



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.

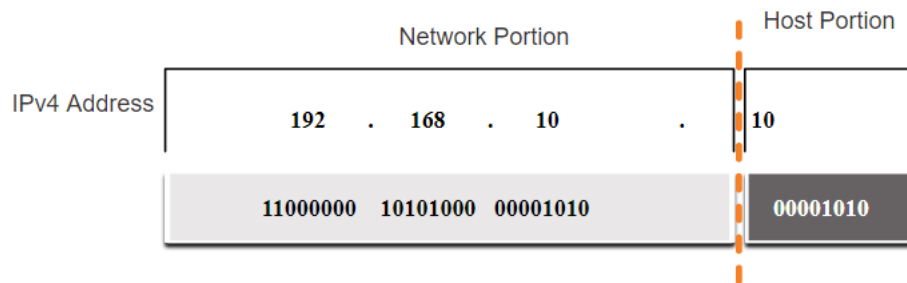


11.1 IPv4 Address Structure



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, you 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**.

	Network Portion				Host Portion
IPv4 Address	192	.	168	.	10
	11000000	10101000	00001010		00001010
Subnet Mask	255	.	255	.	0
	11111111	11111111	11111111		00000000

IPv4 Address Structure

The Prefix Length

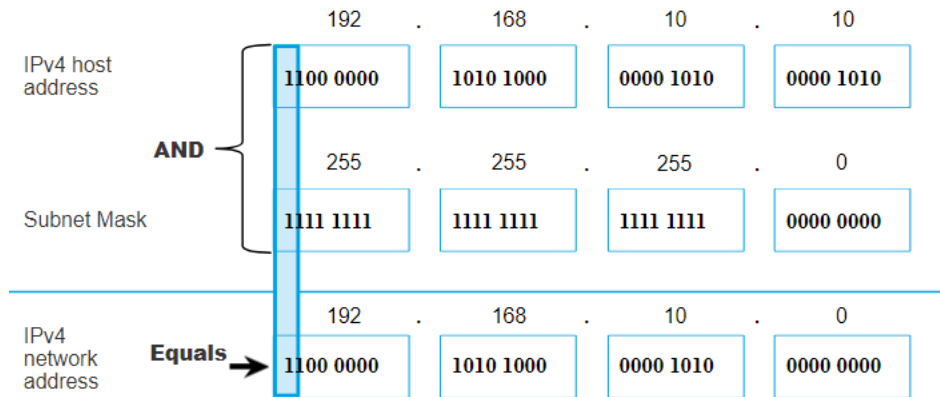
- A prefix length is a less cumbersome method used to identify a subnet mask address.
- The **prefix length** is the **number of bits set to 1** in the subnet mask.
- It is written in “**slash notation**” therefore, count the number of bits in the subnet mask and prepend it with a slash.

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



Determining the Network: Logical AND

- A **logical AND** Boolean operation is used in **determining** the **network** address.
- Logical AND is the comparison of two bits where only a **1 AND 1 produces a 1** and any other combination results in a 0.
- $1 \text{ AND } 1 = 1$, $0 \text{ AND } 1 = 0$, $1 \text{ AND } 0 = 0$, $0 \text{ AND } 0 = 0$
- $1 = \text{True}$ and $0 = \text{False}$
- To identify the network address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the network address.





Video – Network, Host and Broadcast Addresses

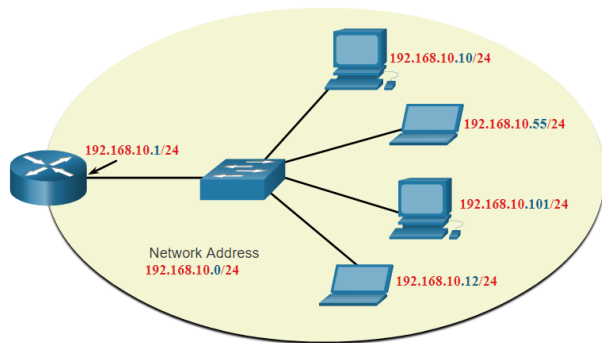
This video will cover the following:

- Network address
- Broadcast Address
- First usable host
- Last usable host



Network, Host, and Broadcast Addresses

- Within each **network** 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

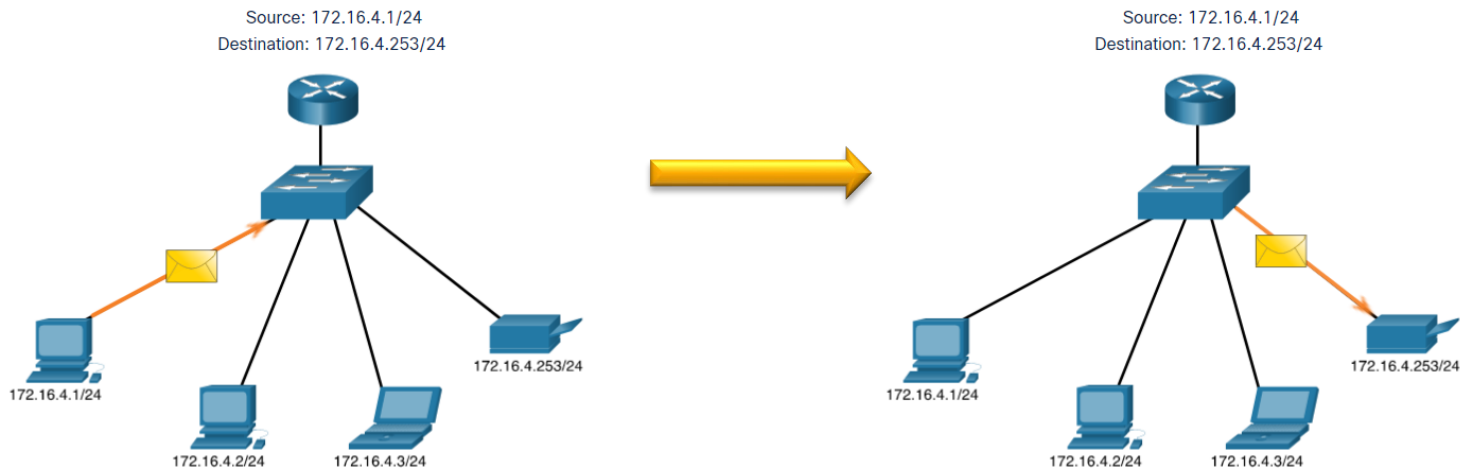


11.2 IPv4 Unicast, Broadcast, and Multicast

IPv4 Unicast, Broadcast, and Multicast

Unicast

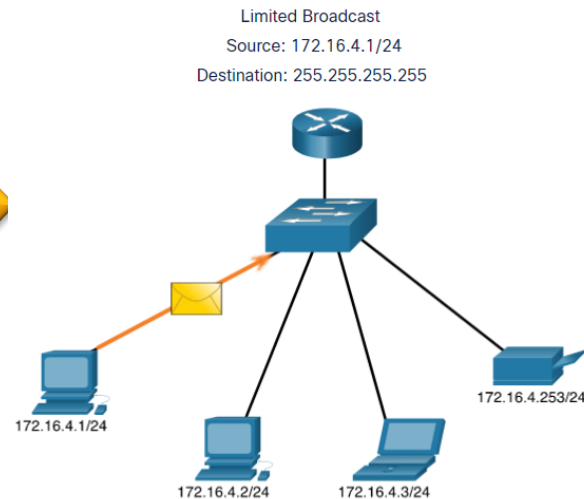
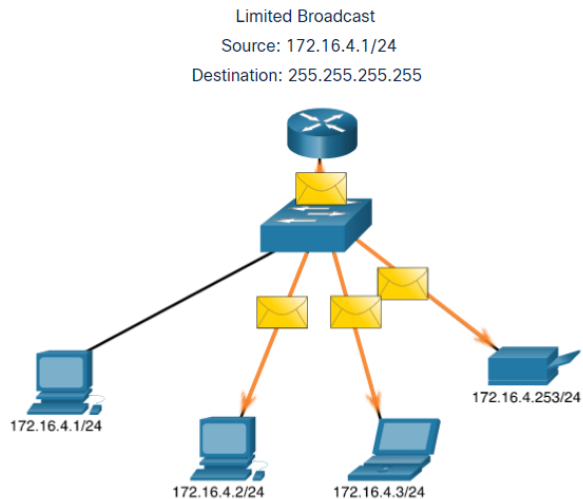
- Unicast transmission is sending a packet to **one destination** IP address.
- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.



IPv4 Unicast, Broadcast, and Multicast

Broadcast

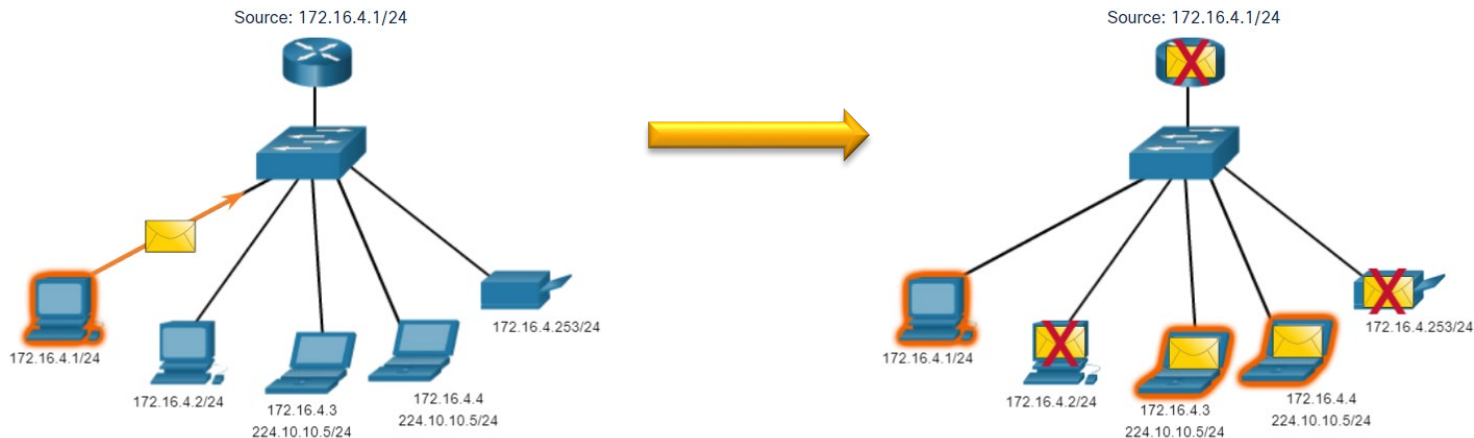
- Broadcast transmission is sending a packet to **all other** destination IP addresses.
- For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts.



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.





11.3 Types of IPv4 Addresses



Public and Private IPv4 Addresses

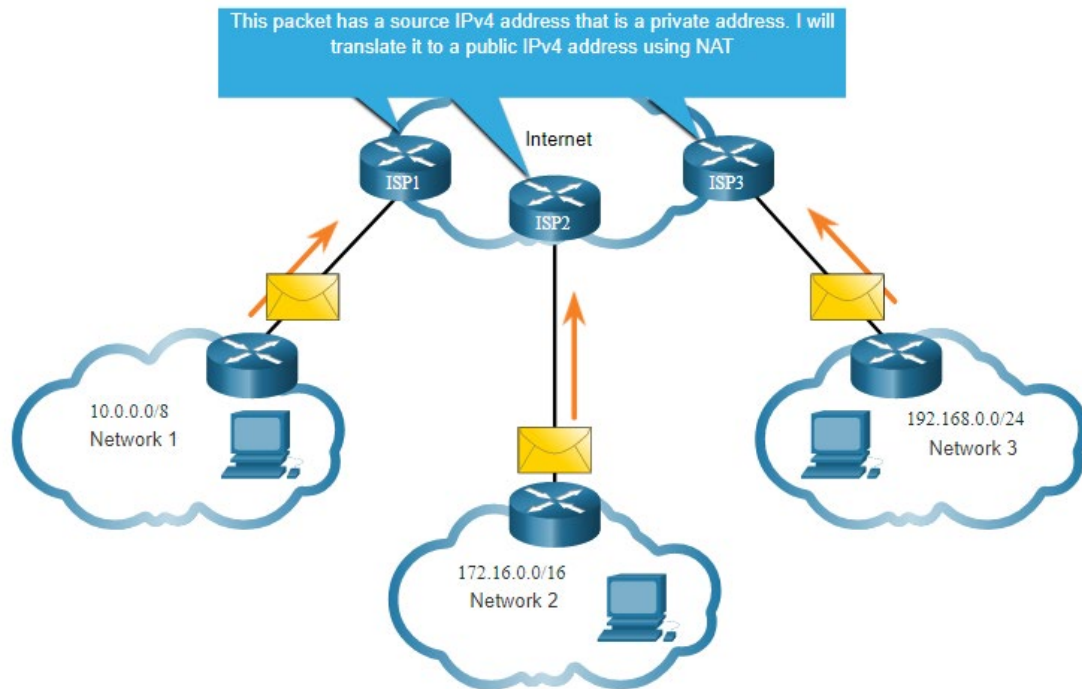
- As defined in in RFC 1918, **public IPv4** addresses are **globally routed** between internet service provider (**ISP**) routers.
- Private addresses** are common blocks of addresses used by most organizations to assign IPv4 addresses to **internal hosts**.
- Private IPv4 addresses are **not unique** 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**.

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

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.

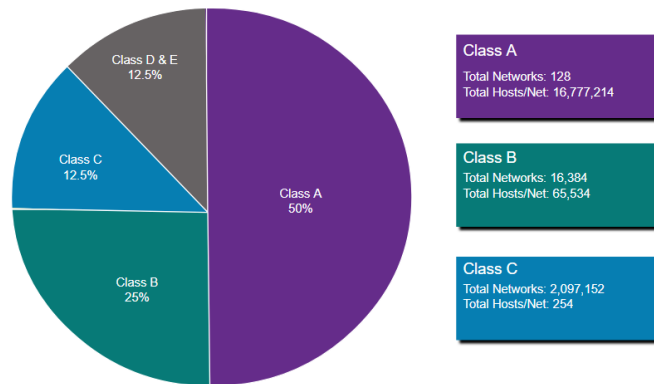
Legacy Classful Addressing

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)

- Classful addressing wasted many IPv4 addresses.

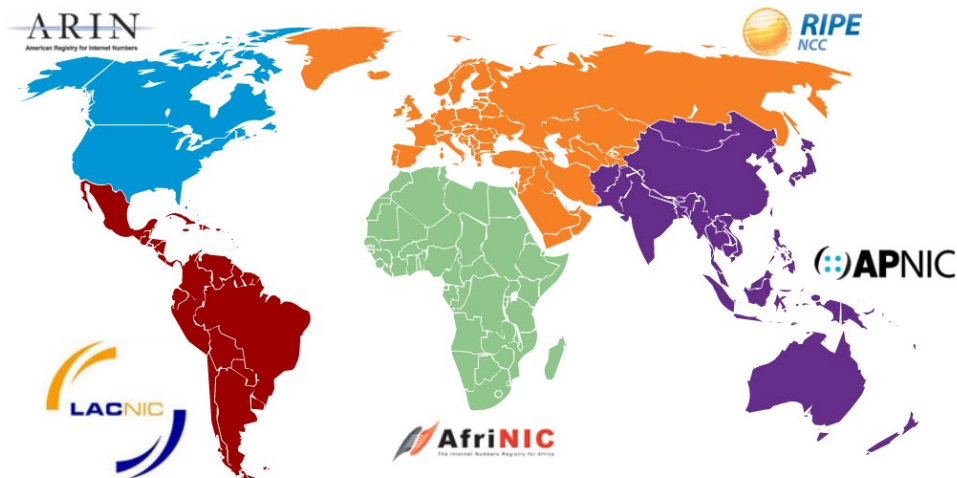
Classful address allocation was replaced with **classless addressing** which ignores the rules of classes (A, B, C).



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.



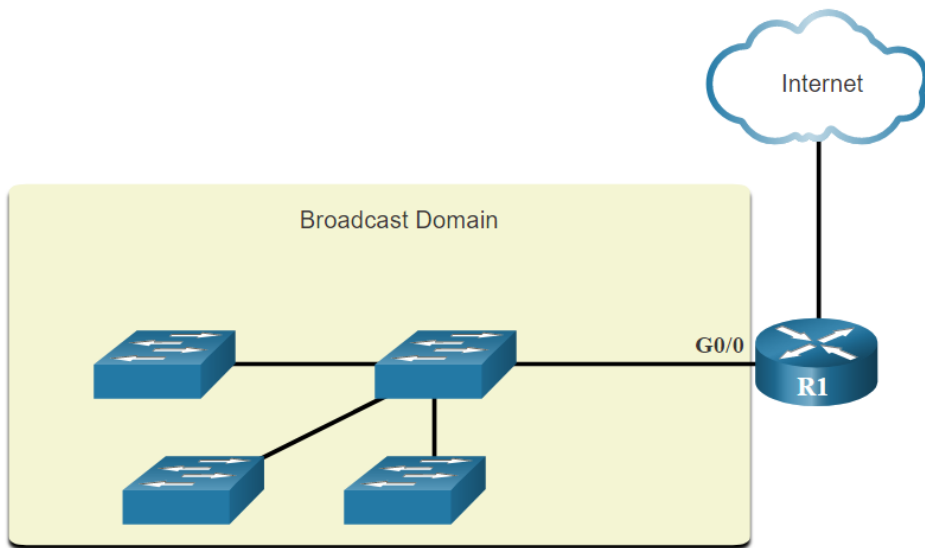


11.4 Network Segmentation

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**.

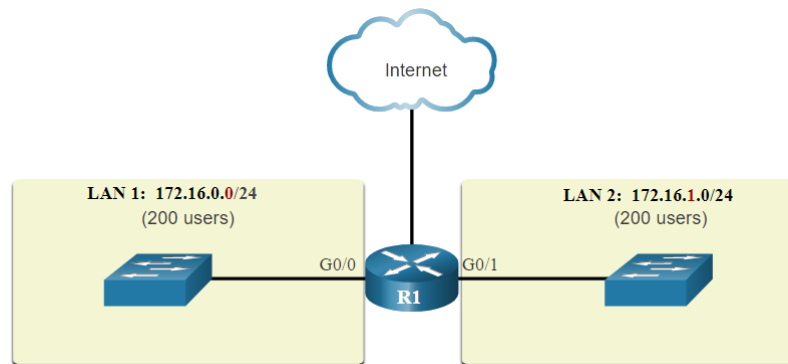
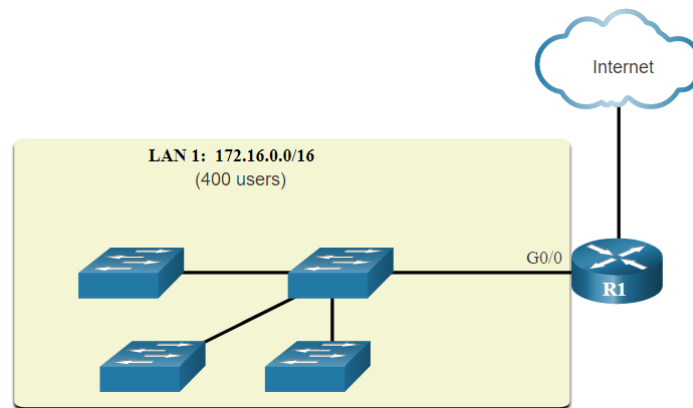


- The only device that **stops** broadcasts is a **router**.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific **broadcast domain**.

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.

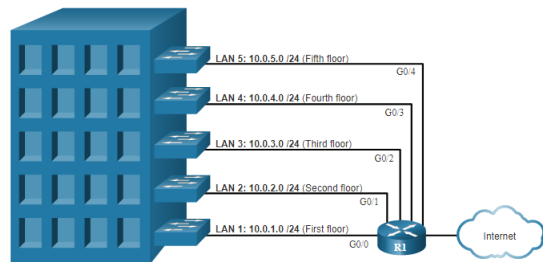


Network Segmentation

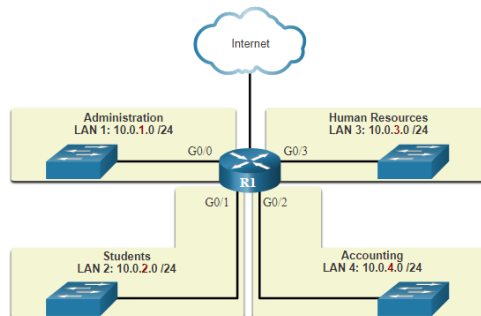
Reasons for Segmenting Networks

- 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:

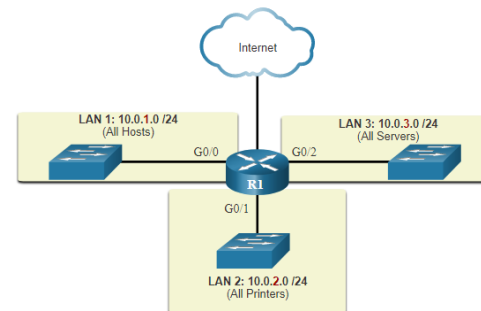
Location



Group or Function



Device Type





11.5 Subnet an IPv4 Network

Subnet 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	nnnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnnn.nnnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.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



Subnet an IPv4 Network

Video – The Subnet Mask

- This video will demonstrate the process of subnetting.



Video – Subnet with the Magic Number

- This video will demonstrate subnetting with the magic number.



Packet Tracer – Subnet an IPv4 Network

In this Packet Tracer, you will do the following:

- Design an IPv4 Network Subnetting Scheme
- Configure the Devices
- Test and Troubleshoot the Network



11.6 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**.

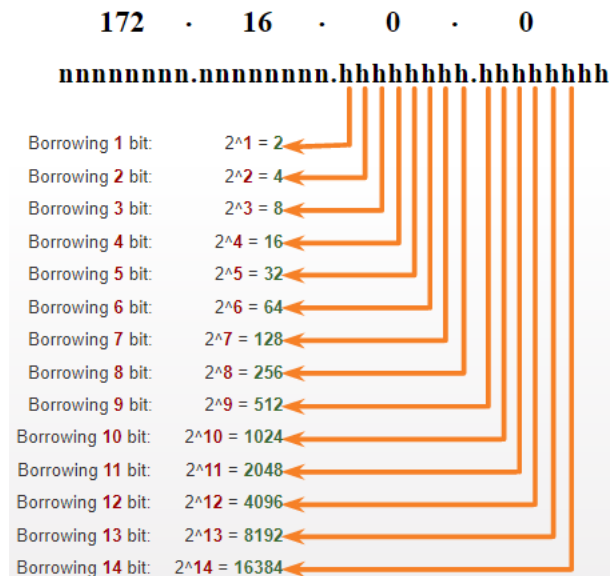
Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000	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.nhhhhhhh 11111111.11111111.11111111.10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100	16384	2

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).



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., $2^{10}=1024$ subnets) would need to be borrowed (for a total of 1024 subnets)





Subnet a Slash 16 and a Slash 8 Prefix

Video – Subnet Across Multiple Octets

This video will demonstrate creating subnets across multiple octets.



Subnet a Slash 16 and a Slash 8 Prefix

Lab – Calculate IPv4 Subnets

In this lab, you will complete the following objectives:

- Part 1: Determine IPv4 Address Subnetting
- Part 2: Calculate IPv4 Address Subnetting

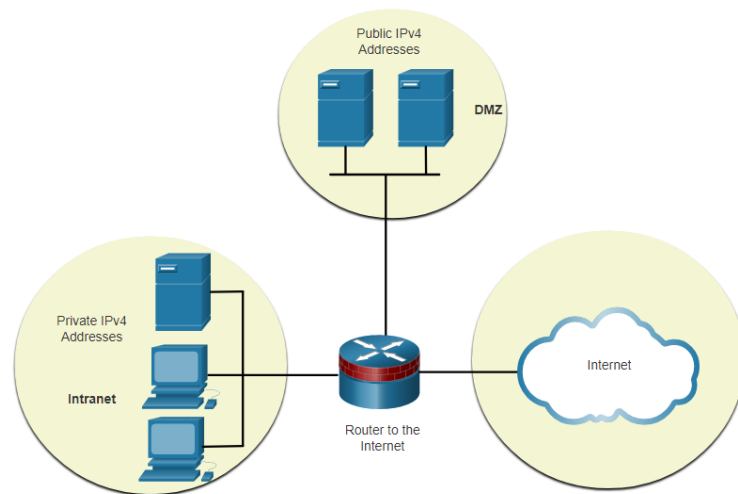


11.7 Subnet to Meet Requirements

Subnet Private versus Public IPv4 Address Space

Enterprise networks will have an:


- **Intranet** - A company's internal network typically using **private** IPv4 addresses.
- **DMZ** - A company's internet facing servers. 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.



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

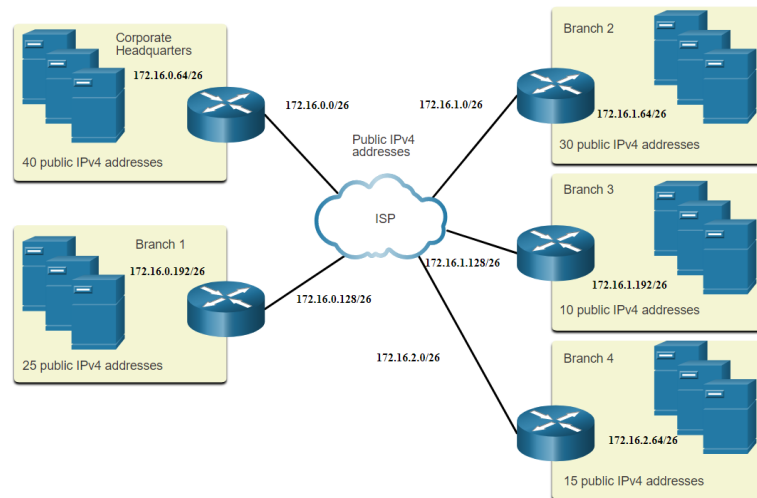
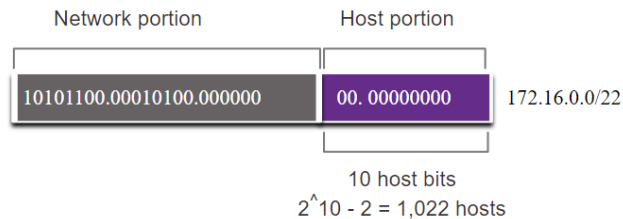


Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.10000000	2	126
/26	255.255.255.192	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.11000000	4	62
/27	255.255.255.224	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.11100000	8	30
/28	255.255.255.240	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.11110000	16	14
/29	255.255.255.248	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.11111000	32	6
/30	255.255.255.252	nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn.nnnnnnnnnn 11111111.11111111.11111111.11111100	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 1,022 host addresses.
- There are five sites and therefore five internet connections 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.



Packet Tracer – Subnetting Scenario

In this Packet Tracer, you will do the following:

- Design an IP Addressing Scheme
- Assign IP Addresses to Network Devices and Verify Connectivity



11.8 VLSM

 VLSM

Video – VLSM Basics

- This video will explain VLSM basics.

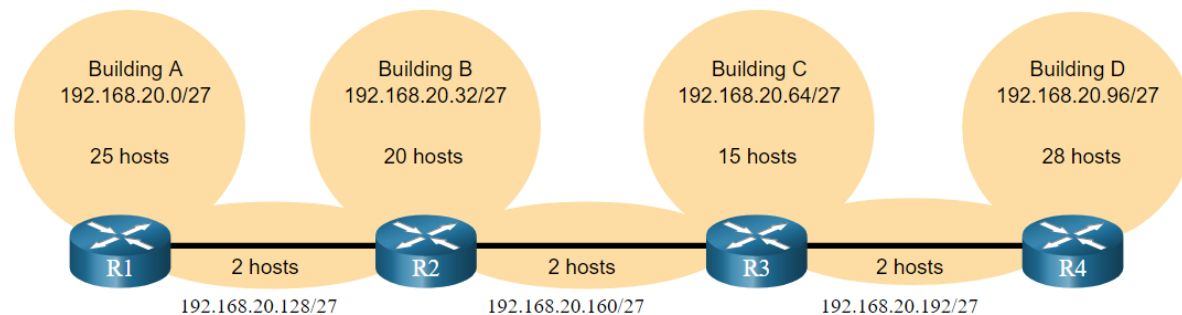
VLSM Video – VLSM Example

- This video will demonstrate creating subnets specific to the needs of the network.

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.

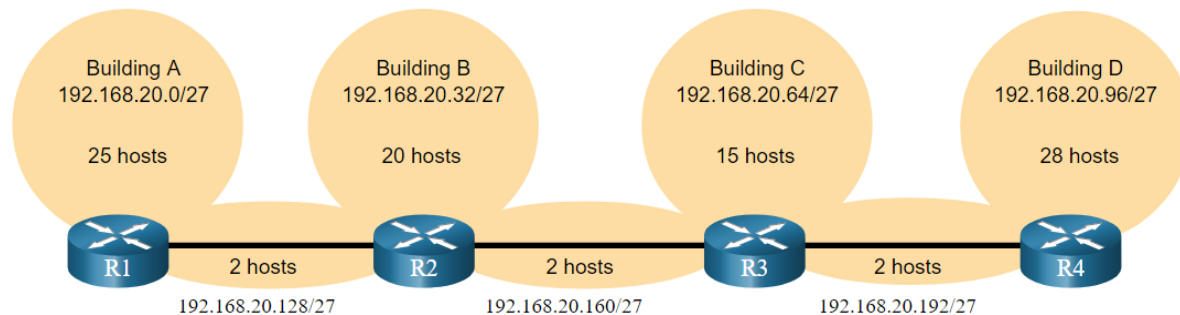
- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.



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.

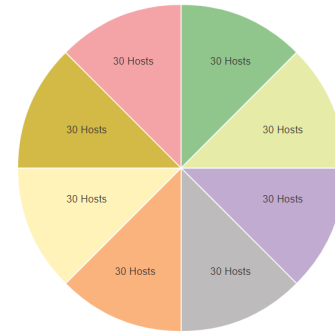
Host portion
 $2^5 - 2 = 30$ host IP addresses per subnet
 $30 - 2 = 28$
Each WAN subnet wastes 28 addresses
 $28 \times 3 = 84$
84 addresses are unused



- 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**.

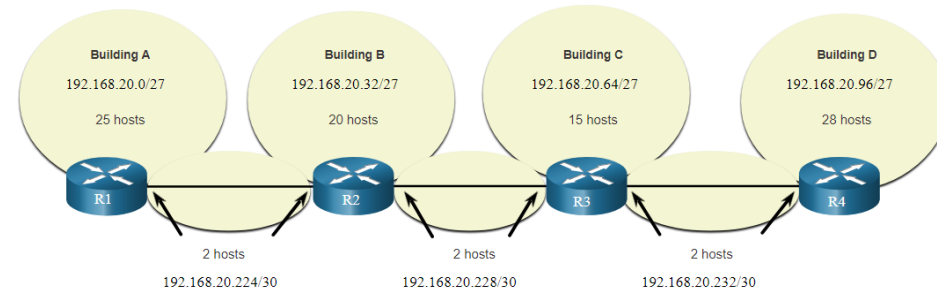
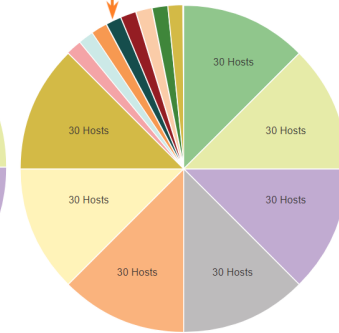
- The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how **VLSM** can be used to **subnet a subnet** and **divided the last subnet** into eight /30 subnets.
- When using VLSM, always **begin** by satisfying the host requirements of the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



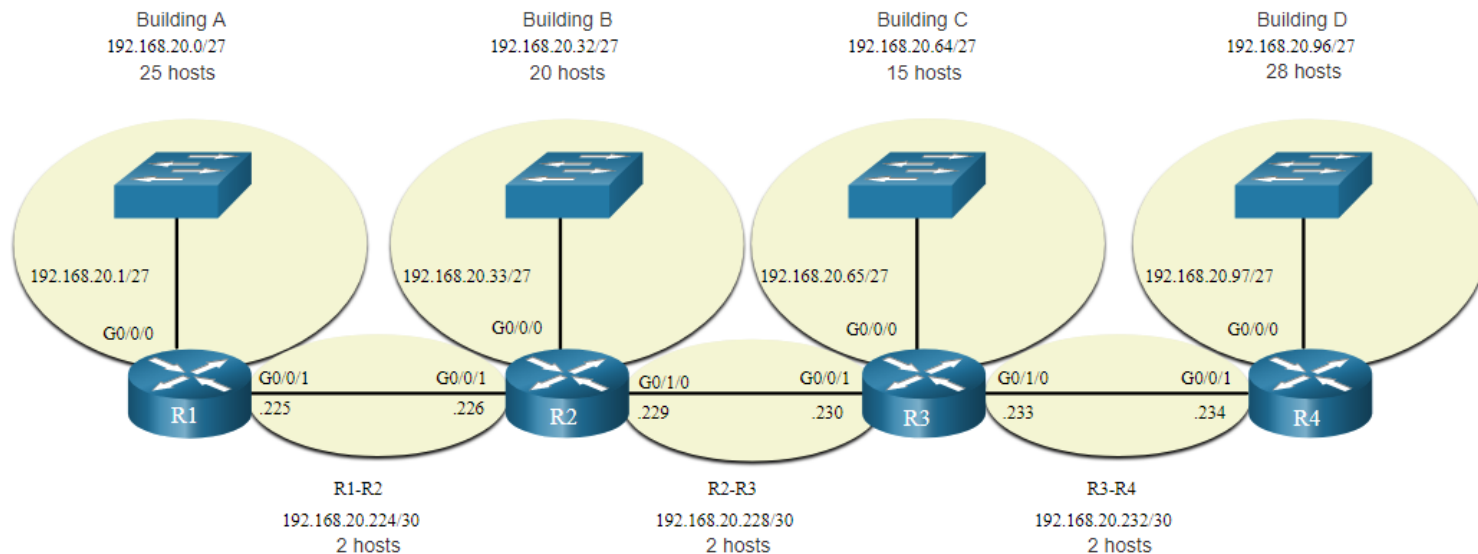
Subnets of Varying Sizes

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



VLSM 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.





11.9 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, you 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 your 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 the 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 you have a set pattern of how addresses are allocated to each type of device.



Packet Tracer – VLSM Design and Implementation Practice

In this Packet Tracer, you will do the following:

- Examine the Network Requirements
- Design the VLSM Addressing Scheme
- Assign IP Addresses to Devices and Verify Connectivity



11.10 Module Practice and Quiz



Packet Tracer – Design and Implement a VLSM Addressing Scheme

In this Packet Tracer, you will do the following:

- Design a VLSM IP addressing scheme given requirements
- Configure addressing on network devices and hosts
- Verify IP connectivity
- Troubleshoot connectivity issues as required.



Lab - Design and Implement a VLSM Addressing Scheme

In this lab, you will complete the following objectives:

- Examine Network Requirements
- Design the VLSM Address Scheme
- Cable and Configure the IPv4 Network



What did I learn in this module?

- The **IP addressing** structure consists of a **32-bit** hierarchical network address that identifies a **network** and a **host portion**. Network devices use a process called **ANDing** using the IP address and associated subnet mask to **identify** the network and host **portions**.
- Destination IPv4 packets can be **unicast**, **broadcast**, and **multicast**.
- There are globally **routable** IP addresses as assigned by the **IANA** and there are three ranges of private IP network addresses that cannot be routed globally but can be used on all internal **private** networks.
- **Reduce large broadcast domains** using **subnets** to create smaller broadcast domains, reduce overall network traffic, and improve network performance.
- Create IPv4 subnets using **one or more of the host bits as network bits**. However, networks are most easily subnetted at the octet boundary of **/8**, **/16**, and **/24**.
- **Larger** networks can be **subnetted** at the **/8** or **/16** boundaries.
- Use **VLSM** to **reduce the number of unused host addresses per subnet**.



What did I learn in this module? (Cont.)

- **VLSM** allows a network space to be **divided into unequal parts**. Always **begin** by satisfying the host requirements of the **largest** subnet. Continue subnetting until the host requirements of the **smallest subnet** are satisfied.
- When designing a network **addressing scheme**, consider **internal, DMZ, and external** requirements. Use a consistent internal IP addressing scheme with a set **pattern** of **how addresses** are **allocated** to each type of device.

New Terms and Commands

- prefix length
- logical AND
- network address
- broadcast address
- first usable address
- last usable address
- unicast, broadcast, and multicast transmissions
- private addresses
- public addresses
- Network Address Translation (NAT)
- loopback addresses
- Automatic Private IP Addressing (APIPA) addresses
- classful addressing (Class A, B, C, D, and E)

Internet Assigned Numbers Authority (IANA)
Regional Internet Registries (RIRs)
AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC
broadcast domains
subnets
octet boundary
variable-length subnet mask (VLSM)

