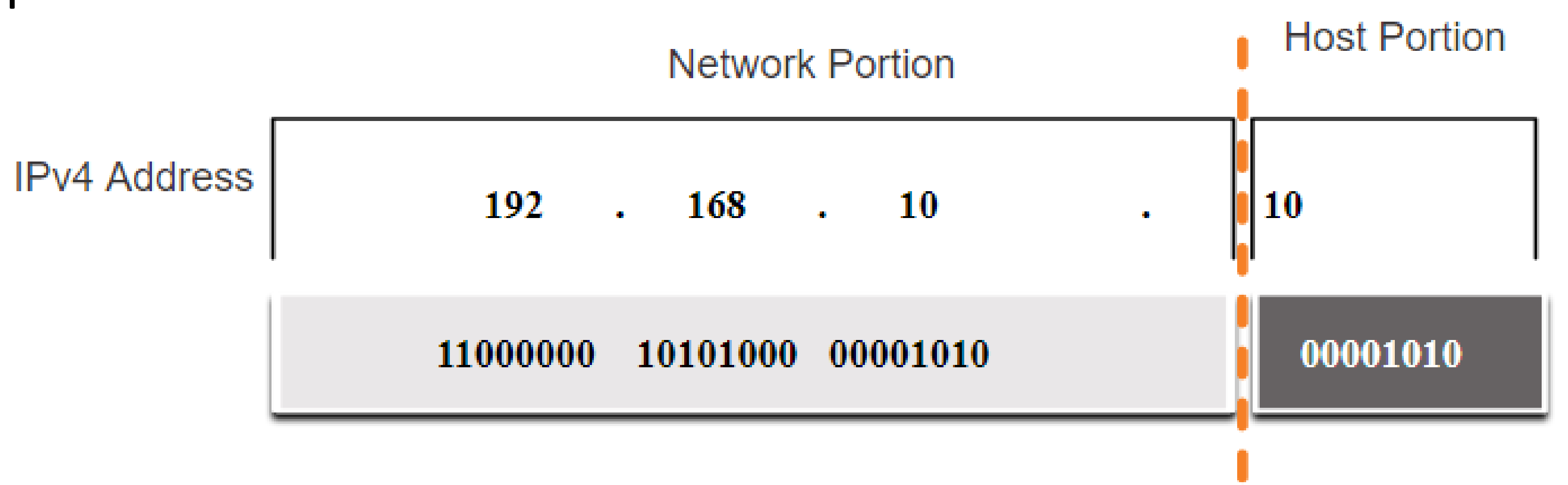
IPv4 Address Structure

- Network and Host Portions

  - An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion

  - When determining the network portion versus the host portion, we must look at the 32-bit stream

  - A subnet mask is used to determine the network and host portions

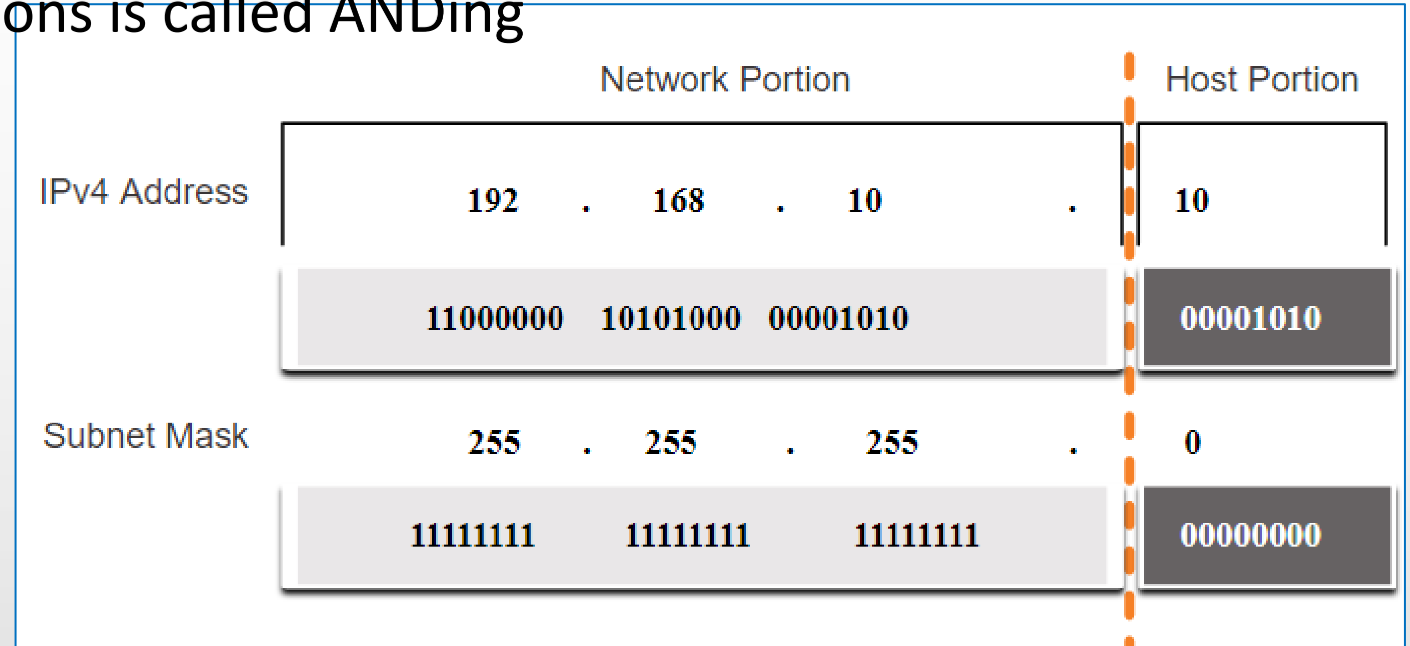


IPv4 Address Structure

- The Subnet Mask

  - To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right

  - The actual process used to identify the network and host portions is called ANDing



IPv4 Address Structure

- The Prefix Length

  - A prefix length is a method used to identify a subnet mask address

  - The prefix length is the number of bits set to 1 in the subnet mask

  - It is written in “slash notation” - count the number of bits in the subnet mask and prepend it with a slash

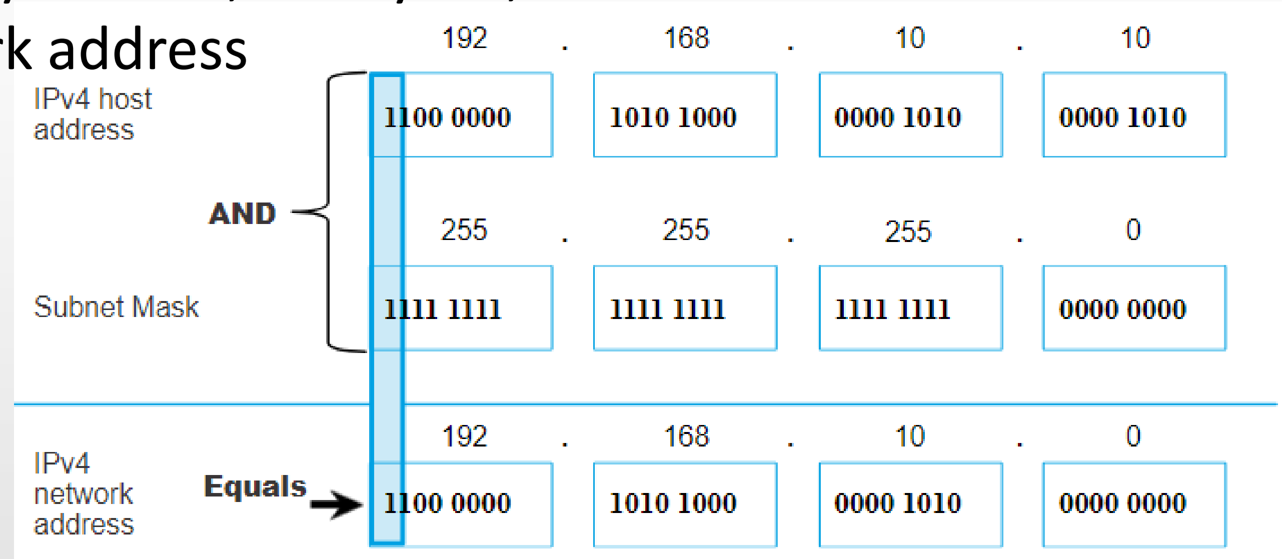
IPv4 Address Structure

- The Prefix Length (cont.)

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

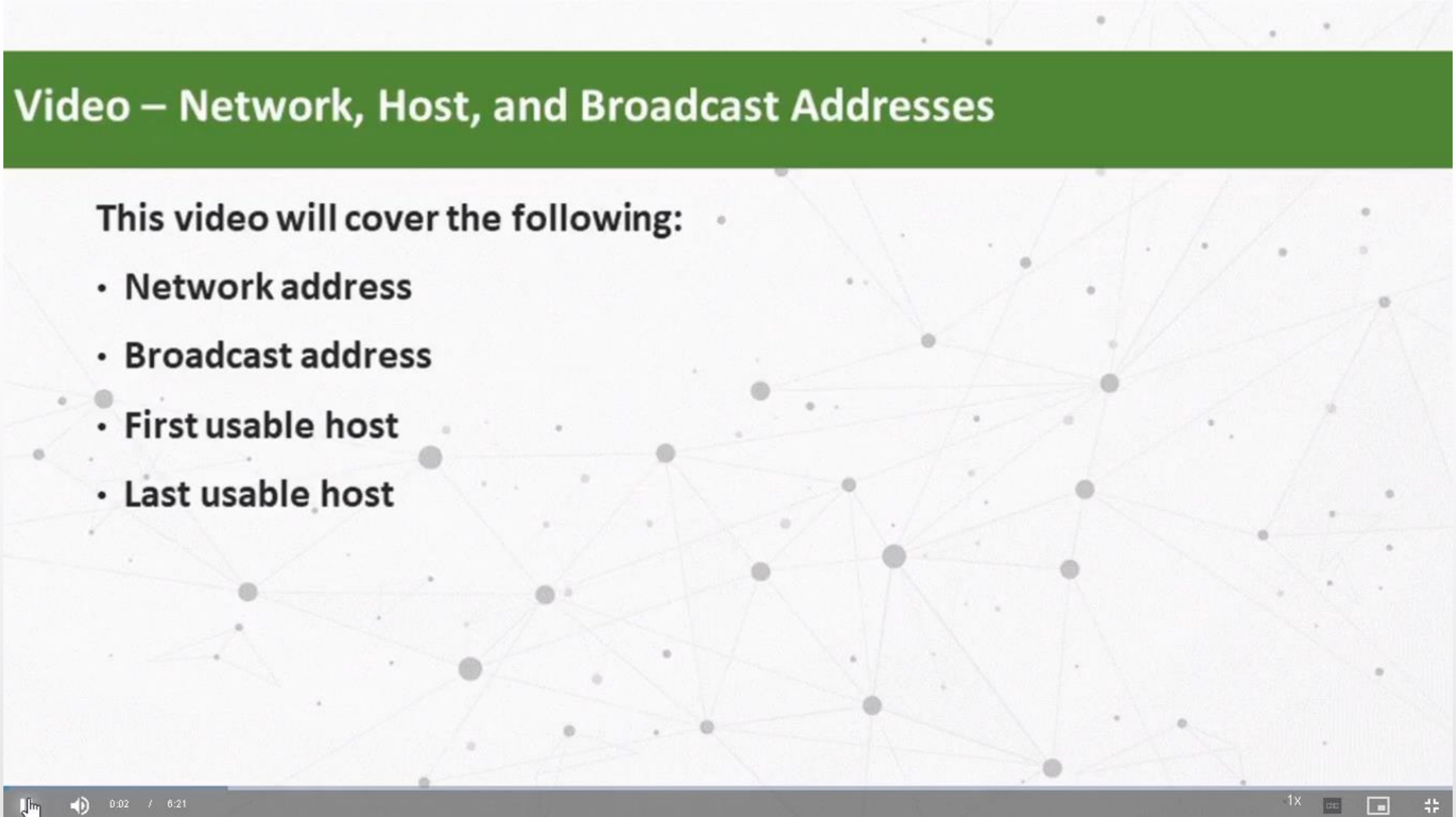
IPv4 Address Structure

- Determining the Network: Logical AND
  - A logical AND Boolean operation is used in determining the network address:
    - 1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0
    - 1 = True and 0 = False
  - To identify the network address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the network address



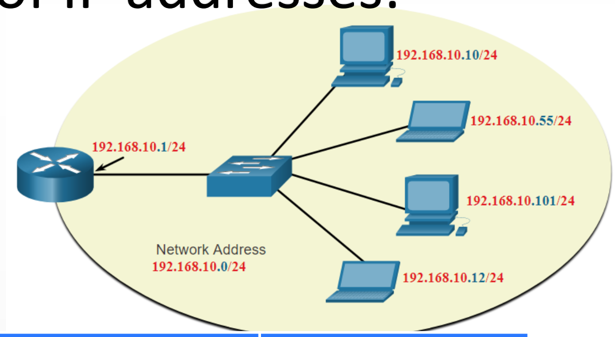
IPv4 Address Structure

- Network, Host and Broadcast Addresses



IPv4 Address Structure

- Network, Host, and Broadcast Addresses
  - Within each network, there are three types of IP addresses:
    - Network address
    - Host addresses
    - Broadcast address



	Network Portion			Host Portion	Host Bits
Subnet mask **255.255.255**.0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10**.0 or **/24**	192 11000000	168 10100000	10 00001010	0 00000000	All 0s
First address **192.168.10**.1 or **/24**	192 11000000	168 10100000	10 00001010	1 00000001	All 0s and a 1
Last address **192.168.10**.254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	All 1s and a 0
Broadcast address **192.168.10**.255 or **/24**	192 11000000	168 10100000	10 00001010	255 11111111	All 1s

IPv4 Unicast, Broadcast, and Multicast

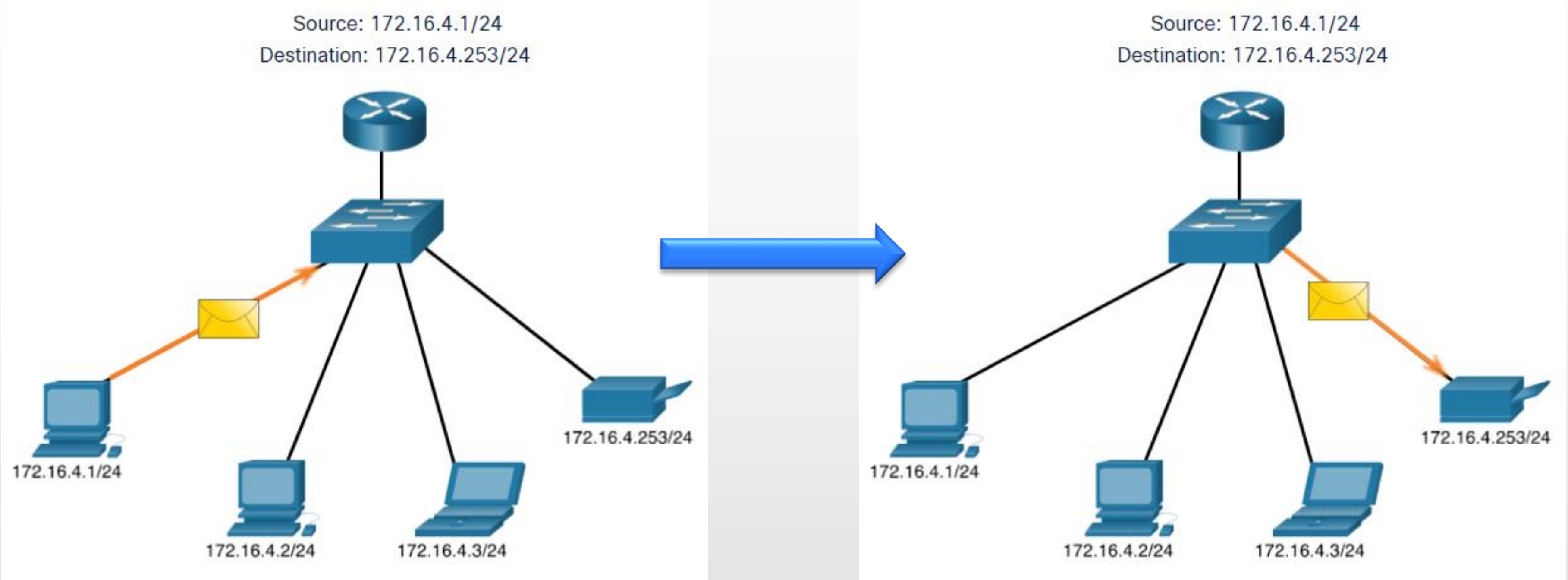
- IPv4 Unicast, Broadcast, and Multicast

IPv4 Unicast, Broadcast, and Multicast

- Unicast

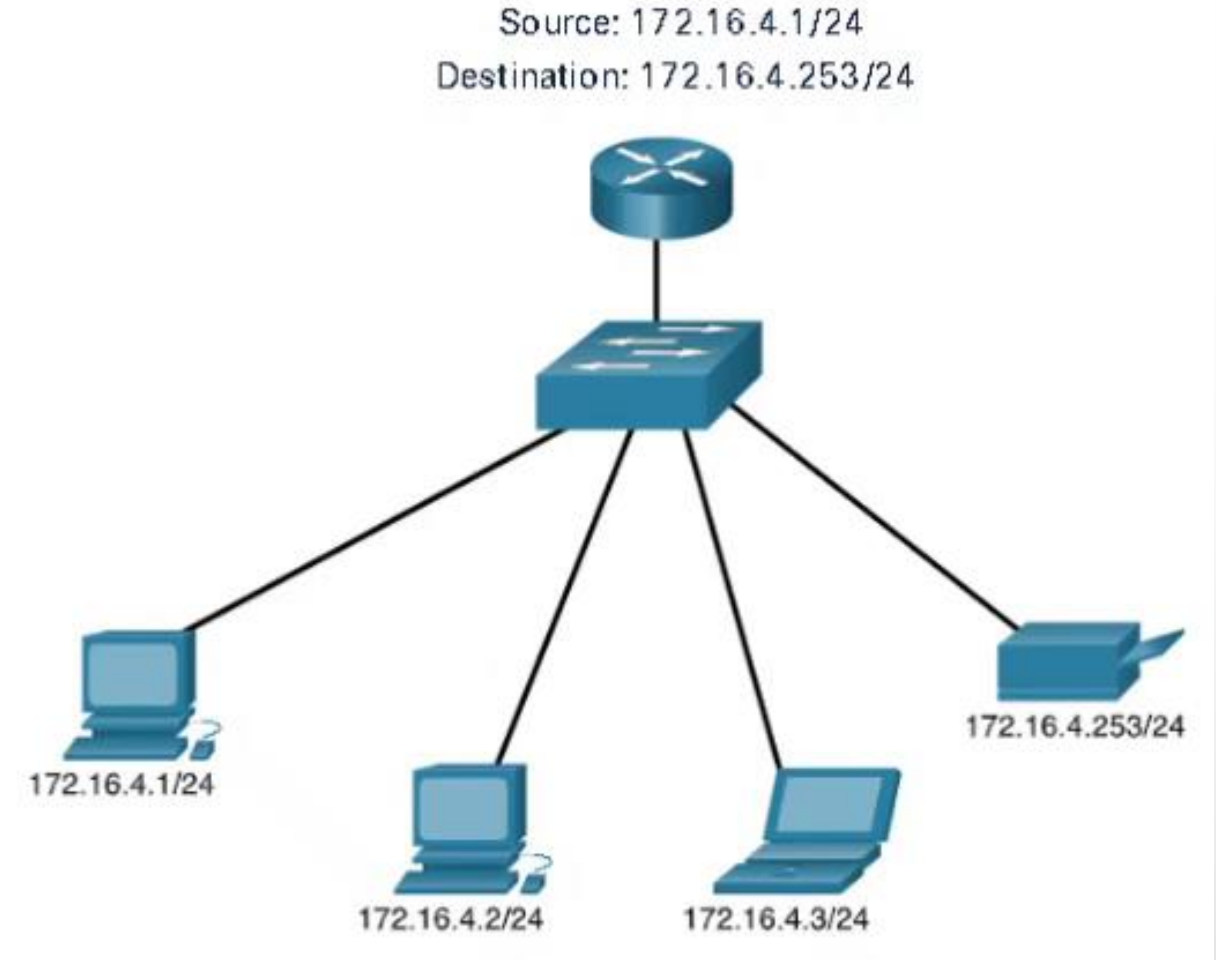
  - Unicast transmission is sending a packet to one destination IP address

  - 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

- Unicast (cont.)

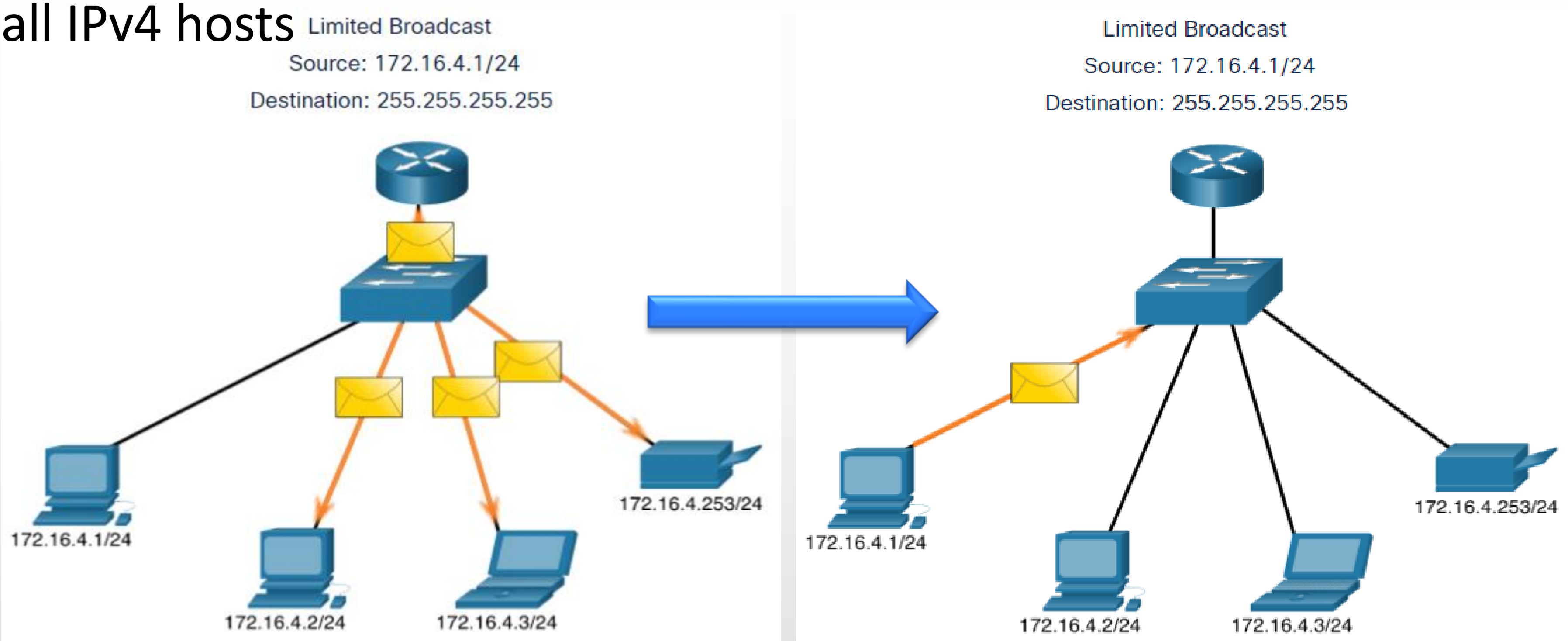


IPv4 Unicast, Broadcast, and Multicast

- Broadcast

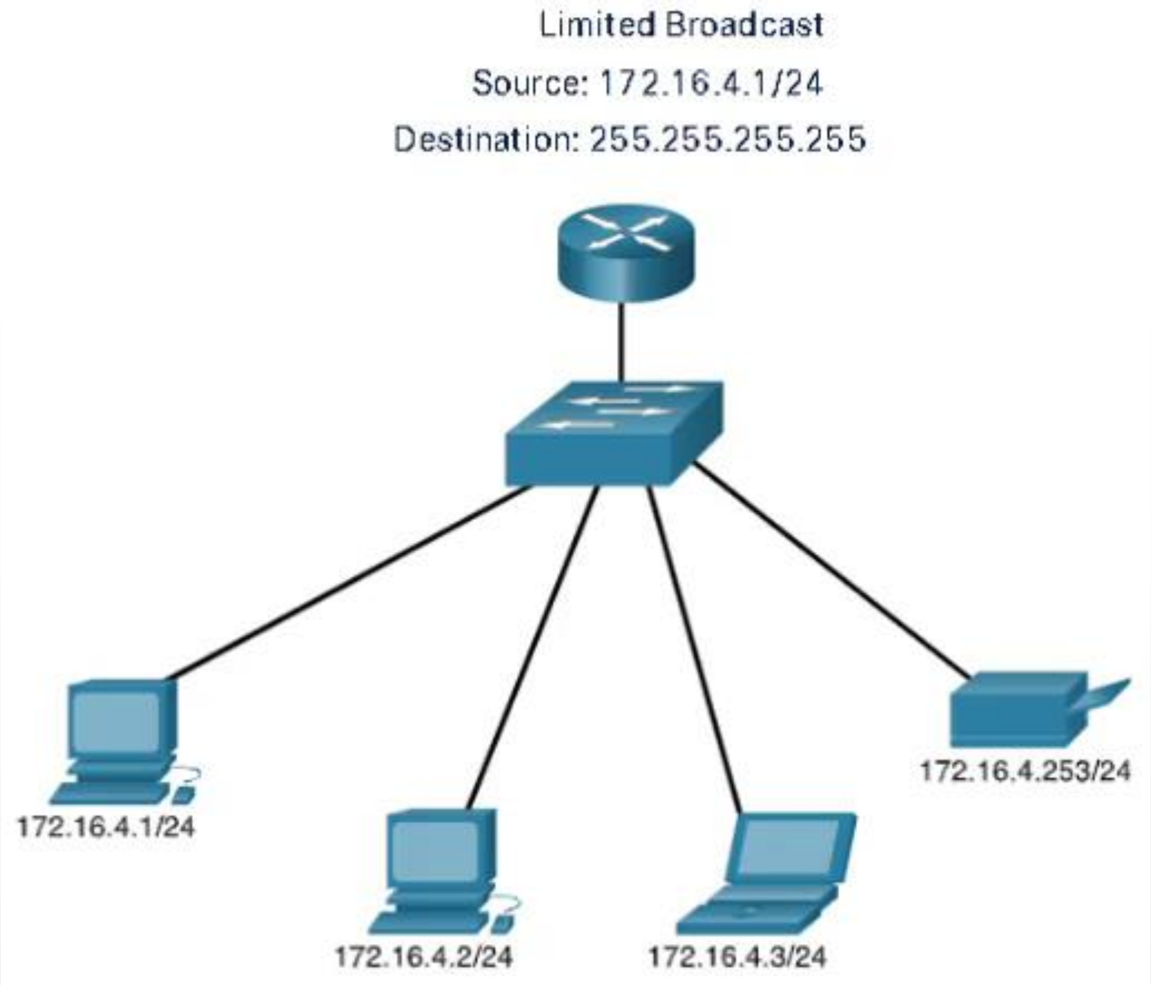
  - Broadcast transmission is sending a packet to all other destination IP addresses

  - For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts



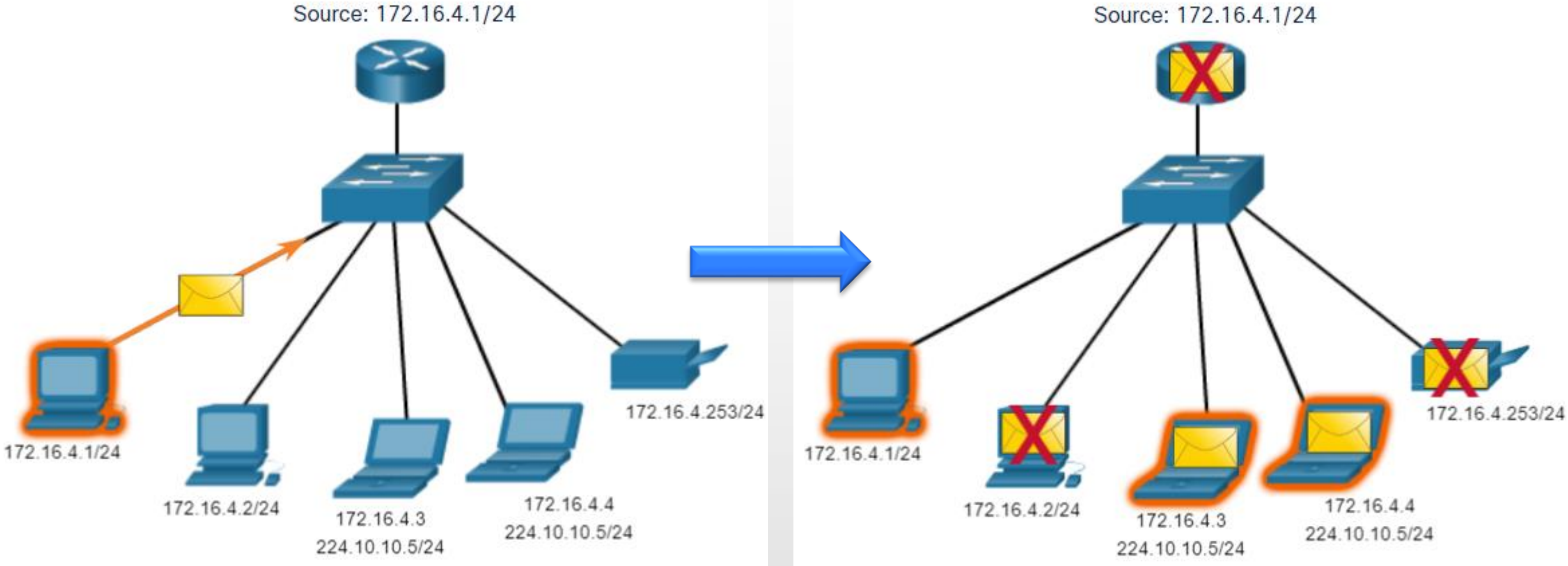
IPv4 Unicast, Broadcast, and Multicast

- Broadcast (cont.)



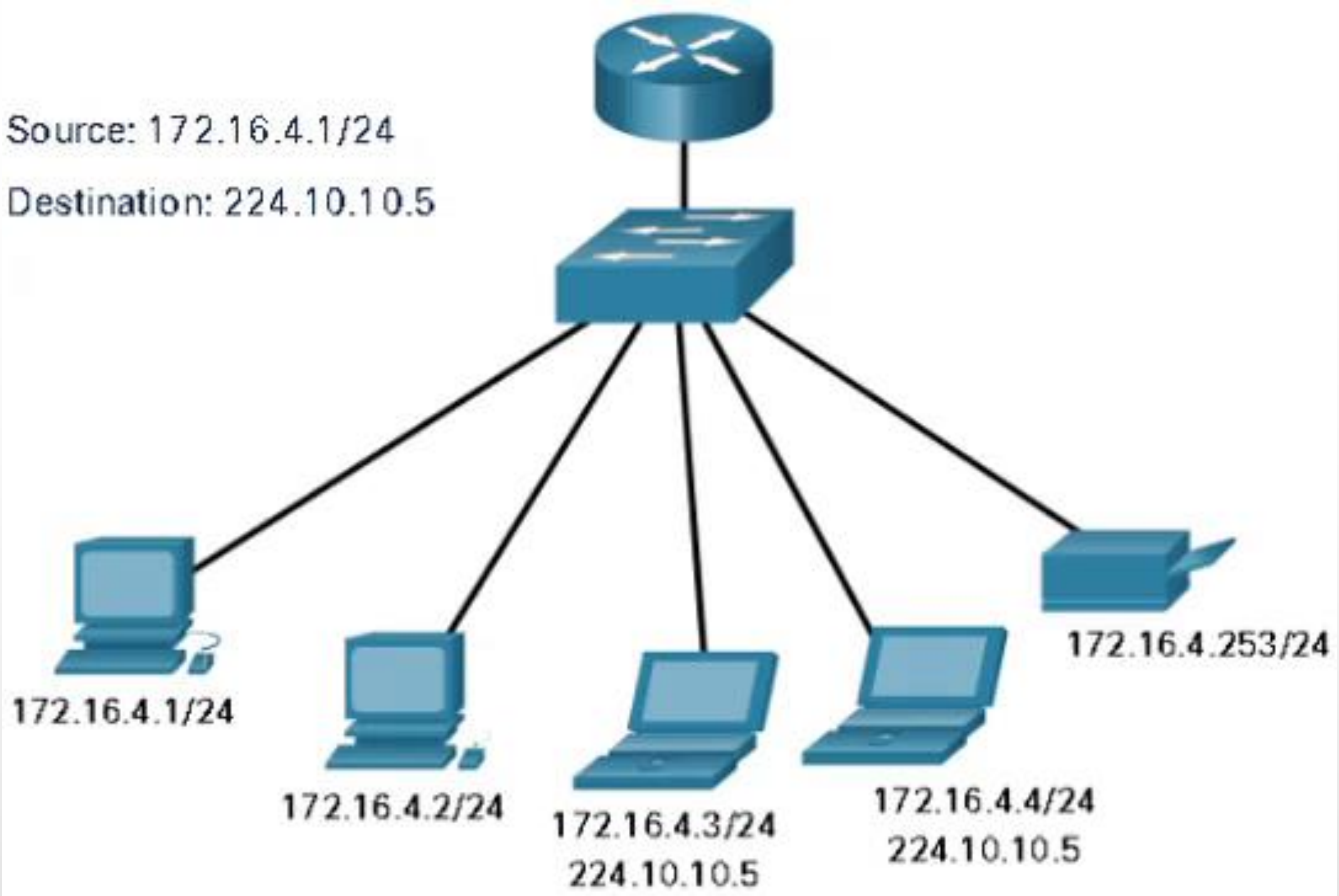
IPv4 Unicast, Broadcast, and Multicast

- 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



IPv4 Unicast, Broadcast, and Multicast

- Multicast



Types of IPv4 Addresses

- Types of IPv4 Addresses

Types of IPv4 Addresses

- Public and Private IPv4 Addresses

  - As defined in RFC 1918, **public IPv4 addresses** are globally routed between internet service provider (ISP) routers

  - **Private addresses** are common blocks of addresses used by most organizations to assign IPv4 addresses to internal hosts

  - Private IPv4 addresses are not unique and can be used internally within any network

  - However, private addresses are not globally routable

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

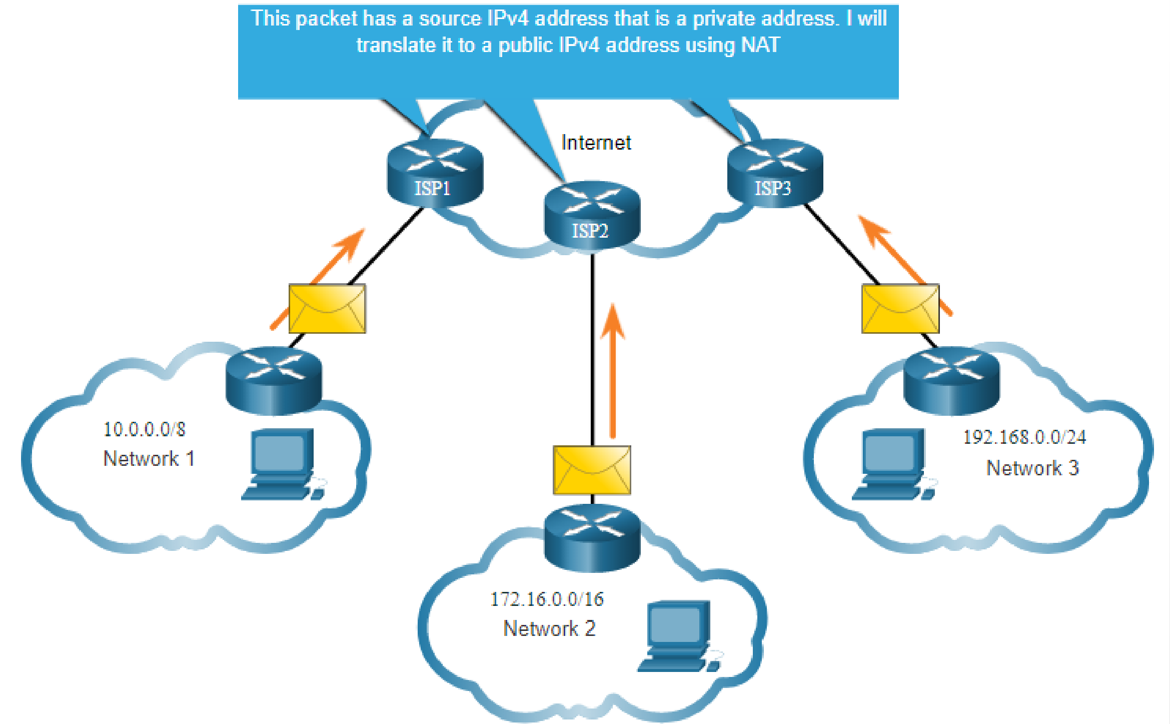
Types of IPv4 Addresses

- Routing to the Internet

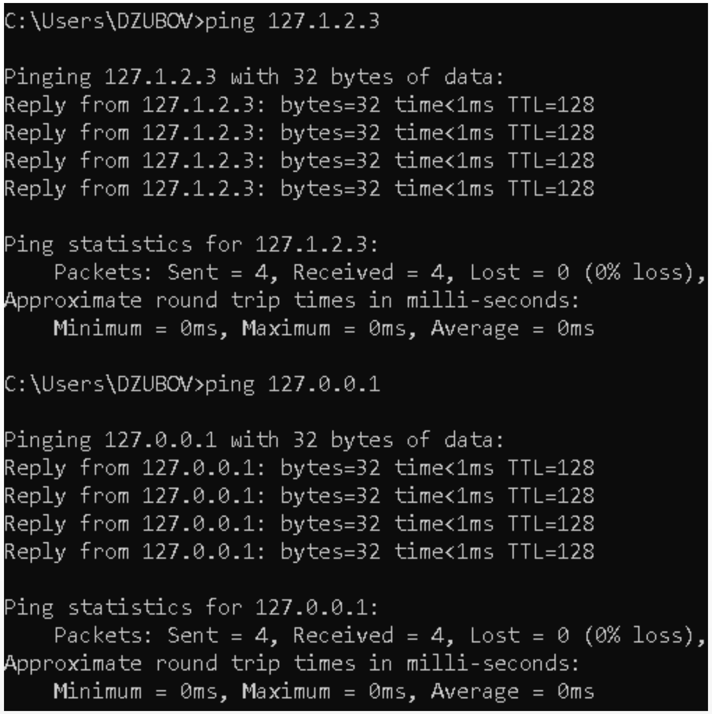
  - Network Address Translation (NAT) translates private IPv4 addresses to public IPv4 addresses

  - NAT is typically enabled on the edge router connecting to the internet

  - It translates the internal private address to a public global IP address



Types of IPv4 Addresses



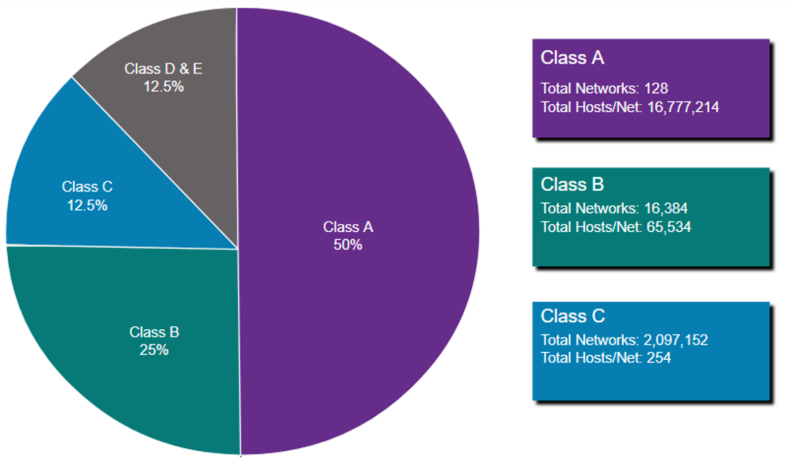
- Special Use IPv4 Addresses
  - Loopback addresses
    - 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
    - Commonly identified as only 127.0.0.1
    - Used on a host to test if TCP/IP is operational
  - Link-Local addresses
    - 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
    - Commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses
    - Used by Windows DHCP clients to self-configure when no DHCP servers are available

Types of IPv4 Addresses

- Legacy Classful Addressing

  - RFC 790 (1981) allocated IPv4 addresses in classes

    - Class A (0.0.0.0/8 to 127.0.0.0/8)
    - Class B (128.0.0.0 /16 – 191.255.0.0 /16)
    - Class C (192.0.0.0 /24 – 223.255.255.0 /24)
    - Class D (224.0.0.0 to 239.0.0.0)
    - Class E (240.0.0.0 – 255.0.0.0)



- <u>**Classful addressing wasted many IPv4 addresses**</u>

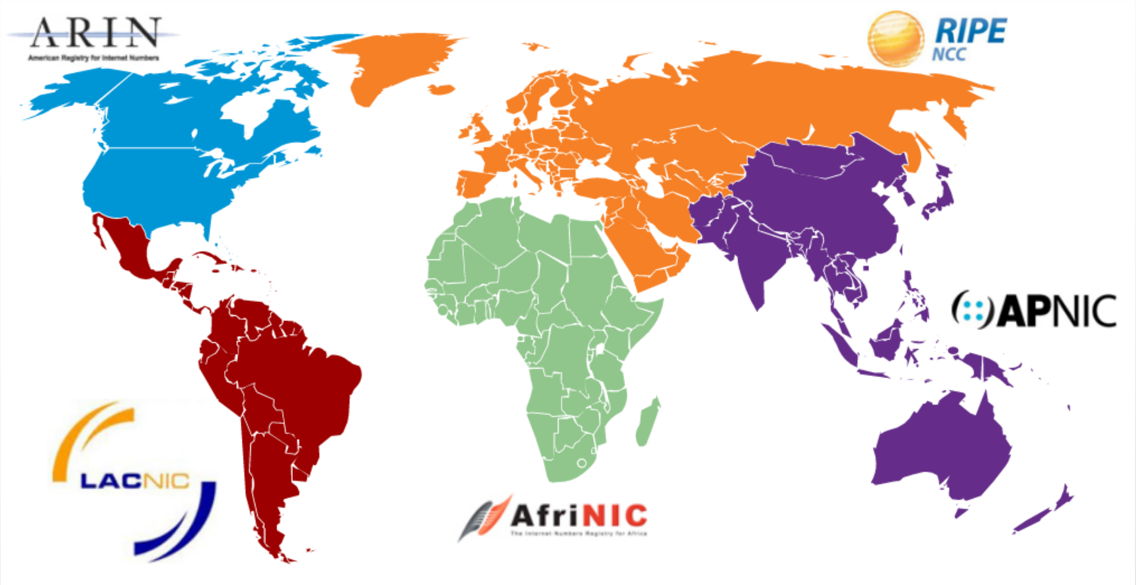
  - Classful address allocation was replaced with classless addressing which ignores the rules of classes (A, B, C)

Types of IPv4 Addresses

- Assignment of IP Addresses

  - The Internet Assigned Numbers Authority (IANA) manages and allocates blocks of IPv4 and IPv6 addresses to five Regional Internet Registries (RIRs)

  - RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to smaller ISPs and organizations



Network Segmentation

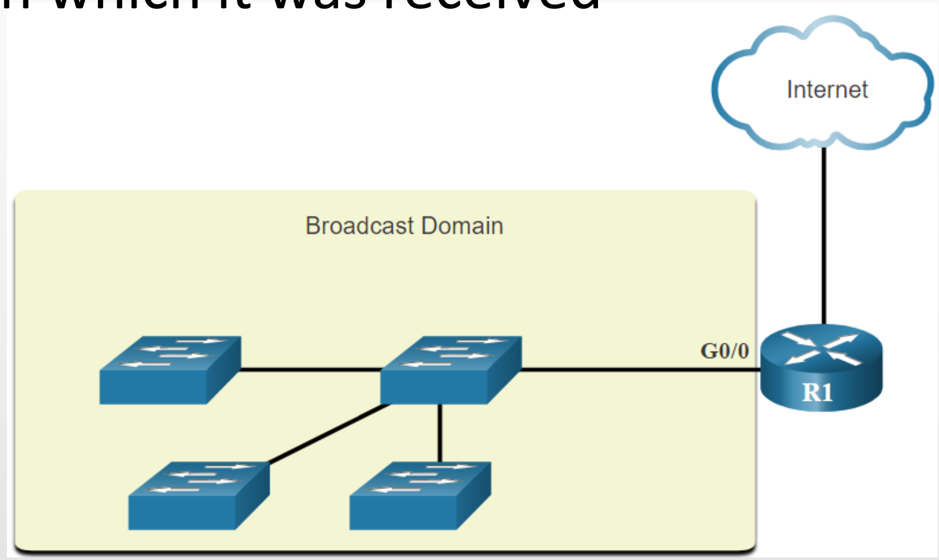
- Network Segmentation

Network Segmentation

- Broadcast Domains and Segmentation

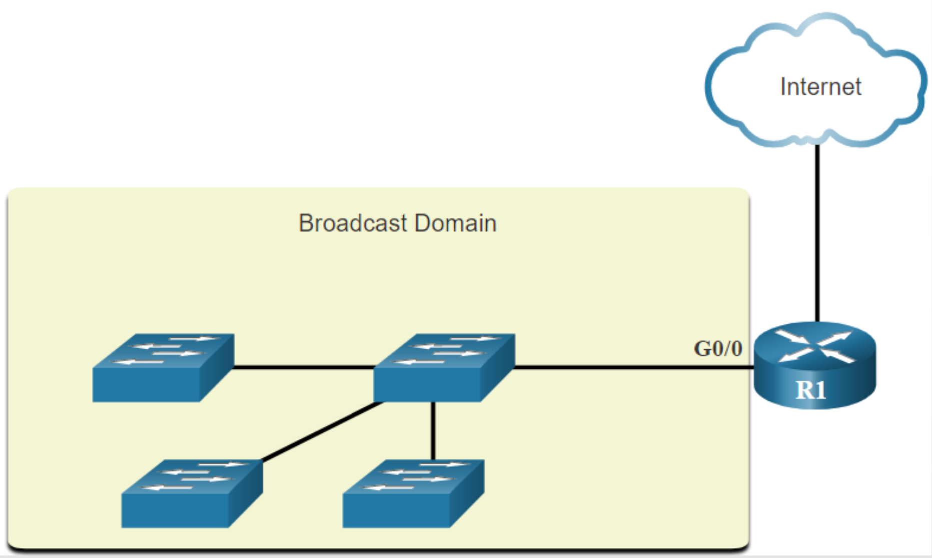
  - Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server)

  - Switches propagate broadcasts out all interfaces except the interface on which it was received



Network Segmentation

- Broadcast Domains and Segmentation (cont.)
  - 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



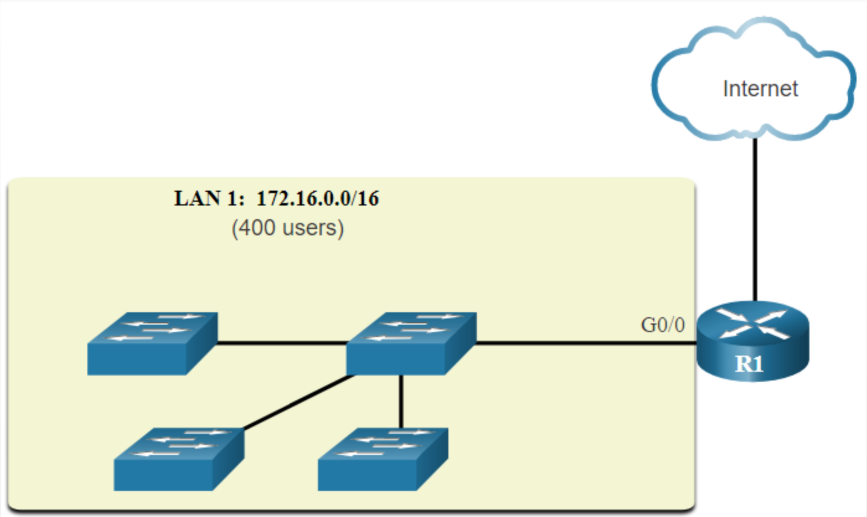
Network Segmentation

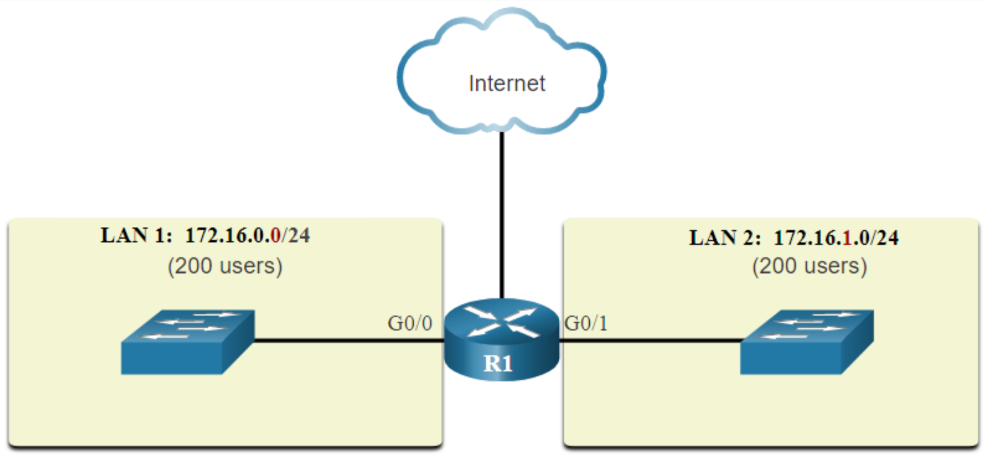
- Problems with Large Broadcast Domains

  - 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:

    - For example, 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

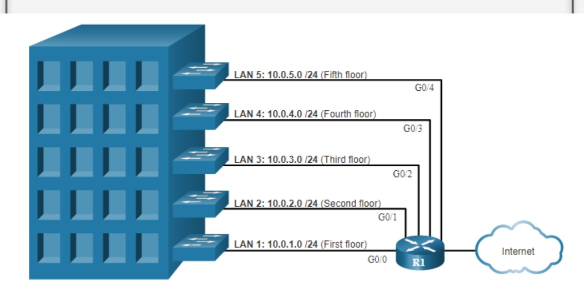




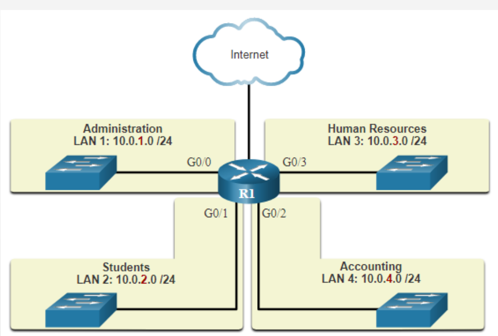
Network Segmentation

- 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:

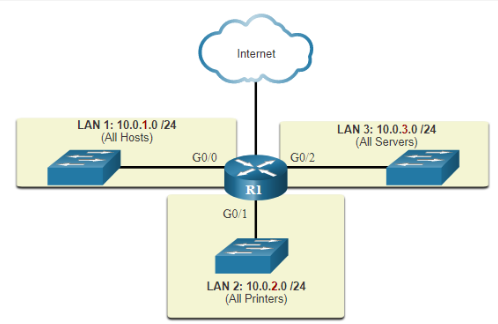
Location



Group or Function



Device Type



Subnet an IPv4 Network

- Subnet an IPv4 Network

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 an IPv4 Network

- Subnet on an Octet Boundary (cont.)

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

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 - **10.2255.255**.254	**10.255.255**.255

Subnet an IPv4 Network

- 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	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Subnet an IPv4 Network

- The Subnet Mask

Video – The Subnet Mask

This video will demonstrate the process of subnetting.

Subnet a Slash 16 and a Slash 8 Prefix

- Subnet a Slash 16 and a Slash 8 Prefix

Subnet a Slash 16 and a Slash 8 Prefix

- Create Subnets with a Slash 16 prefix
  - The table highlights all the possible scenarios for subnetting a /16 prefix

Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.**128**.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.**192**.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.**224**.0	nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh 11111111.11111111.**111**00000.00000000	**8**	8190
/20	255.255.**240**.0	nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh 11111111.11111111.**1111**0000.00000000	**16**	4094
/21	255.255.**248**.0	nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh 11111111.11111111.**11111**000.00000000	**32**	2046
/22	255.255.**252**.0	nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh 11111111.11111111.**111111**00.00000000	**64**	1022
/23	255.255.**254**.0	nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh 11111111.11111111.**1111111**0.00000000	**128**	510
/24	255.255.**255.0**	nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh 11111111.11111111.**11111111**.00000000	**256**	254
/25	255.255.**255.128**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh 11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.**255.192**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh 11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.**255.224**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh 11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.**255.240**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh 11111111.11111111.**11111111.1111**0000	**4096**	14
/29	255.255.**255.248**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh 11111111.11111111.**11111111.11111**000	**8192**	6
/30	255.255.**255.252**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh 11111111.11111111.**11111111.111111**00	**16384**	2

Subnet a Slash 16 and a Slash 8 Prefix

Create 100 Subnets with a slash 16 prefix

- Consider a large enterprise that requires at least 100 subnets and has chosen the private address 172.16.0.0/16 as its internal network address

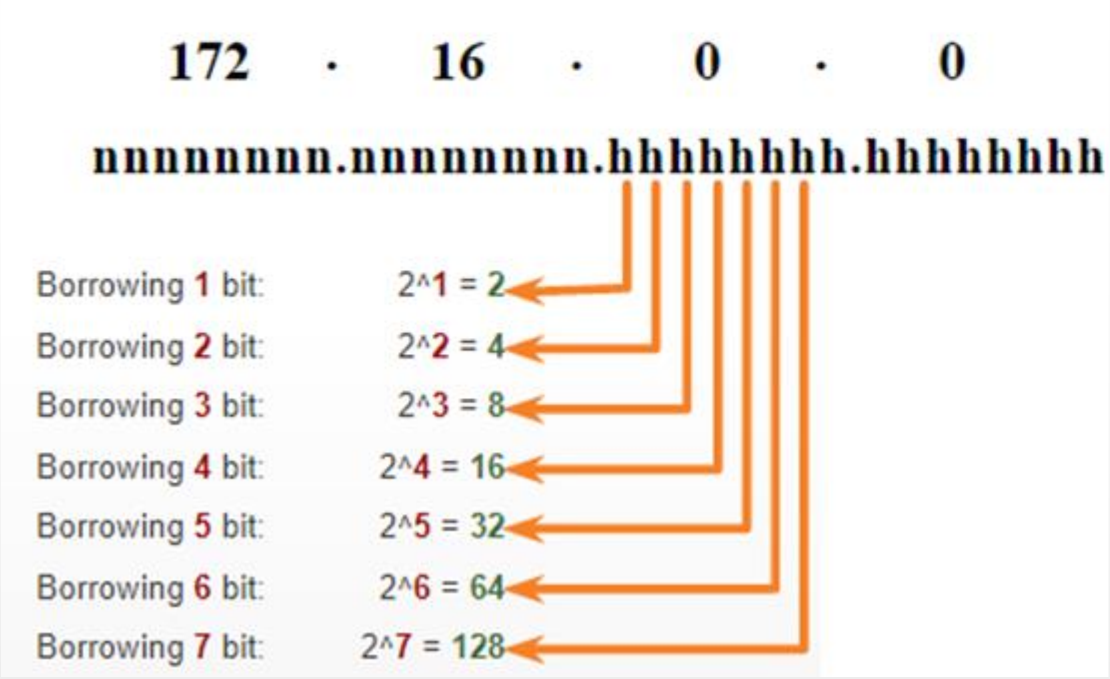
  - The figure displays the number of subnets that can be created when borrowing bits from the third octet and the fourth octet

  - Notice there are now up to 14 host bits that can be borrowed (i.e., last two bits cannot be borrowed)

- To satisfy the requirement of 100 subnets for the enterprise, 7 bits (i.e., $2^7 = 128$ subnets) would need to be borrowed (for a total of 128 subnets)

Subnet a Slash 16 and a Slash 8 Prefix

Create 100 Subnets with a slash 16 prefix



Subnet a Slash 16 and a Slash 8 Prefix

Create 1000 Subnets with a Slash 8 prefix

- Consider a small ISP that requires 1000 subnets for its clients using network address 10.0.0.0/8 which means there are 8 bits in the network portion and 24 host bits available to borrow toward subnetting
  - The figure displays the number of subnets that can be created when borrowing bits from the second and third.
  - Notice there are now up to 22 host bits that can be borrowed (i.e., last two bits cannot be borrowed)
- To satisfy the requirement of 1000 subnets for the enterprise, 10 bits (i.e., 210=1024 subnets) would need to be borrowed (for a total of 128 subnets)

Subnet a Slash 16 and a Slash 8 Prefix

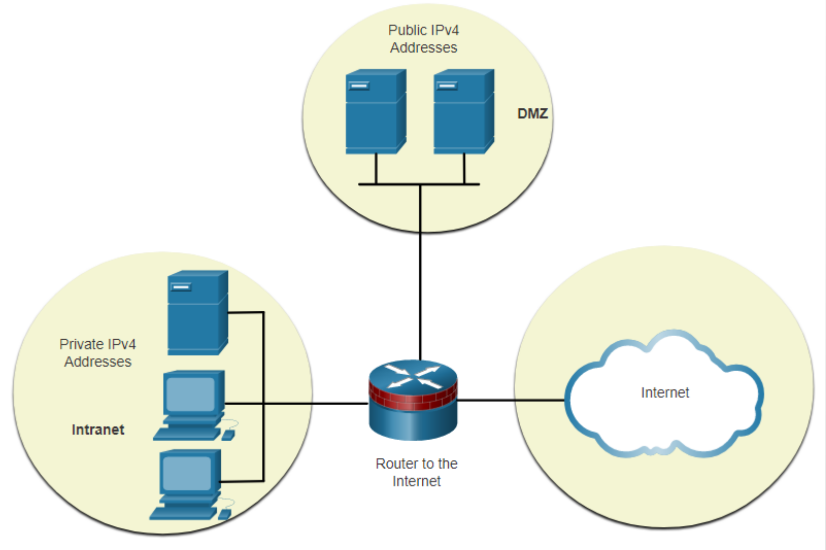
Create 1000 Subnets with a slash 8 prefix

Subnet to Meet Requirements

- Subnet to Meet Requirements

Subnet to Meet Requirements

- Subnet Private versus Public IPv4 Address Space
  - Enterprise networks will have an:
    - Intranet - A company's internal network typically using private IPv4 addresses
    - DMZ (demilitarized zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. Devices in the DMZ use public IPv4 addresses.
    - A company could use the 10.0.0.0/8 and subnet on the /16 or /24 network boundary
    - The DMZ devices would have to be configured with public IP addresses



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	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

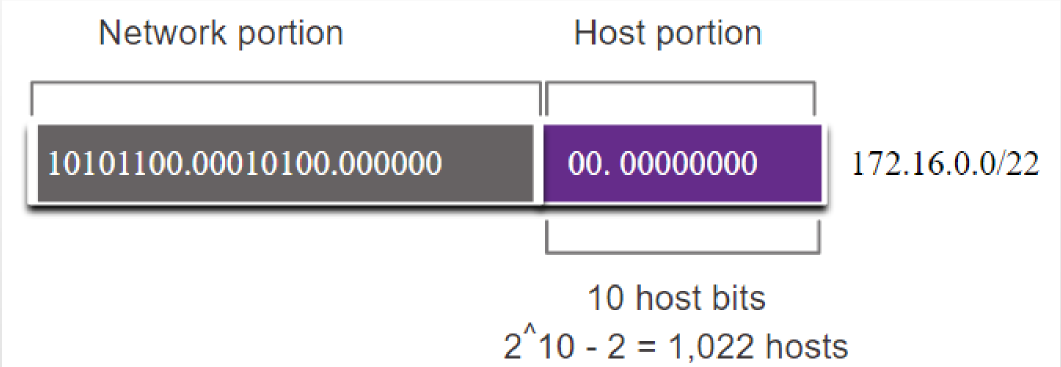
Subnet to Meet Requirements

- Example: Efficient IPv4 Subnetting

  - In this example, corporate headquarters has been allocated a public network address of 172.16.0.0/22 (10 host bits) by its ISP providing 1022 host addresses.

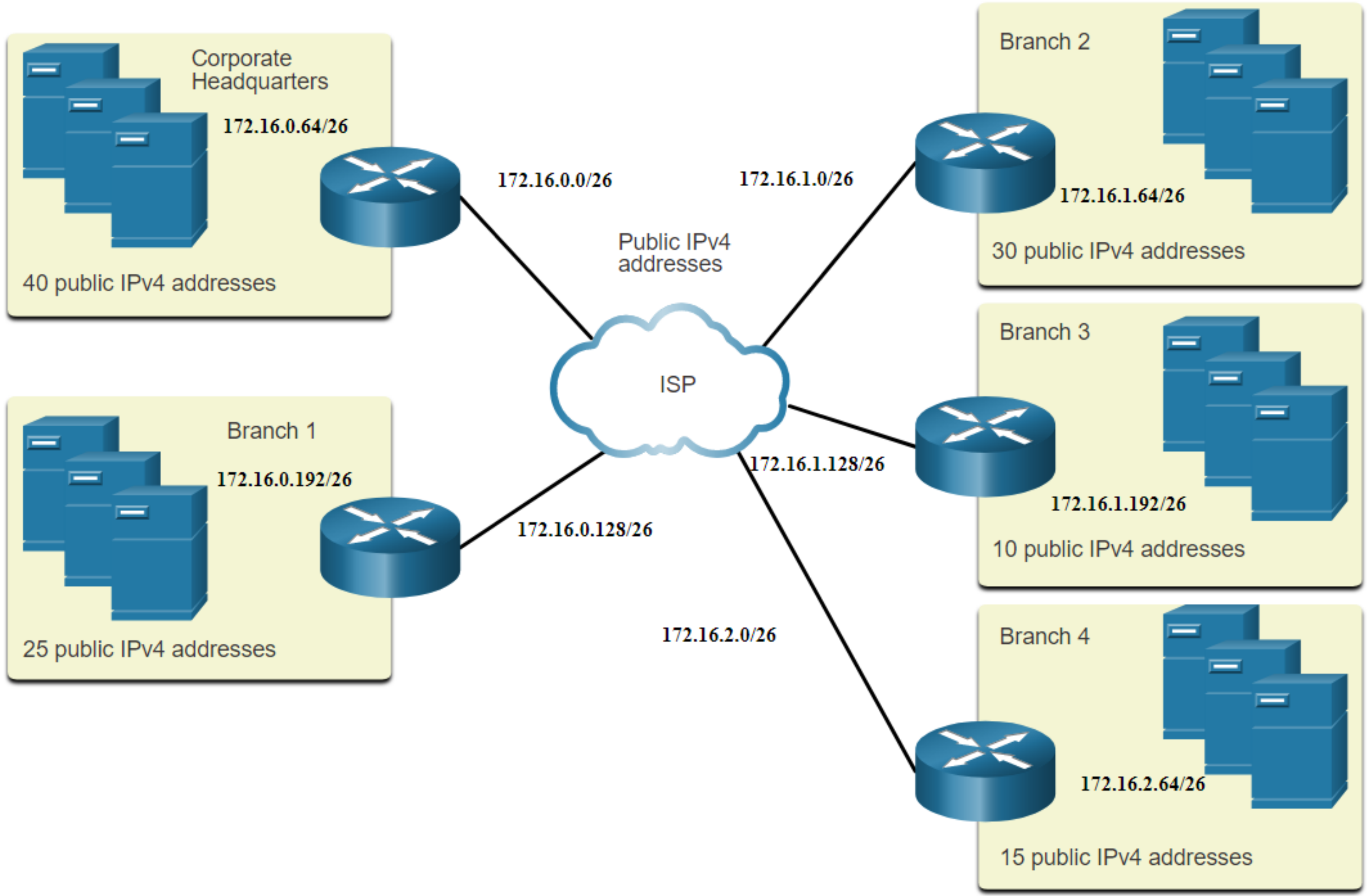
  - There are five sites (i.e., five LANs) and therefore five internet connections (i.e., LANs are connected to the internet) which means the organization requires 10 subnets with the largest subnet requires 40 addresses.

  - It allocated 10 subnets with a /26 (i.e., 255.255.255.192) subnet mask



Subnet to Meet Requirements

- Example: Efficient IPv4 Subnetting (cont.)



VLSM

- VLSM (Variable Length Subnet Mask)

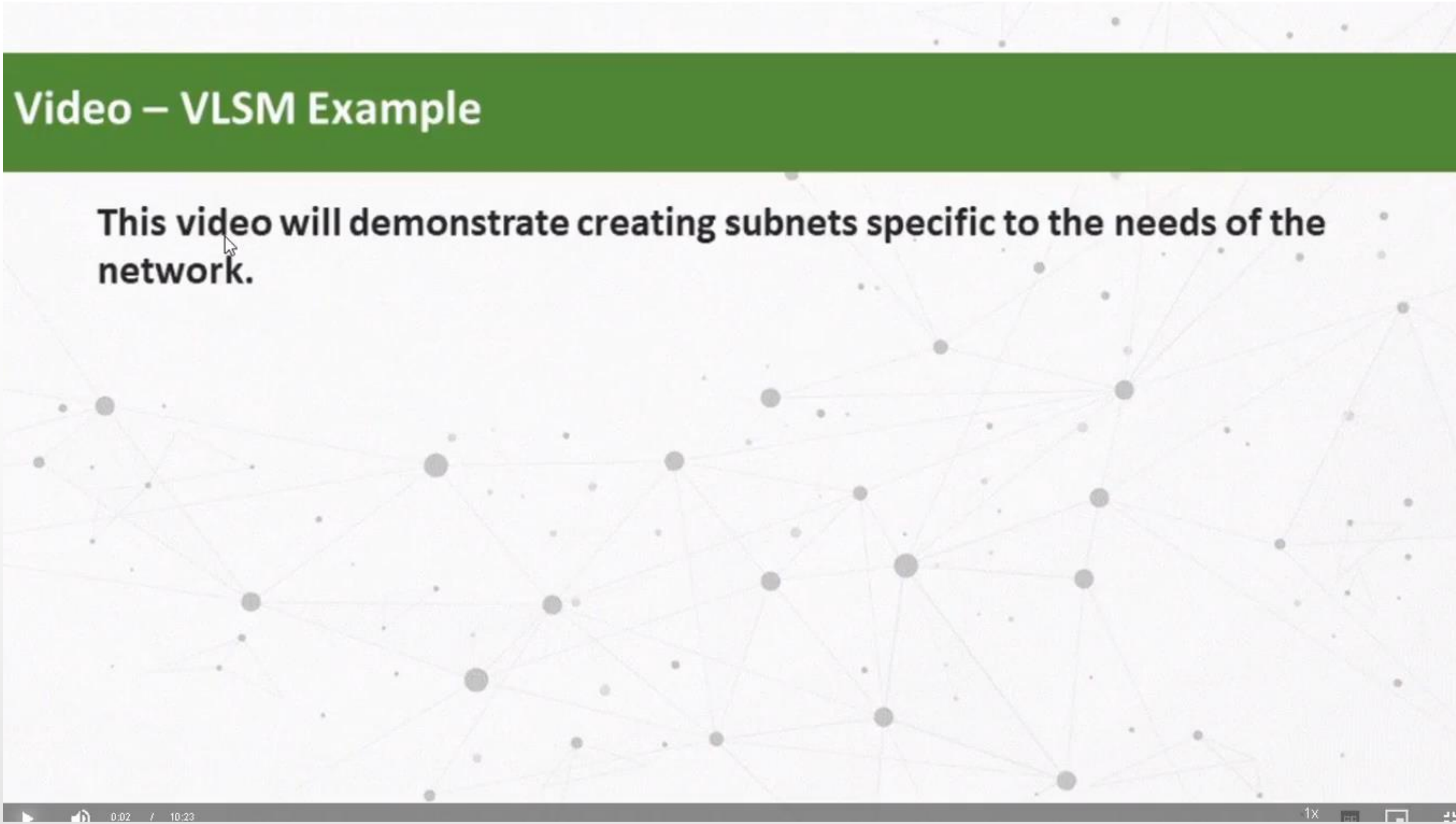
VLSM

- VLSM


Video – VLSM Basics
This video will explain VLSM basics.
0:02 / 2:31
1X

VLSM

- VLSM Example

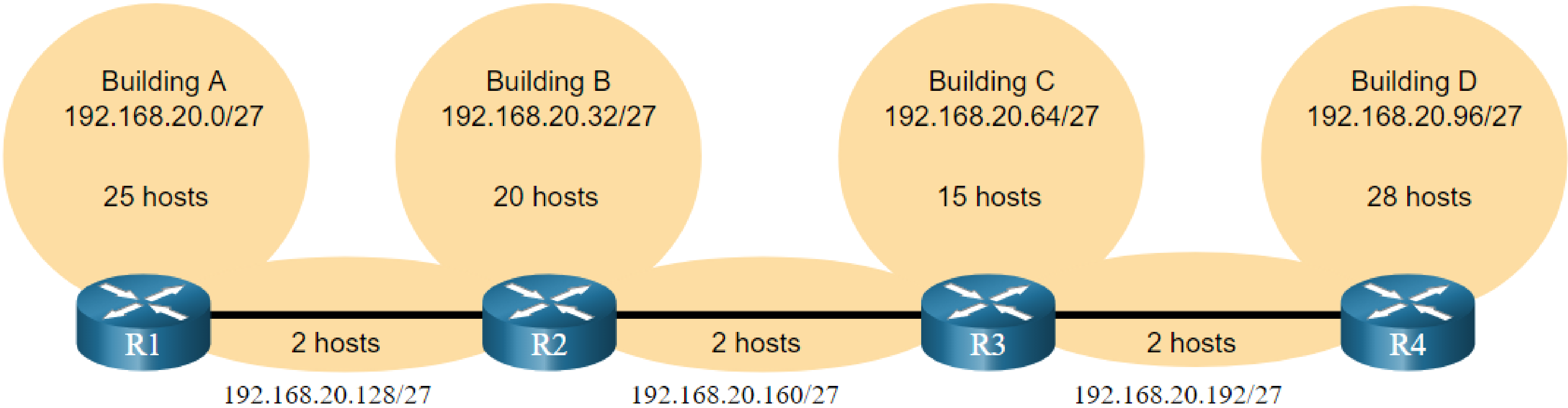


VLSM

- IPv4 Address Conservation

  - Given the topology, 7 subnets are required (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



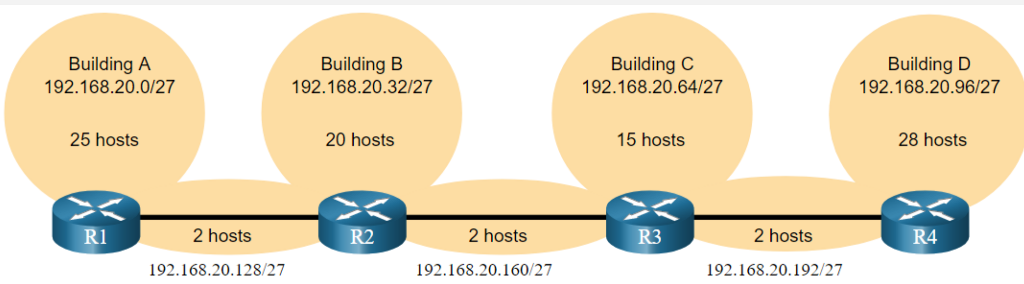
VLSM

- 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

  - 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



Host portion
2^5 – 2 = 30 host IP addresses per subnet

30 – 2 = 28
Each WAN subnet wastes 28 addresses

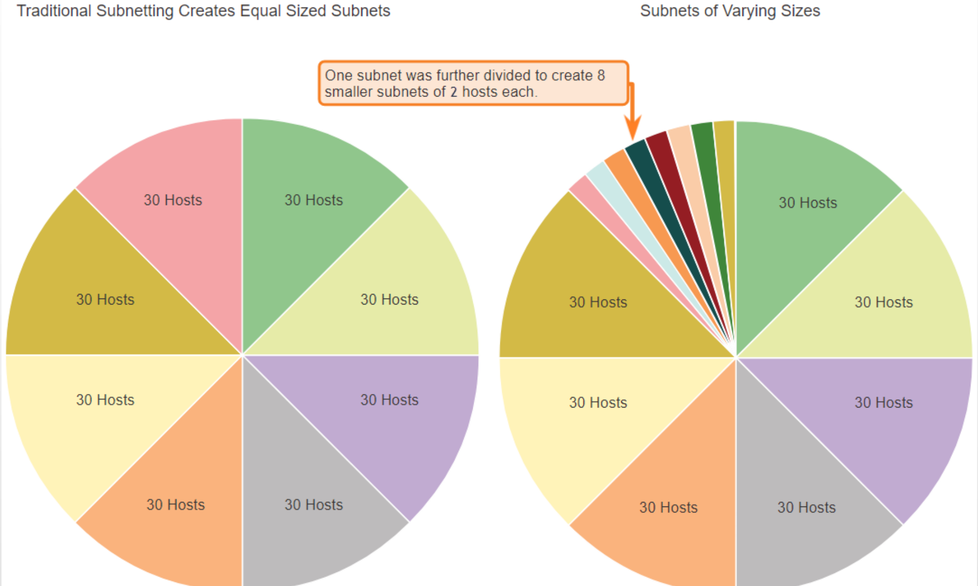
28 x 3 = 84
84 addresses are unused

VLSM

- VLSM

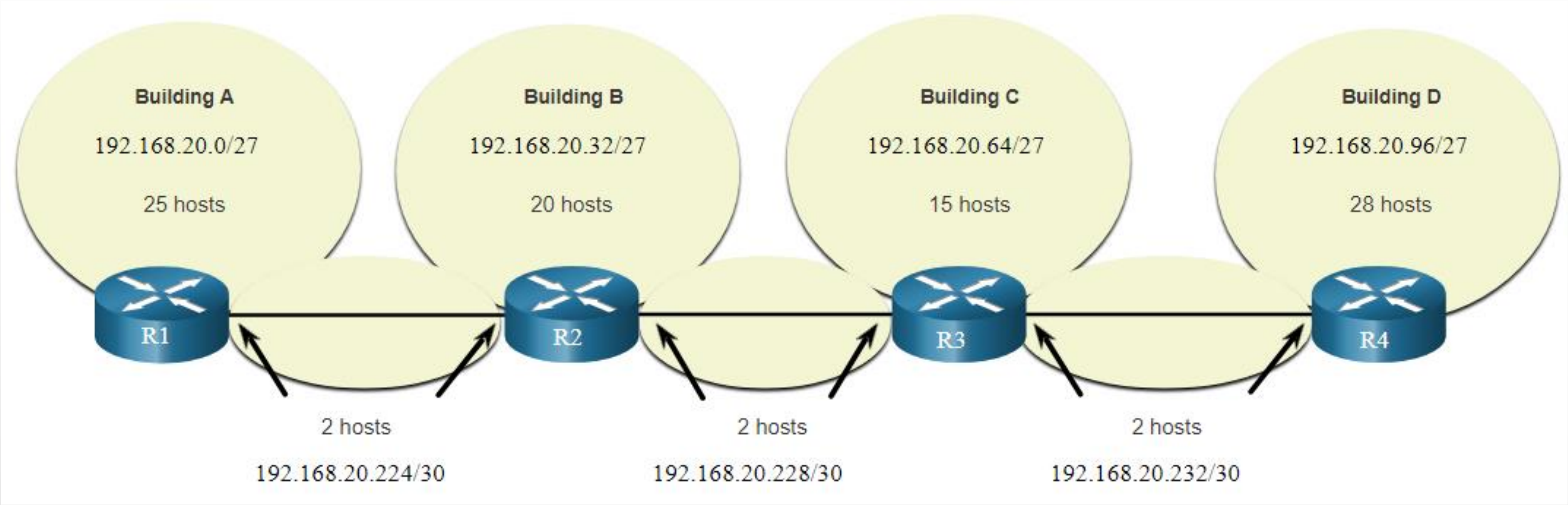
  - The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how VLSM can be used to subnet a subnet and divided the last subnet into eight /30 subnets

  - 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



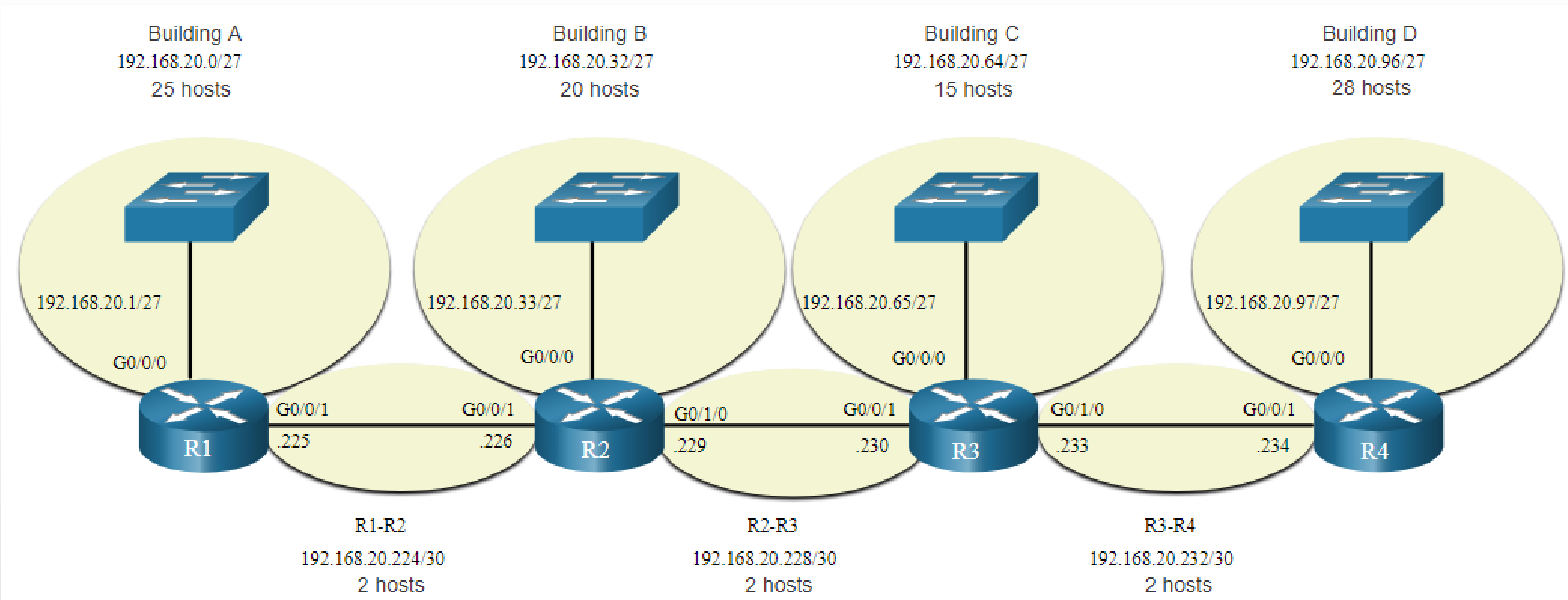
VLSM

- VLSM (cont.)
  - The resulting topology with VLSM applied:



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



VLSM

- VLSM: An example

  - We design a network with three subnets: A (100 hosts), B (200 hosts), and C (17 hosts). The network address of the largest network is 192.168.0.0.

  - Descending sort of networks and finding prefixes:

  B (200 hosts): /24 (2^8-2=254)

  A (100 hosts): /25 (2^7-2=126)

  C (17 hosts): /27 (2^5-2=30)

Network B:	**192.168.00000000**.00000000	Network address (192.168.0.0)
	192.168.00000000.11111111	Broadcast address (192.168.0.255)
Network A:	**192.168.00000001.0**0000000	Network address (192.168.1.0)
	192.168.00000001.01111111	Broadcast address (192.168.1.127)
Network C:	**192.168.00000001.100**00000	Network address (192.168.1.128)
	192.168.00000001.10011111	Broadcast address (192.168.1.159)

VLSM

- VLSM: One more example

  - We design a network with three subnets: A (50 hosts), B (600 hosts), and C (1200 hosts). The network address of the largest network is 192.168.0.0.

  - Descending sort of networks and finding prefixes:

  C (1200 hosts): /21 (2^{11}-2=2046)

  B (600 hosts): /22 (2^{10}-2=1022)

  A (50 hosts): /27 (2^{6}-2=62)

Network C:	**<u>192.168.00000</u>**000.00000000	Network address (192.168.0.0)
	<u>192.168.00000</u>111.11111111	Broadcast address (192.168.7.255)
Network B:	**<u>192.168.00001</u>0**00.00000000	Network address (192.168.8.0)
	<u>192.168.00001</u>011.11111111	Broadcast address (192.168.11.255)
Network A:	**<u>192.168.00001100.00</u>**000000	Network address (192.168.12.0)
	<u>192.168.00001100.00</u>111111	Broadcast address (192.168.12.63)

Structured Design

- Structured Design

Structured Design

- IPv4 Network Address Planning
  - IP network planning is crucial to develop a scalable solution to an enterprise network
    - To develop an IPv4 network wide addressing scheme, we need to know how many subnets are needed, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of our network use private addresses, and which use public, and many other determining factors
  - Examine the needs of an organization’s network usage and how the subnets will be structured.
    - Perform a network requirement study by looking at the entire network to determining how each area will be segmented
    - Determine how many subnets are needed and how many hosts per subnet
    - Determine DHCP address pools and Layer 2 VLAN pools

Structured Design

- Device Address Assignment

  - Within a network, there are different types of devices that require addresses:

    - **End-user clients** – Most use DHCP to reduce errors and burden on network support staff. IPv6 clients can obtain address information using DHCPv6 or SLAAC
    - **Servers and peripherals** – These should have a predictable static IP address
    - **Servers that are accessible from Internet** – Servers must have a public IPv4 address, most often accessed using NAT
    - **Intermediary devices** – Devices are assigned addresses for network management, monitoring, and security
    - **Gateway** – Routers and firewall devices are gateway for the hosts in that network

  - When developing an IP addressing scheme, it is generally recommended that we have a set pattern of how addresses are allocated to each type of device

Route Summarization

- Route Summarization

Route Summarization

- What is Route Summarization?

  - There are a lot of routes on internet and these routes are advertised by routers. But this advertisement capacity is limited. So, we do not advertise every route by the routers not to cause any overflow on these systems. Instead of advertising every route, we use Route Summarization. **Route Summarization is basically advertising many routes into one route.**

Route Summarization

- What is Route Summarization? (cont.)

  - When we advertise routes, we need an update packet and this update packet size increases with every new route. This consumes the bandwidth. This is not a problem for small number of routes. But if we think on the routes in the world, this bandwidth consumption reaches a very high value. <u>**So, one of the reasons of using Route Summarization is reducing bandwidth usage.**</u>

  - Another reason of using Route Summarization is the CPU usage during routing on route tables. If route tables have too much routes, this needs more time. But when we summarize routes, we reduce routing table size. **And this reduces the CPU usage and the required time for routing.**

Route Summarization

- Route Summarization: An example topology that contains four routers from different cities

- Here, we will **<u>summarize routes</u>** on Venice's and Florence's routes and they will be advertised to Milan as summary routes. Then, we will summarize these two routes of Milan and send it to Rome as one summary route.

Route Summarization

- First, let ‘s write Venice’s three routes in binary format and find the common bits of these three routes:

Common Bits of the Venice's Routes

11000000.10101000.00011001.00000000	192.168.25.0/28
11000000.10101000.00011010.00000000	192.168.26.0/28
11000000.10101000.00011011.00000000	192.168.27.0/28

- As we can see above, the first 22 bits are common in these three routes, so our **summary route for Venice is 192.168.24.0/22**

Route Summarization

- Second, let’s write Florence’s three routes into binary format and find the common bits:

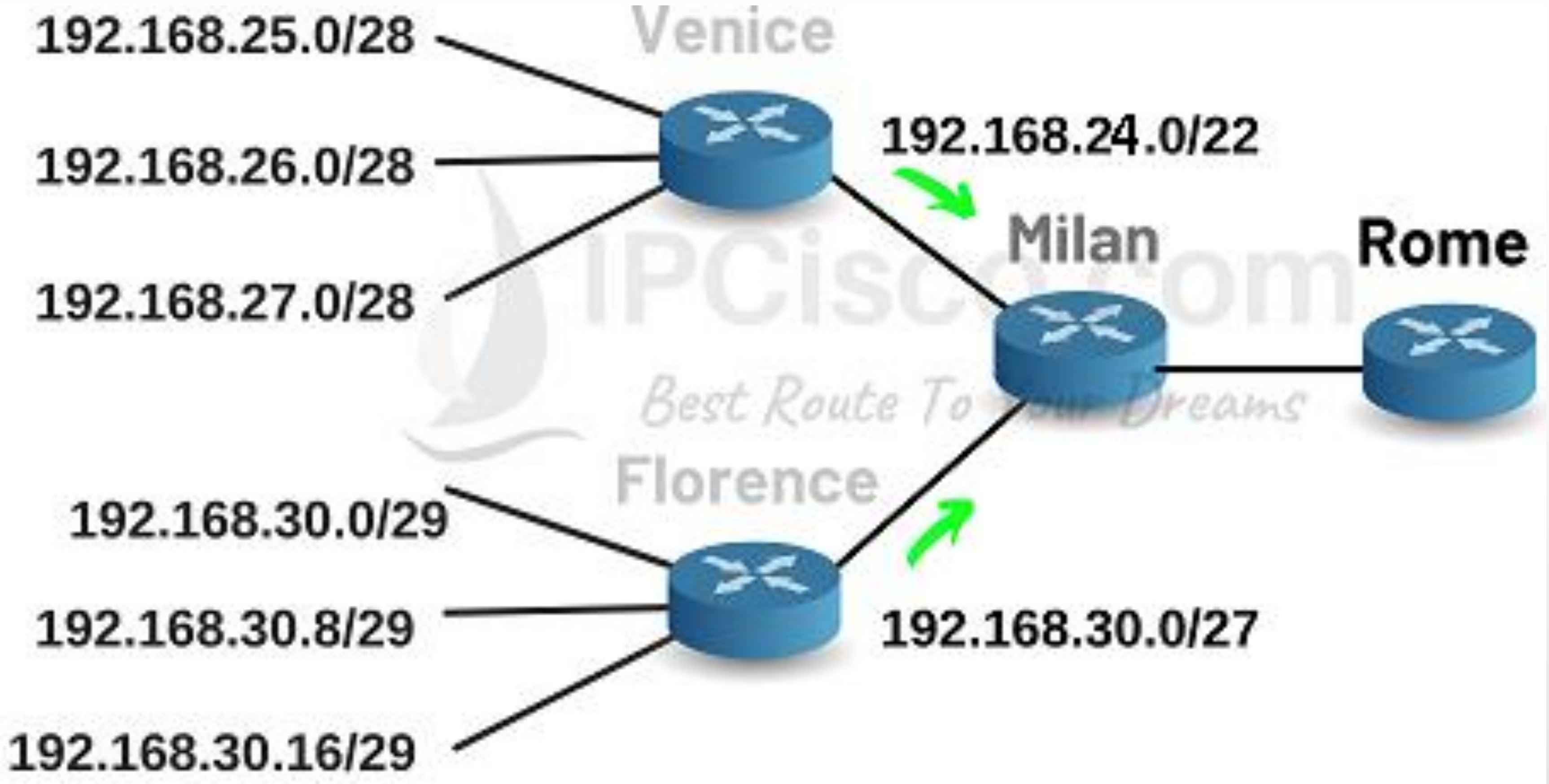
Common Bits of the Florence's Routes

11000000.10101000.00011110.00000000	192.168.30.0/29
11000000.10101000.00011110.00001000	192.168.30.8/29
11000000.10101000.00011110.00010000	192.168.30.16/29

According to these 27 common bits, our **summary route for Florence is 192.168.30.0/27**

Route Summarization

- Both 192.168.24.0/22 and 192.168.30.0/27 will be advertised to Milan as a result of Route Summarization



Route Summarization

- On Milan, there will be two routes and we will summarize these routes too. To do this, again, let’s write the routes in binary format and find the common bits:

Common Bits of the Milan's Routes

11000000.10101000.00011000.00000000	192.168.24.0/22
11000000.10101000.00011110.00000000	192.168.30.0/27

Summary Route For Milan 192.168.24.0/21

- According to binary bits, we have 21 common bits. So, the summary route for these routes is 192.168.24.0/21

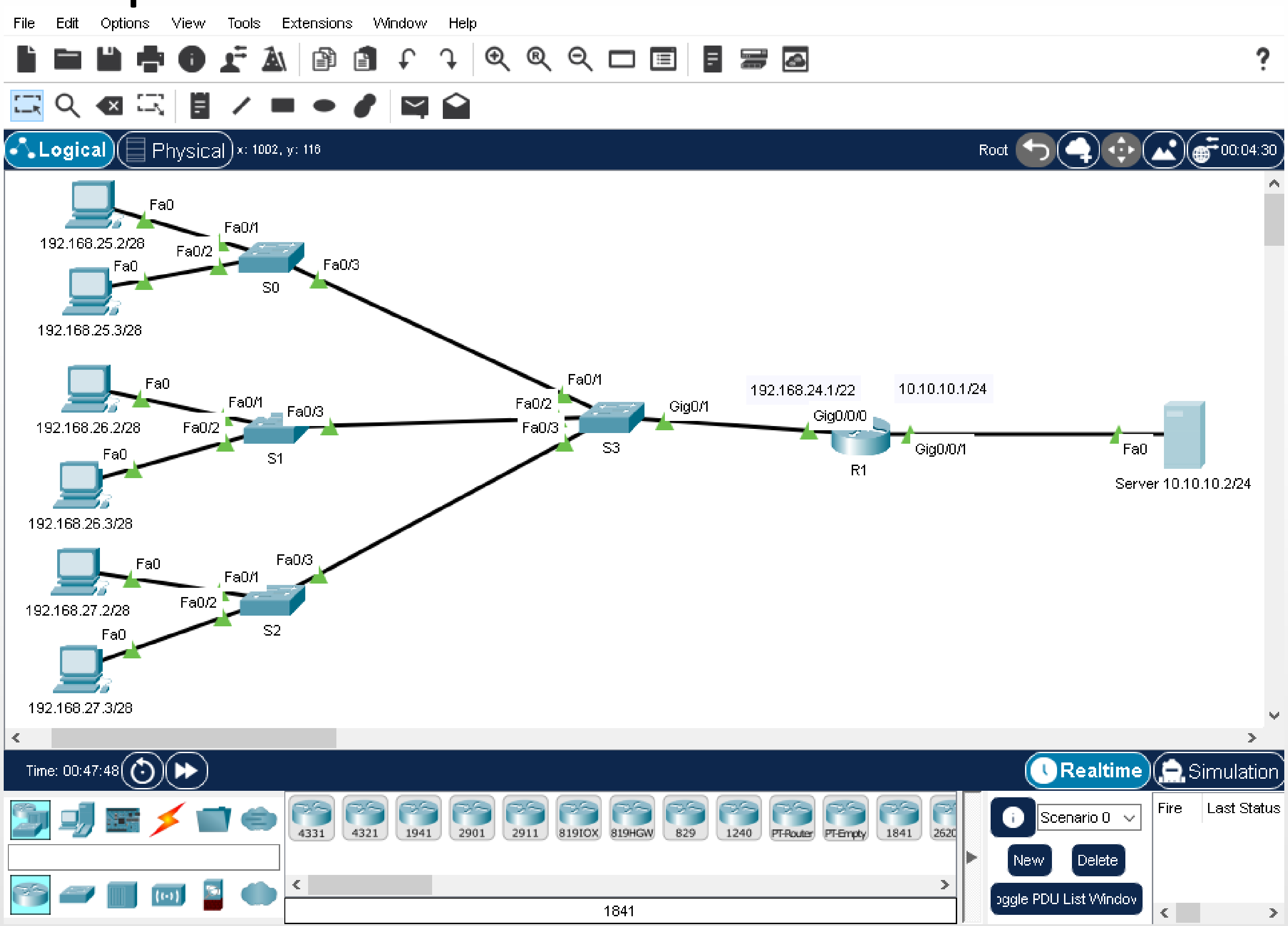
Route Summarization

- From Milan to Rome, only one summary route will be sent for the 6 routes of Venice and Florance

- As we can see here, with Route Summarization, route numbers reduce extremely. This reduces the bandwidth and used CPU by routing.

Route Summarization

- An example in Cisco Packet Tracer:



Route Summarization

- An example in Cisco Packet Tracer (cont.)

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 192.168.24.1 255.255.252.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

255.255.252.0 equals /22

```
R1(config)# interface g0/0/1
R1(config-if)# ip address 10.10.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

255.255.255.0 equals /24

```
R1(config)#ip route 192.168.24.0 255.255.252.0 10.10.10.1
```

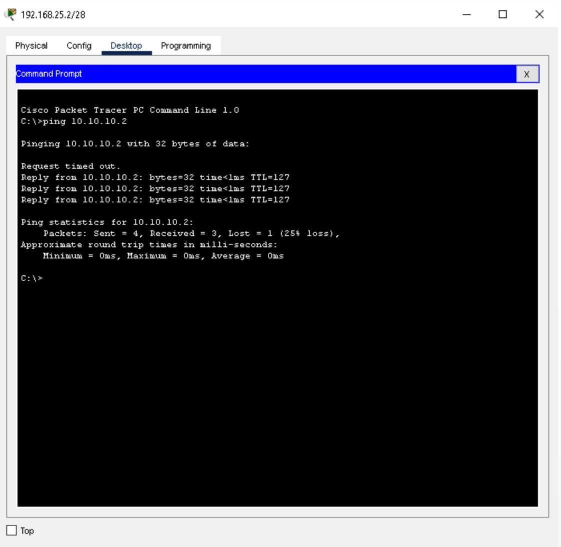
router(config)#`ip route` ***<Destination prefix> <Destination prefix mask> <Forwarding router's address>***

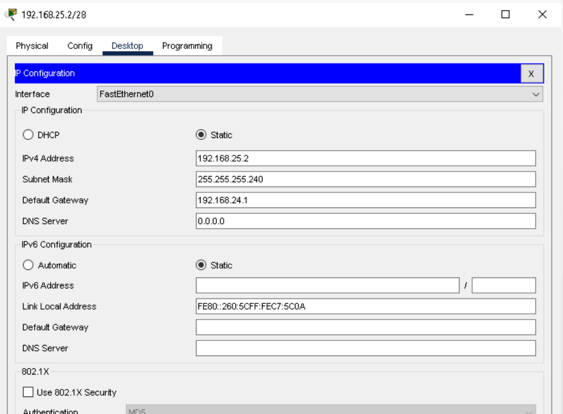
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/0/1
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0/1
C    192.168.24.0/22 is directly connected, GigabitEthernet0/0/0
     192.168.24.0/32 is subnetted, 1 subnets
L       192.168.24.1/32 is directly connected, GigabitEthernet0/0/0

R1#
```





Do you have any questions or comments?

Thank you
for your attention !

In this presentation:
- Some icons were downloaded from flaticon.com and iconscout.com