Elk Technologies
https://elktech.org
Scott Stephenson

Module 11: IPv4 Addressing

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

CCNAv7

Module Objectives

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

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

11.1 IPv4 Address Structure

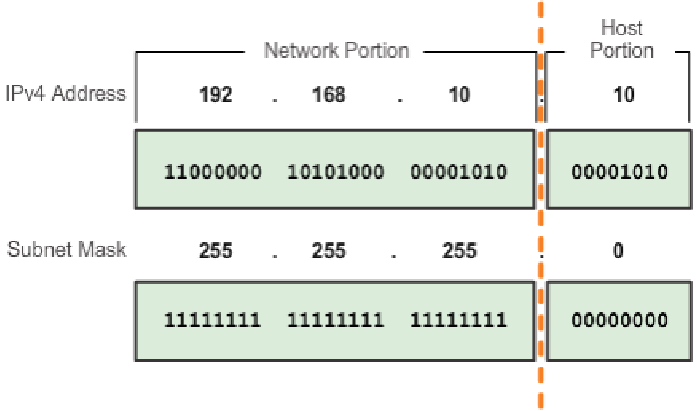
Network Portion and Host Portion

	1 Byte ← 8 bits →	1 Byte ← 8 bits →	1 Byte ← 8 bits →	1 Byte ← 8 bits →
Class A	**N**	**H**	**H**	**H**
Class B	**N**	**N**	**H**	**H**
Class C	**N**	**N**	**N**	**H**

- An IPv4 address is a 32-bit hierarchical address that is made up of a **network** portion and a **host** portion.
- The formulas are the default configuration for each class:
  - **N = Network Number**
    - Assigned by the American Registry for Internet Numbers (ARIN)
    - Administrator has no control over this part of the address
  - **H = Host Number**
    - Assigned and controlled by the network administrator

The Subnet Mask

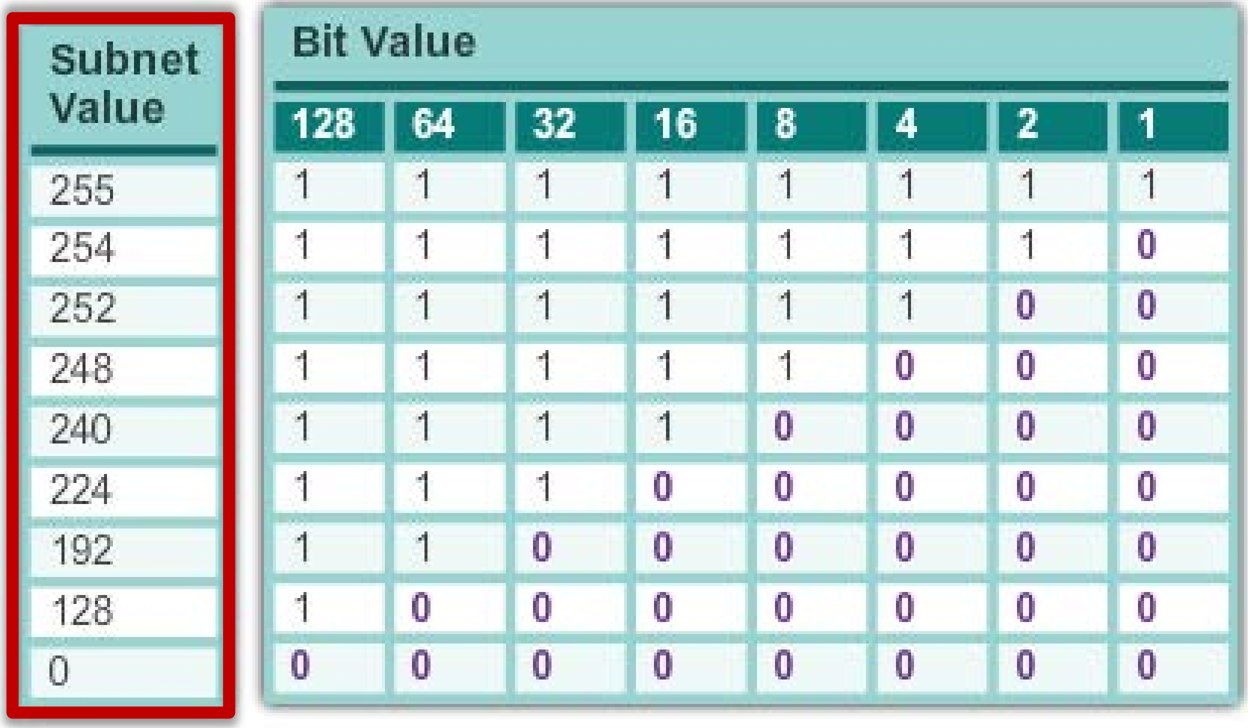
- To define the network and host portions of an address, a devices use a separate 32-bit pattern called a **subnet mask**.
- The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address.
- To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right.



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

The Subnet Mask

- 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

The Prefix Length

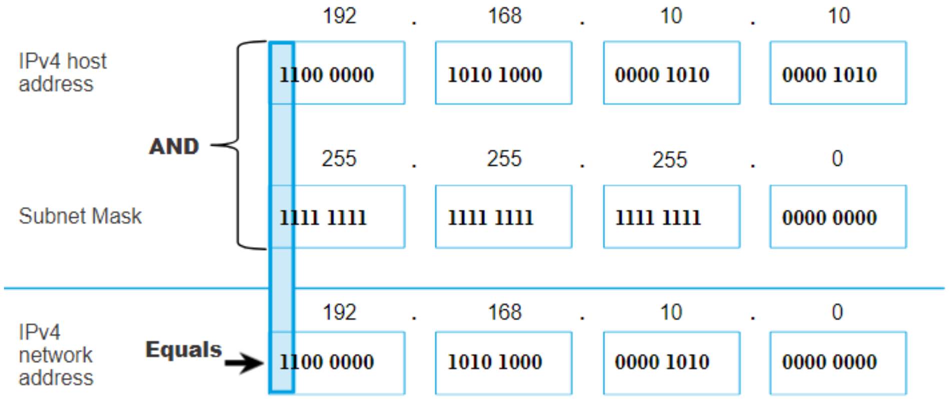
- A prefix length is a less cumbersome or shorthand method used to identify a subnet mask address.
- The prefix length is the number of bits set to 1 in the subnet mask. This indicates the number of bits in the network portion.
- It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.
- Note: Know how to convert the Prefix Length into the Subnet Mask.

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

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

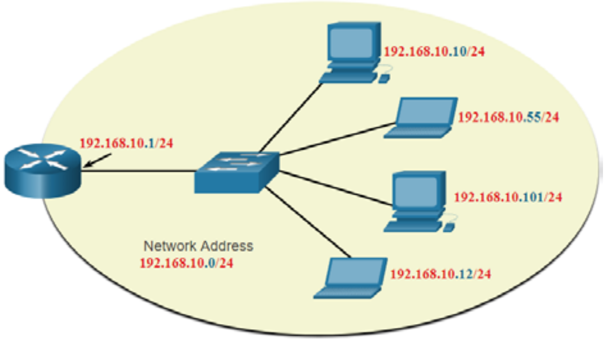
AND	**0**	**1**
0	0	0
1	0	1



		192 .	168 .	10 .	10
IPv4 host address		1100 0000	1010 1000	0000 1010	0000 1010
	AND	255 .	255 .	255 .	0
Subnet Mask		1111 1111	1111 1111	1111 1111	0000 0000
		192 .	168 .	10 .	0
IPv4 network address	**Equals**	1100 0000	1010 1000	0000 1010	0000 0000

Network, Host, and Broadcast Addresses

- Within each network are three types of IP addresses:
  - Network address
  - Host addresses (usable range)
  - Broadcast address

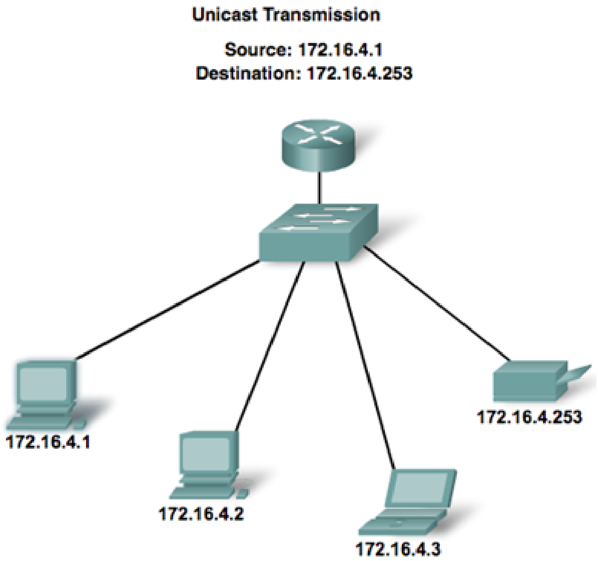


	Network Portion	Host Portion	Host Bits
Subnet mask 255.255.255.0 or /24	255 255 255 11111111 11111111 11111111	0 00000000	
Network address 192.168.10.0 or /24	192 168 10 11000000 10100000 00001010	0 00000000	All 0s
First address 192.168.10.1 or /24	192 168 10 11000000 10100000 00001010	1 00000001	All 0s and a 1
Last address 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 11111110	All 1s and a 0
Broadcast address 192.168.10.255 or /24	192 168 10 11000000 10100000 00001010	255 11111111	All 1s

11.2 IPv4 Unicast, Broadcast, and Multicast

Unicast

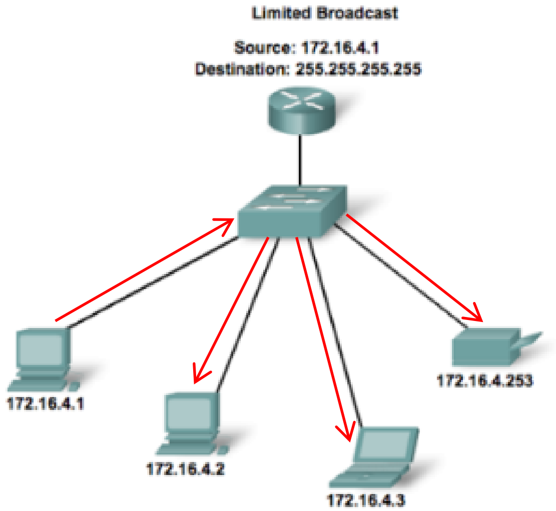
- Unicast transmission is sending a packet from one host to an specific host.
- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.



Broadcast

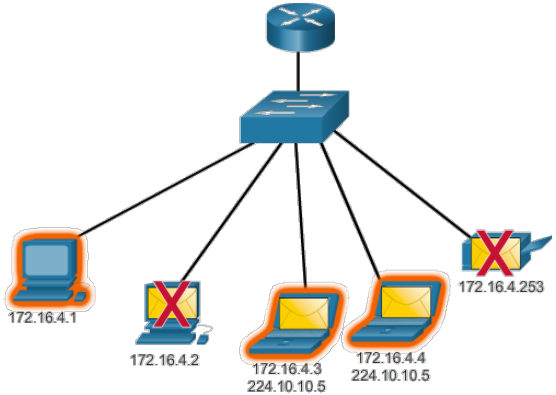
- Broadcast transmission is sending a packet from one host to all hosts in the network.
- A **Limited Broadcast** packet has a destination IP address of 255.255.255.255
- A **Directed Broadcast** sends a message to all hosts on its network.
  - All hosts within the 172.16.4.0/24 network
  - Destination 172.16.4.255

- Note:
  - Routers do not forward broadcasts.
  - Routers create broadcast domains.



Multicast

- Multicast transmission is sending a packet from one host to a selected group of hosts, possibly in different networks (multicast address group).
  - Can be used by routers to exchange routing information
  - Reserved for addressing multicast groups on a local network (Link local) – 224.0.0.0 to 224.0.0.255
  - **Globally scoped addresses** - 224.0.1.0 to 239.255.255.255
    - (Example: 224.0.1.1 has been reserved for Network Time Protocol)
  - Reduces traffic
- 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

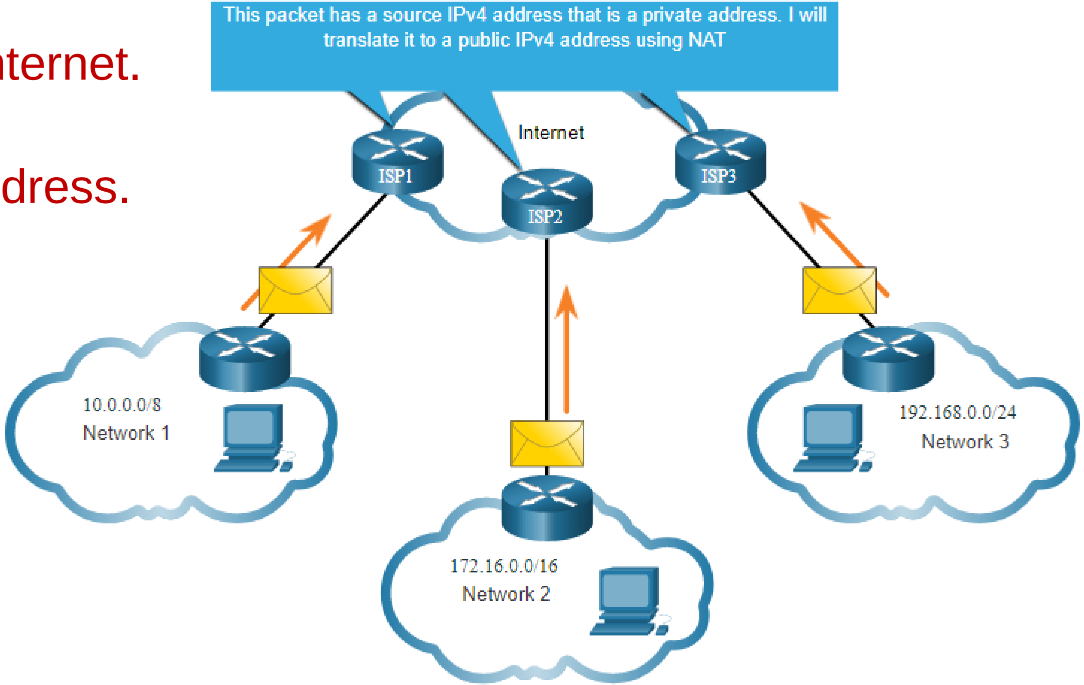
Public and Private IPv4 Addresses

- 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 (shared address space) 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

Routing to the Internet

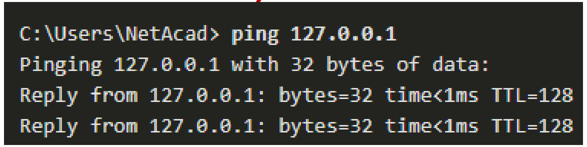
- **Network Address Translation** (NAT) translates private IPv4 addresses to public IPv4 addresses.
- NAT is typically enabled on the edge router connecting to the internet.
- It translates the internal private address to a public global IP address.



This packet has a source IPv4 address that is a private address. I will translate it to a public IPv4 address using NAT

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.

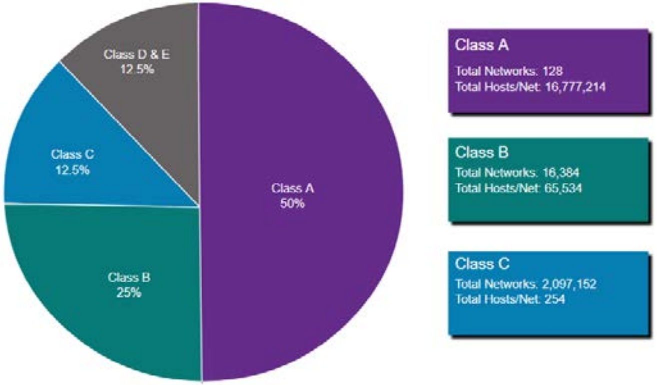


```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

- **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.
- **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
  - Listed as reserved.

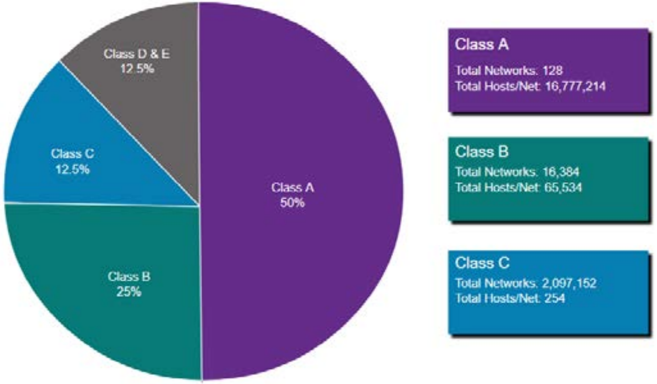
Legacy Classful Addressing

- In 1981, Internet IPv4 addresses were assigned using classful addressing (RFC 790)
  - 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.
- Subnets are all the same size.
- Subnet mask is the same for all subnetworks.
- Subnet mask is NOT sent as part of routing updates.



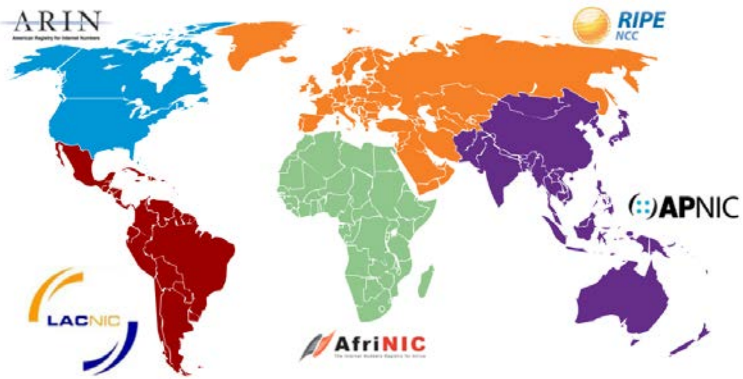
Classless Addressing

- Classful Addressing wasted addresses and exhausted the availability of IPv4 addresses.
- Replaced with classless addressing which ignores the rules of classes (A, B, C).
- Classless Addressing Introduced in the 1990s.
- Formal name is Classless Inter-Domain Routing (CIDR, pronounced “Cider”).
- 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.
- Subnets can be different sizes
- Subnet masks can be different for each subnetwork
- Subnet mask is sent as part of routing updates

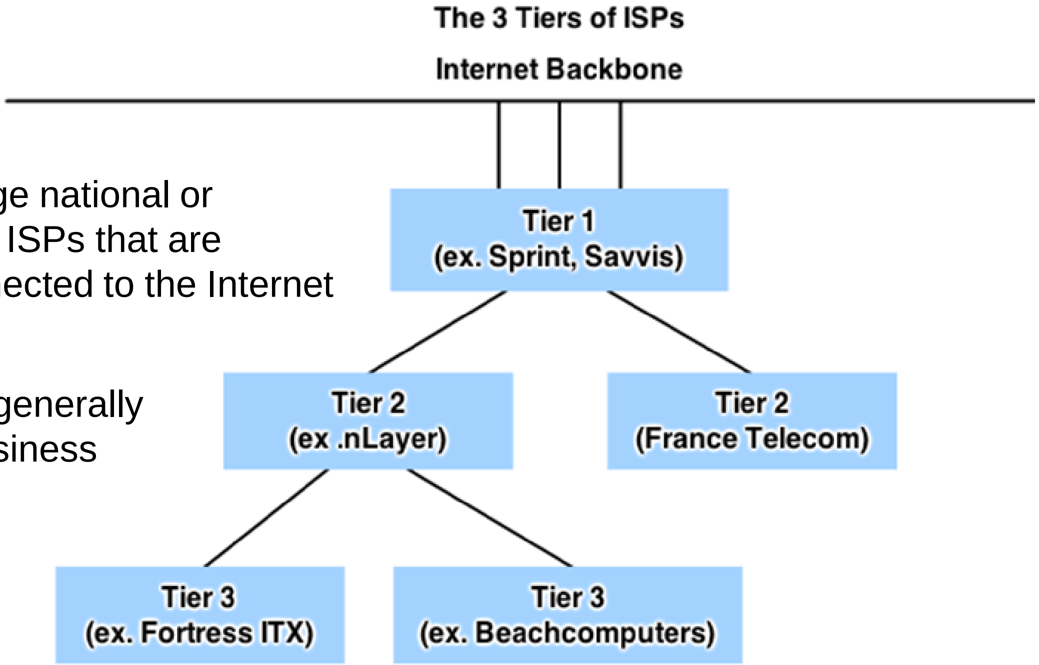


Assignment of IP Addresses

- The Internet Assigned Numbers Authority (IANA) manages and allocates blocks of IPv4 and IPv6 addresses to five Regional Internet Registries (RIRs).
  - **American Registry for Internet Numbers** (ARIN) – North America.
  - **Réseaux IP Europeans** (RIPE) – Europe, the Middle East, and Central Asia
  - **Asia Pacific Network Information Centre** (APNIC) – Asia and Pacific regions
  - **African Network Information Centre** (AfriNIC) – Africa
  - **Regional Latin-American and Caribbean IP Address Registry** (LACNIC) – Latin America and some Caribbean islands
- RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to smaller ISPs and organizations.



Assignment of IP Addresses



ISPs are large national or international ISPs that are directly connected to the Internet backbone.

Tier 2 ISPs generally focus on business customers.

Tier 3 ISPs often bundle Internet connectivity as a part of network and computer service contracts for their customers.

Tier 3 ISPs purchase their Internet service from Tier 2 ISPs.

Know Your Address

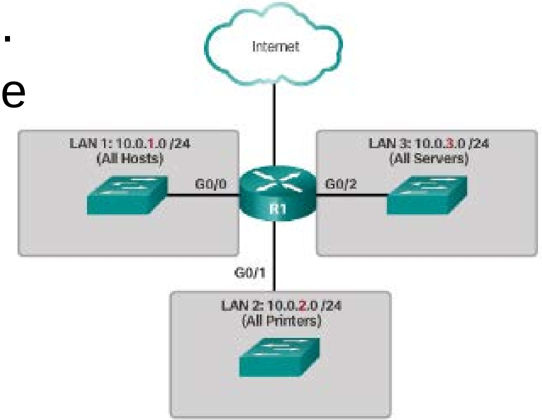
Match each description with an appropriate IP address:

E	1. A legacy Class “A” address	A. 192.31.18.123
H	2. A legacy Class “B” address	B. 127.0.0.1
A	3. A legacy Class “C” address	C. 198.256.2.3
I	4. A legacy Class “D” address	D. 169.254.1.5 **APIPA**
C	5. An invalid IPv4 address	E. 64.100.3.5
G	6. A Private address	F. 242.56.6.1
B	7. A Loopback address	G. 172.19.20.5
F	8. An experimental address	H. 128.107.5.1
J	9. A TEST-NET address	I. 224.2.6.255
D	10. A Link-Local address	J. 192.0.2.123

11.4 Network Segmentation

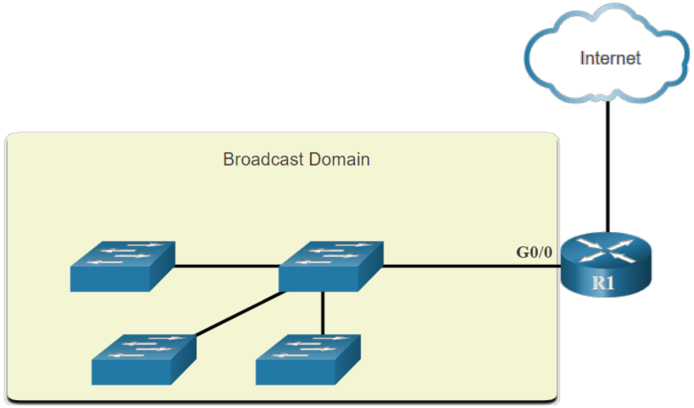
Broadcast Domains

- Each router interface connects a broadcast domain.
- Broadcasts are only propagated within its broadcast domain.
- Devices use broadcasts in an Ethernet LAN to locate:
  - **Other devices** - Address Resolution Protocol (ARP) which sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address.
  - **Services** – Dynamic Host Configuration Protocol (DHCP) which sends broadcasts on the local network to locate a DHCP server.
- Switches propagate broadcasts out all interfaces except the interface on which it was received.
  - Connecting switches together increases the size of the broadcast domain.
- How many broadcast domains are there if the graphic? **4**



Broadcast Domains and Segmentation

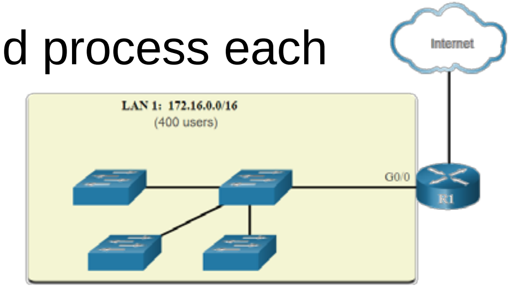
- Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server.)
- Switches propagate broadcasts out all interfaces except the interface on which it was received.

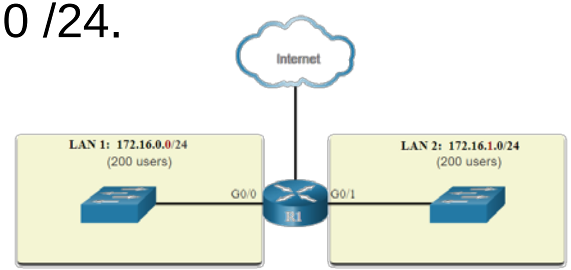


- The only device that stops broadcasts is a router.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

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.
  - Slow network operations due to the significant amount of traffic it can cause.
  - Slow device operations because a device must accept and process each broadcast packet.
- 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.

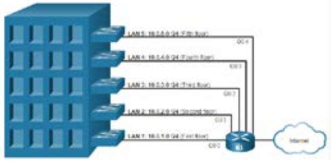




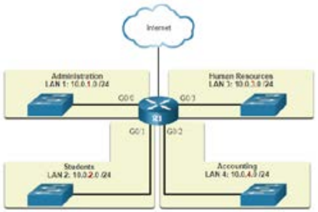
Reasons for Segmenting Networks

- Large networks need to be segmented into smaller sub-networks, creating smaller groups of devices and services in order to:
  - Reduce the size of the network to create smaller broadcast domains .
  - Control traffic by containing broadcast traffic within subnetwork .
  - Reduce overall network traffic and improve network performance.
  - Enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together.
  - Subnetting reduces the number of devices affected by abnormal broadcast traffic.
- **Subnetting** - process of segmenting a network into multiple smaller network spaces called **subnetworks** or **subnets.**

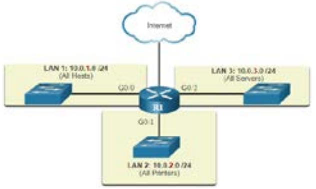
Location


LAN 5: 10.0.5.0 /24 (Fifth floor)
G0/4
LAN 4: 10.0.4.0 /24 (Fourth floor)
G0/3
LAN 3: 10.0.3.0 /24 (Third floor)
G0/2
LAN 2: 10.0.2.0 /24 (Second floor)
G0/1
LAN 1: 10.0.1.0 /24 (First floor)
G0/0
R1
Internet

Group or Function



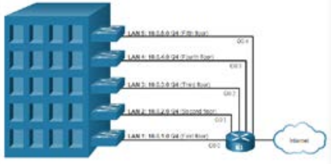
Device Type



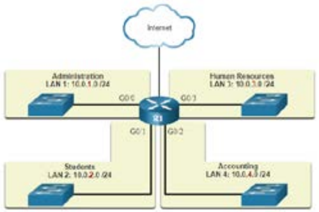
Reasons for Segmenting Networks

- Communication Between Subnets
  - A router is necessary for devices on different networks and subnets to communicate.
  - Because each broadcast domain connects to a different router interface, each domain needs its own network address space.
  - Each router interface must have an IP host address that belongs to the network or subnet that the router interface is connected to.
  - Devices on a network and subnet use the router interface attached to their LAN as their default gateway.
  - Network administrators can group devices into subnets that are determined by location, organizational unit/group/function or device type.

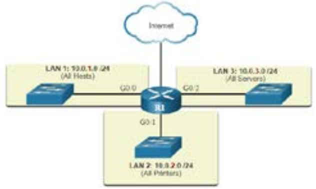
Location


LAN 5: 10.0.5.0 /24 (Fifth floor)
G0/4
LAN 4: 10.0.4.0 /24 (Fourth floor)
G0/3
LAN 3: 10.0.3.0 /24 (Third floor)
G0/2
LAN 2: 10.0.2.0 /24 (Second floor)
G0/1
LAN 1: 10.0.1.0 /24 (First floor)
G0/0
R1
Internet

Group or Function



Device Type



11.5 Subnet an IPv4 Network

Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Prefix length and the subnet mask are different ways of identifying the network portion of an address.
- Subnets are created by borrowing host bits for network bits.
- More host bits borrowed, the more subnets that can be defined.
- Subnetting on the Octet Boundary
  - Also known as IPv4 Classes
  - Uses the octet boundaries to separate network from hosts.
- Classless Subnetting
  - Uses address bits to separate network from hosts.
  - Allows for much more flexibility.

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

- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Subnet on an Octet Boundary

- 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**	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

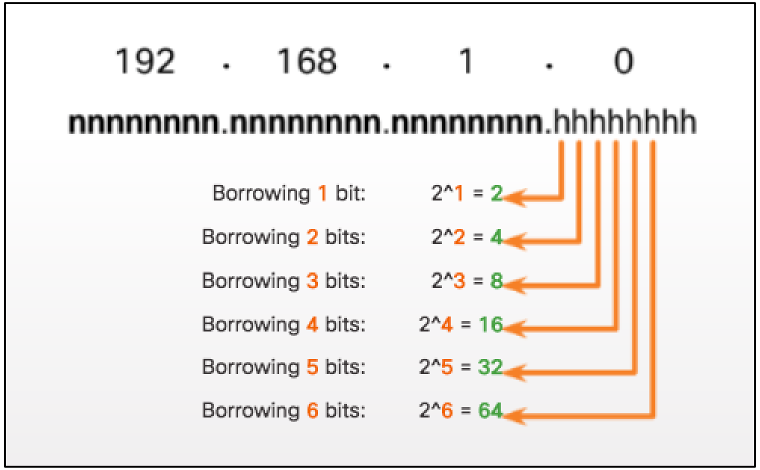
Subnetting Formulas

Calculate the
Number of Subnets

2^B or 2^{B}

B = bits Borrowed

(taken from the host bits)



192 . 168 . 1 . 0

nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh

Borrowing 1 bit: 2^1 = 2

Borrowing 2 bits: 2^2 = 4

Borrowing 3 bits: 2^3 = 8

Borrowing 4 bits: 2^4 = 16

Borrowing 5 bits: 2^5 = 32

Borrowing 6 bits: 2^6 = 64

Calculate the
Number of Hosts

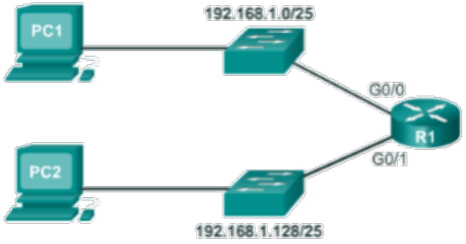
2^U-2 or
$2^{U}-2$

U = Unused bits

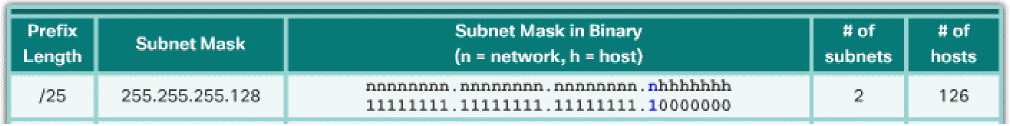
(number of bits remaining in the host)

Subnetting an IPv4 Network

- Creating 2 Subnets from a /24 Prefix
  - A subnet mask of /25 applied to 192.168.10.0, creates two equal subnets, each one with 126 hosts
- Subnetting Formulas
  - Use 2^B, to calculate the number of subnets
    - **B** is the number allocated to the network portion of the address
  - Use 2^U-2 to calculate the number of hosts
    - **U** is the number allocated to the host portion of the address



- Creating 4 Subnets from a /24 Prefix
  - A subnet mask of /26 applied to 192.168.10.0, creates four equal subnets, each one with 62 hosts
  - B = 2 and therefore $2^2 = 4$ Subnets
  - U = 6 and therefore $2^6-2 = 62$ Usable Hosts



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

11.6 Subnet a Slash 16 and a Slash 8 Prefix

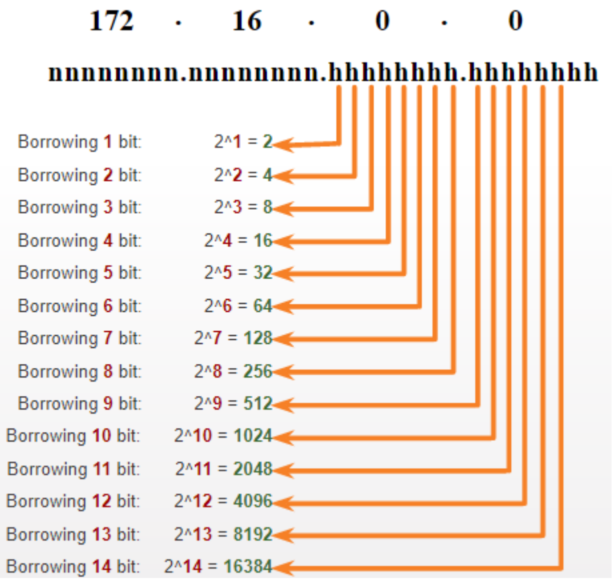
Create Subnets with a Slash 16 prefix

- 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., 27 = 128 subnets) would need to be borrowed (for a total of 128 subnets).



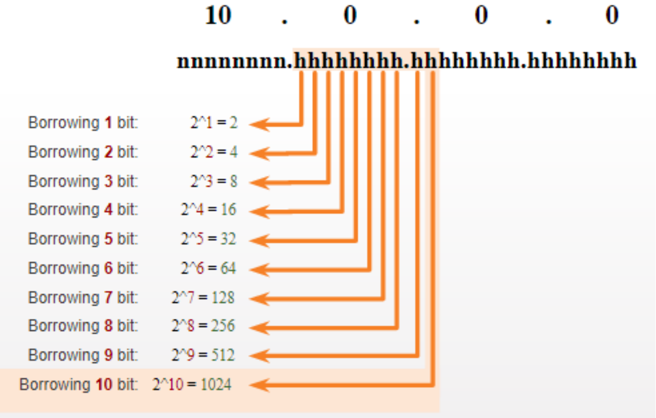
172 . 16 . 0 . 0

nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Borrowing 1 bit:	2^1 = 2
Borrowing 2 bit:	2^2 = 4
Borrowing 3 bit:	2^3 = 8
Borrowing 4 bit:	2^4 = 16
Borrowing 5 bit:	2^5 = 32
Borrowing 6 bit:	2^6 = 64
Borrowing 7 bit:	2^7 = 128
Borrowing 8 bit:	2^8 = 256
Borrowing 9 bit:	2^9 = 512
Borrowing 10 bit:	2^10 = 1024
Borrowing 11 bit:	2^11 = 2048
Borrowing 12 bit:	2^12 = 4096
Borrowing 13 bit:	2^13 = 8192
Borrowing 14 bit:	2^14 = 16384

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 ca 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)


10 . 0 . 0 . 0
nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Borrowing 1 bit: 2^1 = 2
Borrowing 2 bit: 2^2 = 4
Borrowing 3 bit: 2^3 = 8
Borrowing 4 bit: 2^4 = 16
Borrowing 5 bit: 2^5 = 32
Borrowing 6 bit: 2^6 = 64
Borrowing 7 bit: 2^7 = 128
Borrowing 8 bit: 2^8 = 256
Borrowing 9 bit: 2^9 = 512
Borrowing 10 bit: 2^10 = 1024

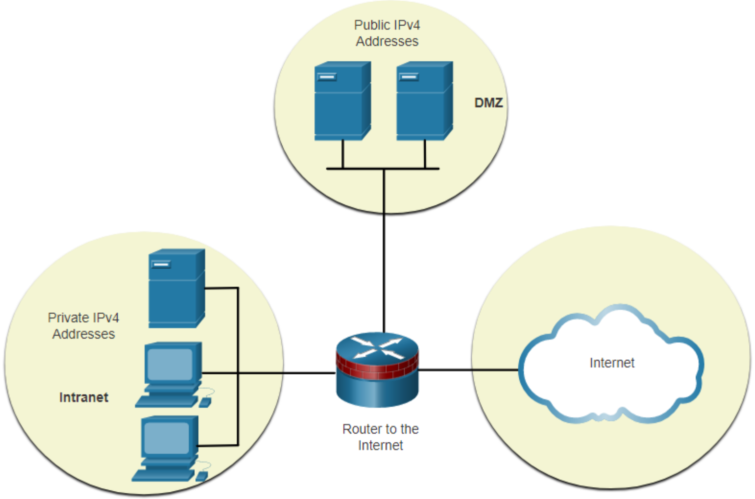
11.7 Subnet to Meet Requirements

Subnetting to Meet Requirements

- Subnetting Based on Host Requirements
  - Two considerations when planning subnets:
    - The number of host addresses required for each network
    - The number of individual subnets needed
- Subnetting Based on Network Requirements
  - Administrators may be asked to subnet an IP range to accommodate a specific number of networks
  - Think of a company with 7 departments where each department must have its own subnetwork
  - The number of hosts per subnet, while secondary, is also important

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 companies 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.



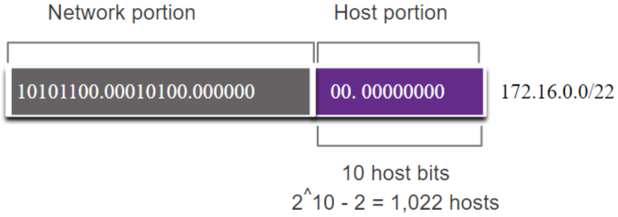
Minimize Unused Host IPv4 Addresses and Maximize Subnets

- 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	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

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.



Network portion

Host portion

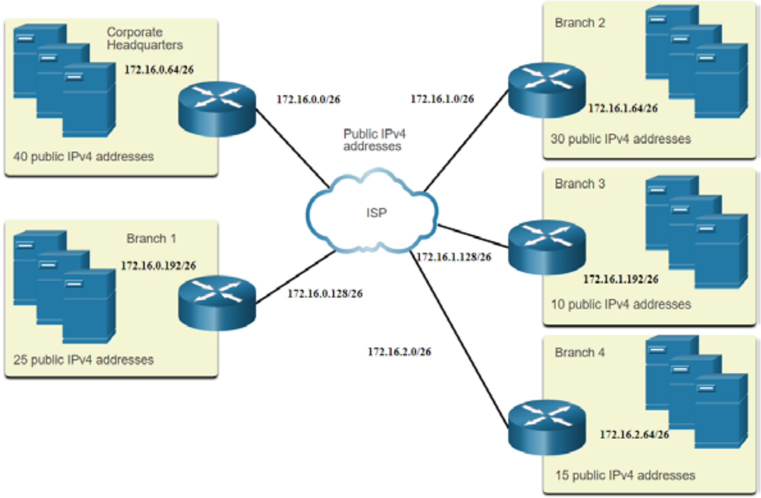
10101100.00010100.000000

00. 00000000

172.16.0.0/22

10 host bits

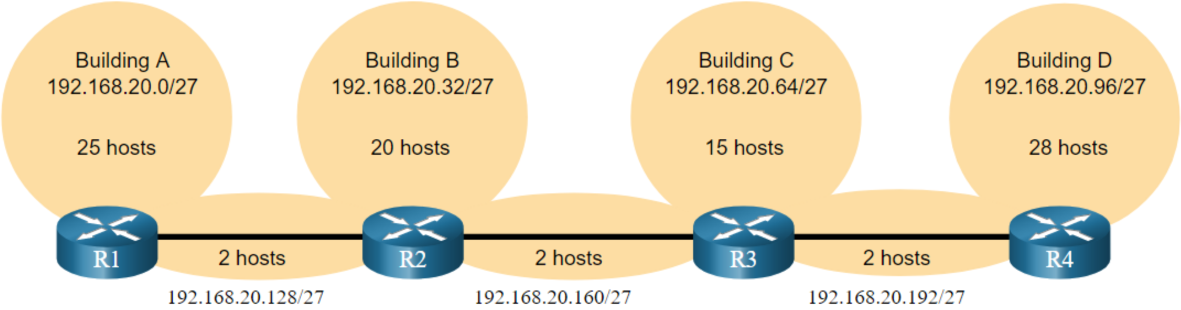
2^10 - 2 = 1,022 hosts



11.8 VLSM

IPv4 Address Conservation

- Given the topology, 7 subnets are required (i.e, four LANs and three WAN links) and the largest number of host is in Building D with 28 hosts.
- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.



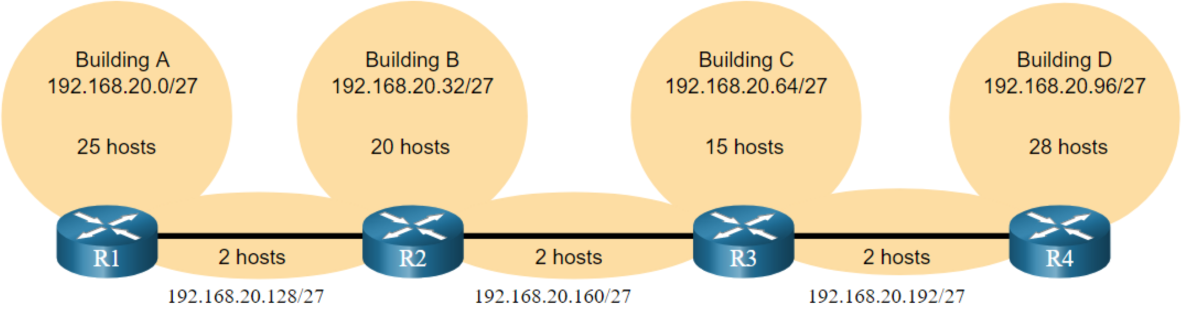
IPv4 Address Conservation

- 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

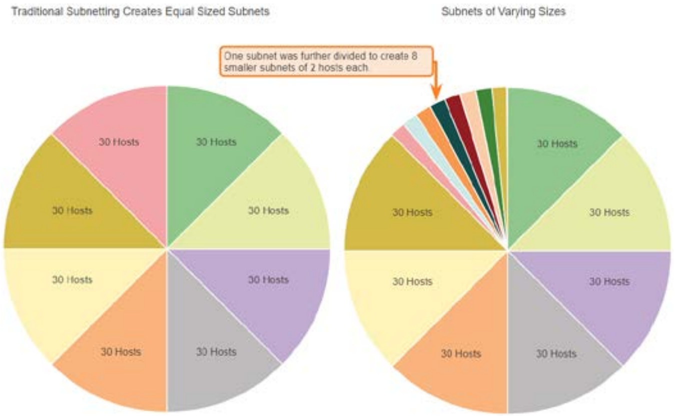
28 x 3 = 84
84 addresses are unused

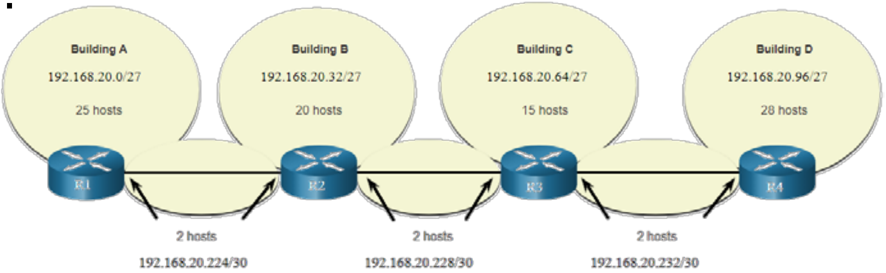


- Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.
- VLSM was developed to avoid wasting addresses by enabling us to subnet a subnet.

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.
- The resulting topology with VLSM applied.

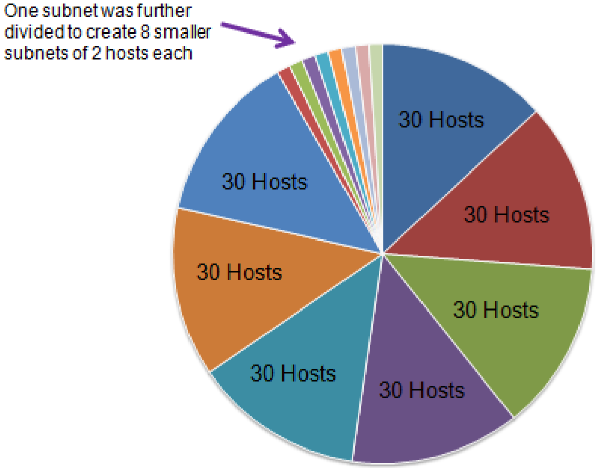




Variable Length Subnet Masks (VLSM)

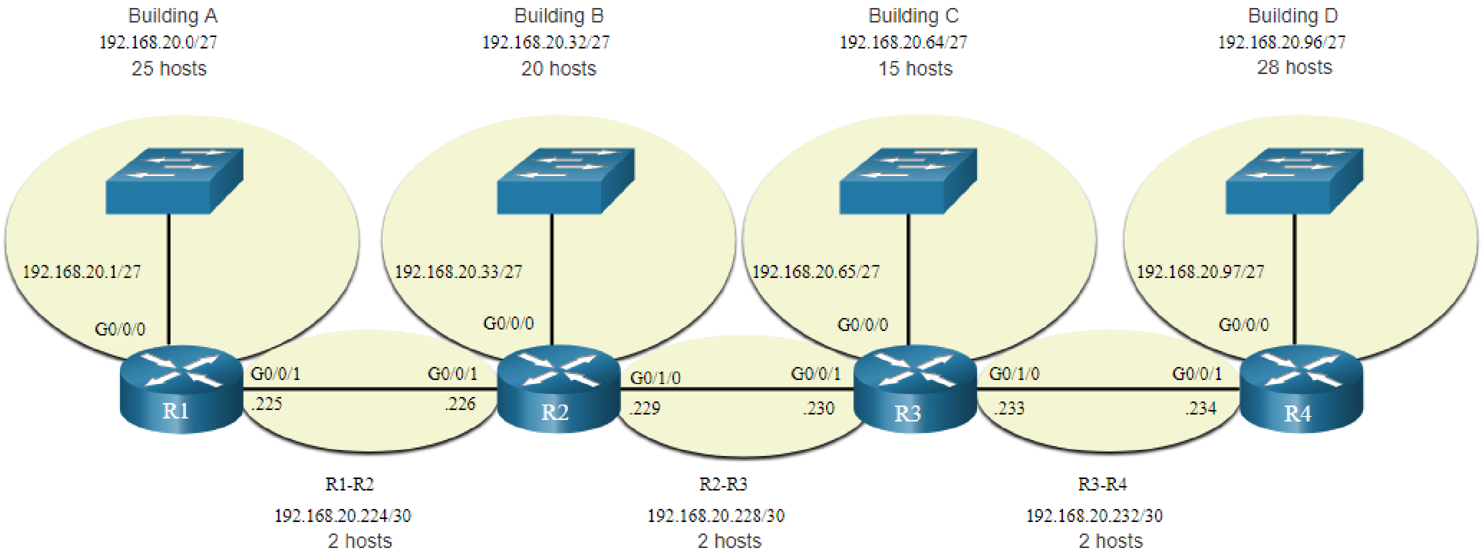
- Variable Length Subnet Mask (VLSM) or subnetting a subnet provides more efficient use of addresses.
  - Allows a network space to be divided in unequal parts.
  - By varying the mask, an administrator has more control.
  - Less waste.
  - Subnet mask will vary depending on how many bits have been borrowed 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.

Subnets of Varying Sizes



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

IPv4 Network Address Planning

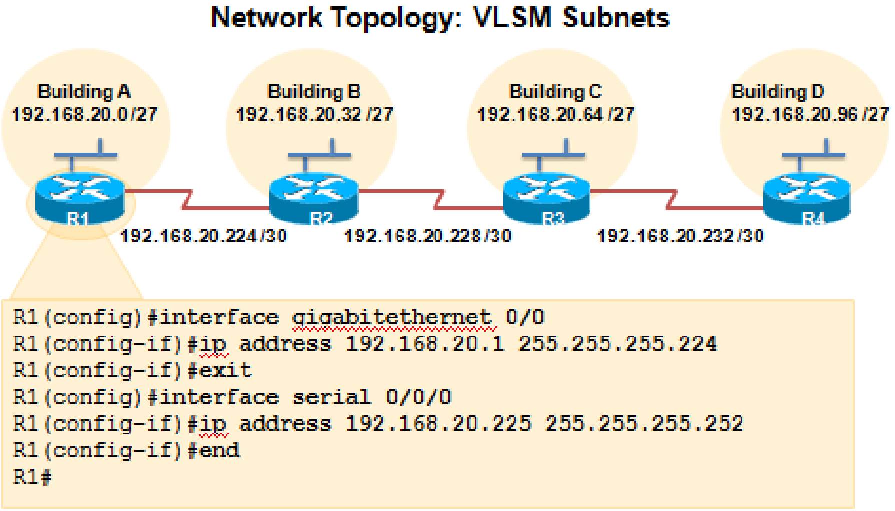
- IP network planning is crucial to develop a scalable solution to an enterprise network.
  - To develop an IPv4 network wide addressing scheme, you need to know how many subnets are needed, how many hosts a particular subnet requires, what devices are part of the subnet, which parts of your network 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.

Device Address Assignment

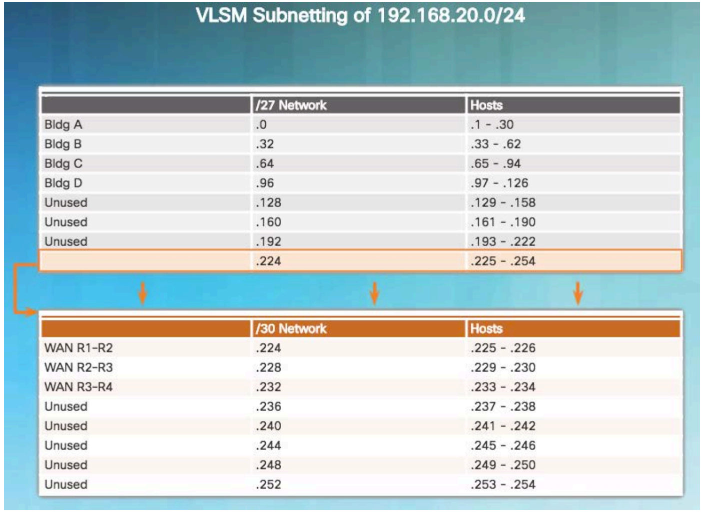
- Within a network, there are different types of devices that require addresses:
  - **End user clients** – Most use DHCP to reduce errors and burden on network support staff. IPv6 clients can obtain address information using DHCPv6 or SLAAC.
  - **Servers and peripherals** – These should have a predictable 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.

VLSM in Practice

- Using VLSM subnets, the LAN and WAN segments in example below can be addressed with minimum waste
- Each LANs will be assigned a subnet with /27 mask
- Each WAN link will be assigned a subnet with /30 mask
- /30 is a preferred match for a serial link


Network Topology: VLSM Subnets

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.20.1 255.255.255.224
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.20.225 255.255.255.252
R1(config-if)#end
R1#
```


VLSM Subnetting of 192.168.20.0/24

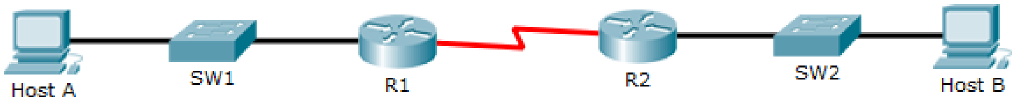
	/27 Network	Hosts
Bldg A	.0	.1 - .30
Bldg B	.32	.33 - .62
Bldg C	.64	.65 - .94
Bldg D	.96	.97 - .126
Unused	.128	.129 - .158
Unused	.160	.161 - .190
Unused	.192	.193 - .222
	.224	.225 - .254

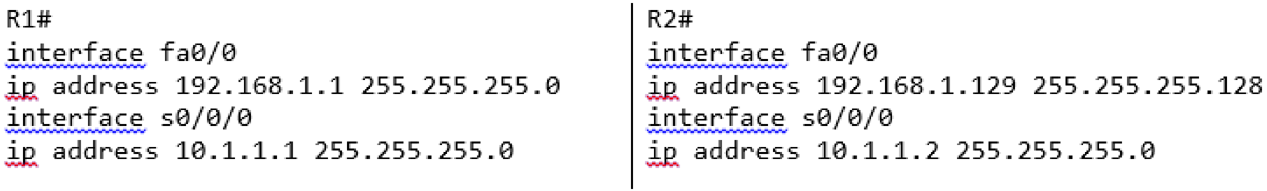
	/30 Network	Hosts
WAN R1-R2	.224	.225 - .226
WAN R2-R3	.228	.229 - .230
WAN R3-R4	.232	.233 - .234
Unused	.236	.237 - .238
Unused	.240	.241 - .242
Unused	.244	.245 - .246
Unused	.248	.249 - .250
Unused	.252	.253 - .254

VLSM in Practice

- What issue is causing Host A to be unable to communicate with Host B?

Host A and host B are on overlapping subnets





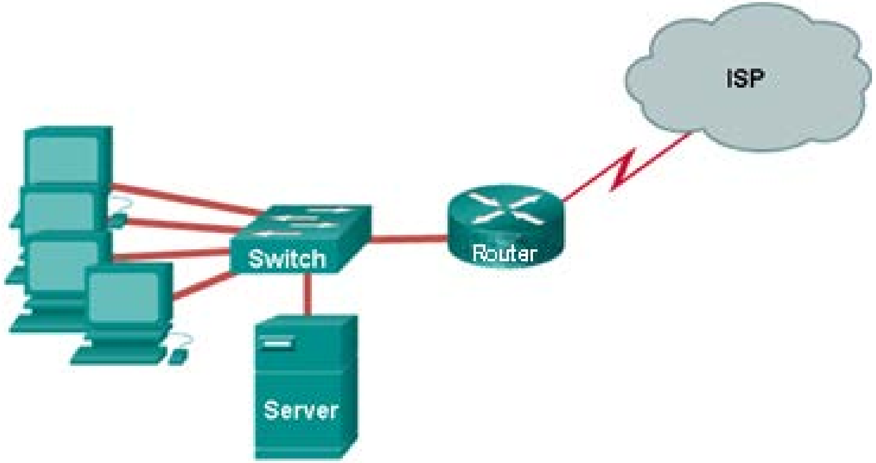
```
R1#
interface fa0/0
ip address 192.168.1.1 255.255.255.0
interface s0/0/0
ip address 10.1.1.1 255.255.255.0
```

```
R2#
interface fa0/0
ip address 192.168.1.129 255.255.255.128
interface s0/0/0
ip address 10.1.1.2 255.255.255.0
```

VLSM in Practice

- You has been given an address range of 192.168.10.0/29. You need to use the fifth subnet to configure the LAN. The router interface gets the first usable host address and the workgroup server is given the last usable host address. Which configuration should be entered on the server?

IP address: 192.168.10.38
Subnet mask: 255.255.255.248
Default gateway: 192.168.10.33



VLSM in Practice

- How many host addresses are available on the network 172.16.128.0 with a subnet mask of 255.255.252.0? **1022**

- Which subnet mask would be used if 5 host bits are available?

  255.255.255.224

- A company has a network address of 192.168.1.64 with a subnet mask of 255.255.255.192. The company wants to create two subnetworks that would contain 10 hosts and 18 hosts respectively. Which two networks would achieve that? (Choose two.)
  - 192.168.1.16/28
  - [✓ 192.168.1.64/27]
  - 192.168.1.128/27
  - [✓ 192.168.1.96/28]
  - 192.168.1.192/28

11.10 Module Practice and Quiz

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?

- 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)

Elk Technologies

https://elktech.org

Scott Stephenson