KEMENTERIAN PENDIDIKAN MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

http://ftmk.utem.edu.my

Chapter 6

by

Dr. Nazrul

nazrulazhar@utem.edu.my

IP ADDRESSING AND SUBNETTING

INTERNET PROTOCOL VERSION 4

BITS 2343 | Computer Network

Objectives

- Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.
- Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.
- Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.

Outline

IPv4 addresses

- Anatomy of an IPv4 address
- Binary-to-decimal conversion
- Decimal-to-binary conversion
- Addressing types of communication: unicast, broadcast and multicast.

IPv4 addresses for different purposes

- Types of addresses in IPv4 network range
- Subnet mask: Defining the network and host portions of the address
- Public and private addresses
- Special unicast IPv4 addresses
- Legacy IPv4 addressing

Outline

Assigning addresses

- Planning to address the network
- Static or dynamic addressing for end-user devices
- Selecting device addresses
- Internet Assigned Numbers Authority (IANA)
- ISPs

Calculating the addresses

- Calculating network, hosts and broadcast addresses
- Basic subnetting
- Subnetting a subnet

Outline

Testing the network layer

- Ping 127.0.0.1: Testing the local stack
- Ping gateway: Testing connectivity to the local LAN
- Ping remote host: Testing connectivity to remote LAN
- Traceroute (tracert): Testing the path
- ICMPv4: The protocol supporting testing and messaging

Overview of IPv6

PART 1

Week 6

(Page 6 → 64)

IPv4 addresses

Anatomy of an IPv4 Address

- Each host in a network must be given a 32-bit address.
- The 32-bit IP address (in binary) is commonly written in dotted decimal notation.
  - The address is divided into 4 octets. Each octet is represented by a binary value.

```
10101001  11000111  01000101  10001001
   169   .   199   .   69    .   137
```

Anatomy of an IPv4 Address

- IP address is divided into two portions: Network portion and Host portion.
  - Network portion is represented by the high-order bits (the most significant bits).
    - The actual number of bits in the network / host portion is specified by the prefix length of the network address.
  - Example: Say that we have a network address 172.6.4.0/24.
    - The /24 network prefix means the leftmost 24 bits are the network portion of the address.
    - The IP address 172.16.4.20 would be an IP address in the network: 172.16.4.20 (network portion . host portion)
- Hosts in the same network must have the same bits for the network portion of their addresses.

Binary-to-decimal Conversion

- Any binary number can be converted to decimal by multiplying the weight of each position with the binary digit and adding together.
- **Example: Convert the binary number** 11110101_2 to its decimal equivalent.

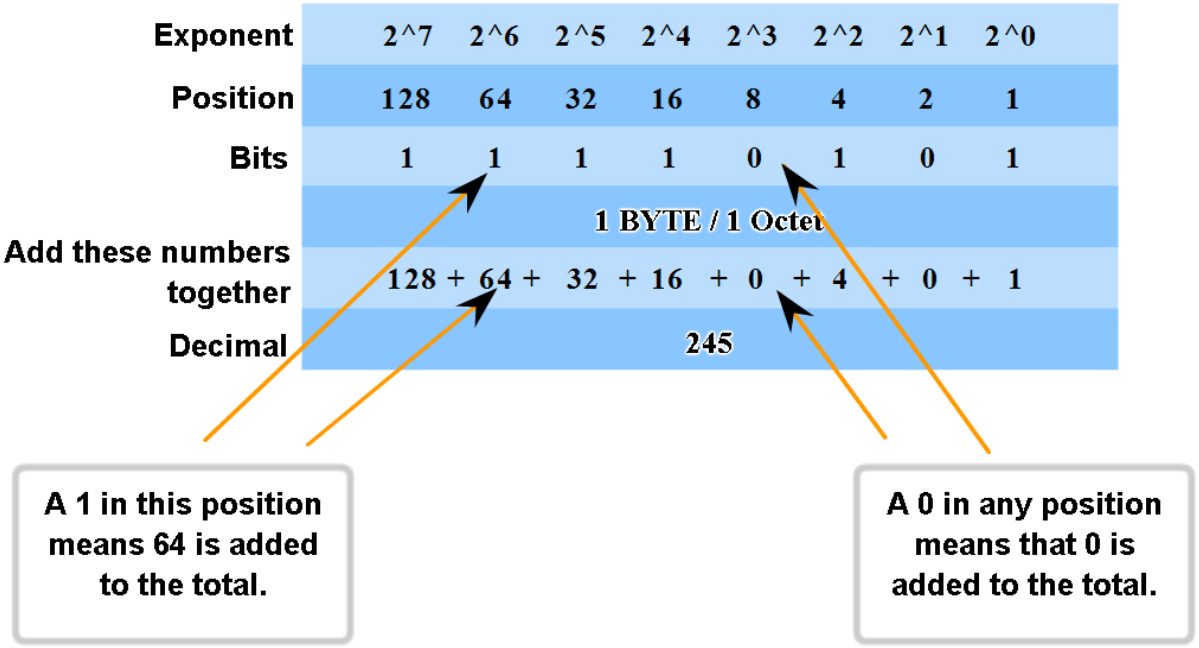
$$11110101_2 = (1 \times 2^7) + (1 \times 2^6) + (1 \times 2^5) + (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0)$$

$$= 128 + 64 + 32 + 16 + 0 + 4 + 0 + 1$$

$$= 245_{10}$$

Binary-to-decimal Conversion

Binary To Decimal Conversion



11110101 in Binary = Decimal Number 245

Decimal-to-binary Conversion

- There are several ways to do this. The most convenient method is called the division by 2 method.
  - Divide the decimal number by 2.
    - This gives two outputs: quotient and remainder.
  - Record the remainder.
  - Divide the quotient by 2.
  - Repeat the process until the quotient becomes 0.
  - The binary representation of the decimal number is the list of remainders recorded.
    - The last remainder is the MSB (the leftmost binary number).

Decimal-to-binary Conversion

- Example: Convert the decimal number 172 to its binary equivalent.
  - 172 / 2 = 86 remainder = 0
  - 86 / 2 = 43 remainder = 0
  - 43 / 2 = 21 remainder = 1
  - 21 / 2 = 10 remainder = 1
  - 10 / 2 = 5 remainder = 0
  - 5 / 2 = 2 remainder = 1
  - 2 / 2 = 1 remainder = 0
  - 1 / 2 = 0 remainder = 1

Read from bottom to top

- Therefore, $172_{10} = 10101100_2$

Unicast, Broadcast and Multicast

- In IPv4 network, hosts can communicate in one of three ways:
  - **Unicast** – from one host to another host.
  - **Broadcast** – from one host to all other hosts in the network.
  - **Multicast** – from one host to a selected group of hosts.
- Each way require a different type of address to be put inside the destination address field in the IP header.

Unicast, Broadcast and Multicast

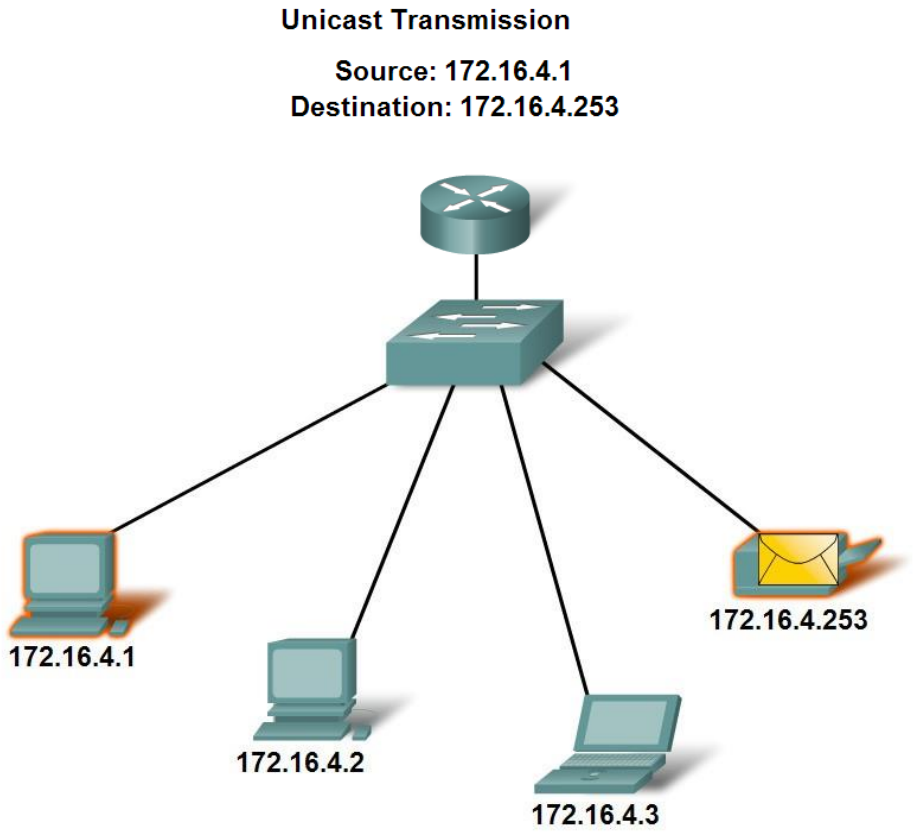
Reserved IPv4 Address Ranges

Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	• used for research or experimentation • cannot currently be used for hosts in IPv4 networks	240.0.0.0 to 255.255.255.254	1700 3330

Unicast Communication and Addresses

- The process of sending a packet from one host to an individual host.
  - Normal host-to-host communication in client/server and peer-to-peer network.
- To perform unicast communication, the address put into the destination address field in the IP header is the IP address of the receiving host.

Unicast Communication and Addresses



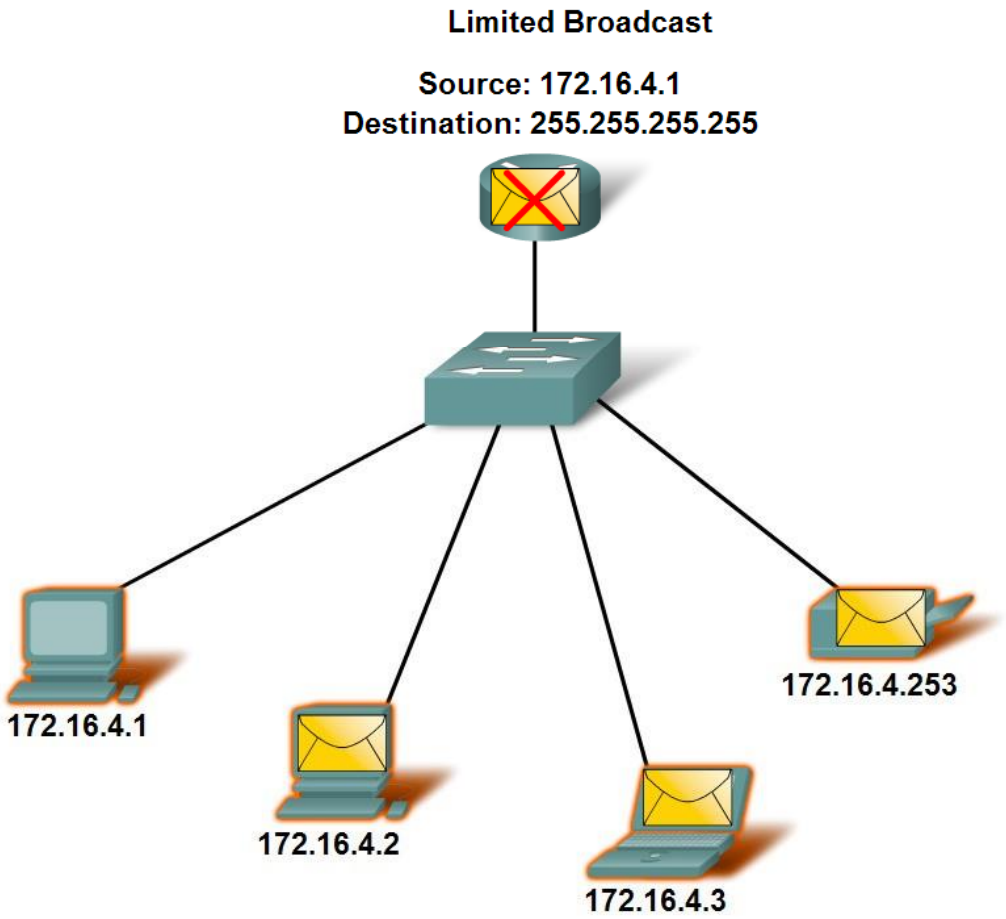
Broadcast Communication and Addresses

- The process of sending a packet from one host to all hosts in the network.
- To perform broadcast communication, the address put into the destination address field in the IP header must be a broadcast address.
- Broadcast is commonly used in the situation where:
  - A host needs to send information to all hosts in the network.
    - Example: Sending routing updates.
  - To find the location of special services / devices for which the address is not known.
    - Example: A newly connected host that tries to find a DHCP server.

Broadcast Communication and Addresses

- There are two types of broadcasts, each with its own broadcast address.
  - Limited broadcast
  - Directed broadcast
- Limited broadcast is used to send a packet to all hosts in the local network.
  - Destination address used is 255.255.255.255.
  - Broadcast is limited to the local network because routers do not forward a limited broadcast packet.

Broadcast Communication and Addresses



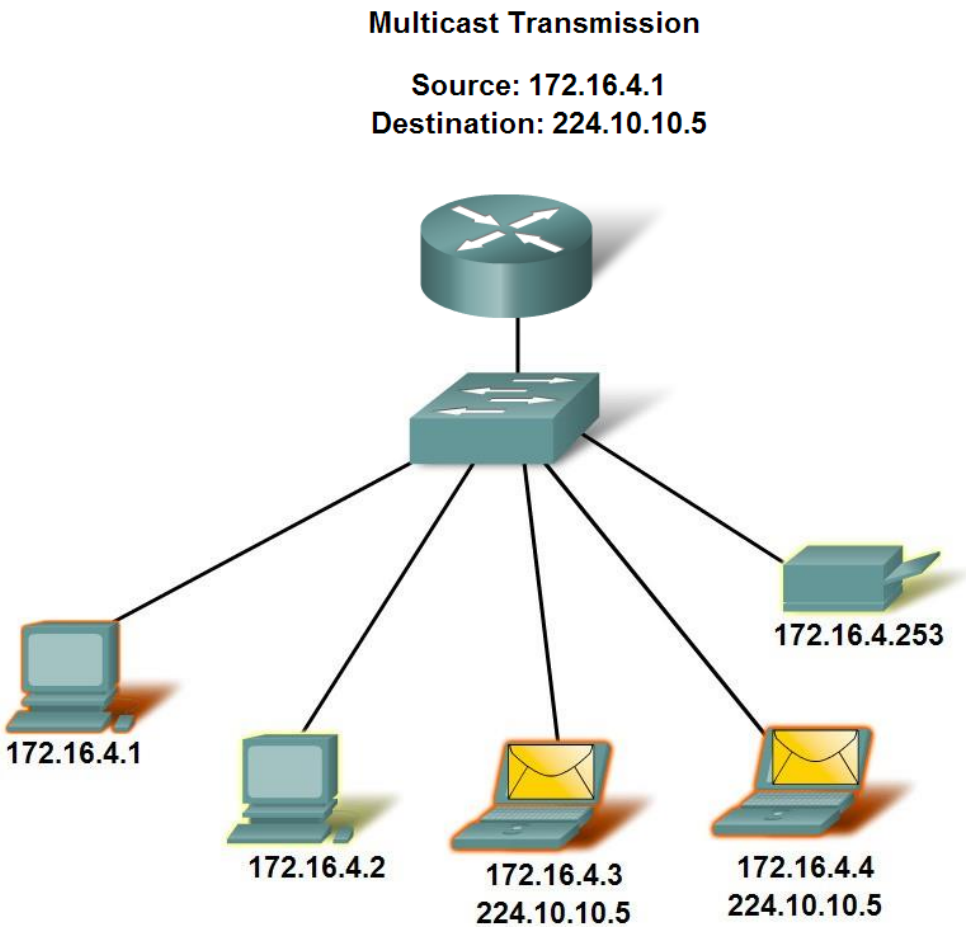
Broadcast Communication and Addresses

- Directed broadcast is used to send a packet to all hosts in a specific network.
  - The destination address used is the highest address in a network.
    - Address with all 1s in the host portion.
  - Example: For the network 172.16.4.0/24, the destination address used to send a broadcast all to hosts in this network is 172.16.4.255.
- Directed broadcast is useful to send a broadcast to all hosts on a non-local network.

Multicast Communication and Addresses

- The process of sending a packet from one host to a selected set of hosts.
- To receive a multicast packet, a host must join a multicast group.
- A multicast group is identified using an IP address in the multicast range.
  - IPv4 multicast addresses: 224.0.0.0 – 239.255.255.255
- To send a multicast packet to a particular multicast group, the address put into the destination address field in the IP header is the multicast IP address assigned to this group.

Multicast Communication and Addresses



Multicast Communication and Addresses

- The IPv4 multicast address range (224.0.0.0 – 239.255.255.255) is sub-divided into two types.
  - Reserved link-local addresses
    - 224.0.0.0 – 224.0.0.255
    - Used for multicast groups in a local network.
    - Only valid within the local network.
  - Globally scoped addresses
    - 224.0.1.0 – 239.255.255.255
    - Used to multicast data across the Internet.

IPv4 addresses for different purposes

Types of Addresses in IPv4 Network Range

- A particular IPv4 network will have a range of addresses to be used in that network.
  - Example: The network 172.20.23.0/24 will have the address range from 172.20.23.0 – 172.20.23.255.
- This range of addresses can be divided into three types:
  - Network address
  - Broadcast address
  - Host address
- Host addresses are the ones assigned to the individual hosts.

Types of Addresses in IPv4 Network Range

- Network address is used to refer to a network.
  - This would be the lowest address in the range.
  - It has a 0 for each host bit in the host portion of the address.
- Broadcast address is used to do a directed broadcast to all hosts in the network.
  - This would be the highest address in the range.
  - It has a 1 for each host bit in the host portion of the address.

Types of Addresses in IPv4 Network Range

Address Types

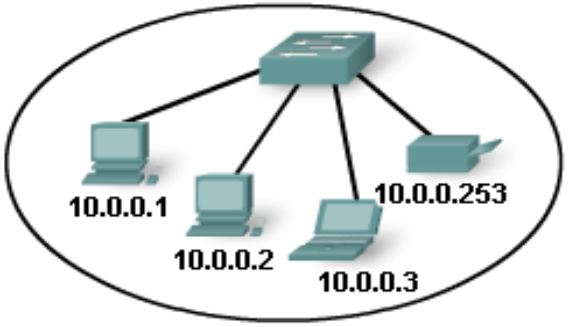
Network Address

Broadcast Address

Host Address

Roll over to learn more.

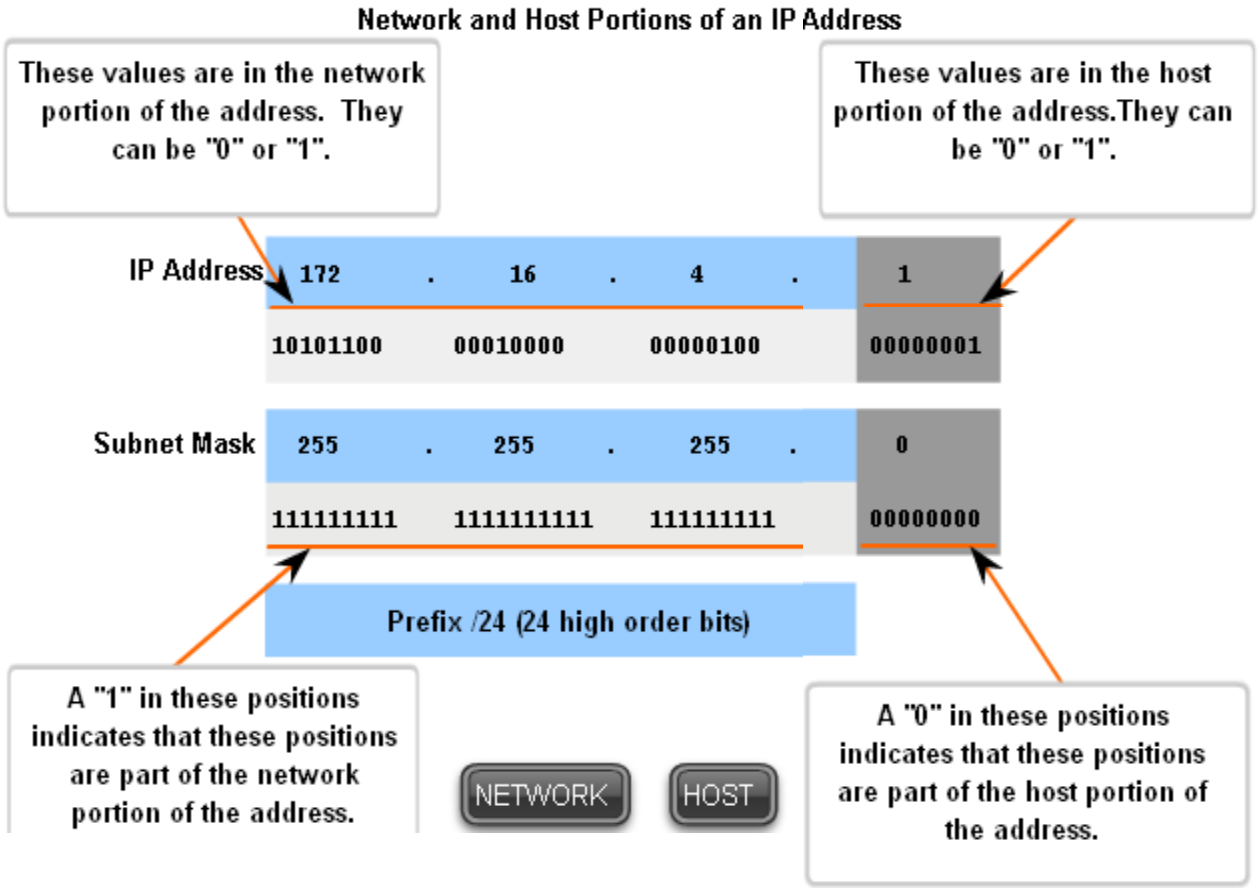
	Network		Host
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001



Subnet Mask

- Subnet mask and prefix length are two different ways of representing the same information which is to define the network portion of an IP address.
- Subnet mask is a 32-bit value, and uses a dotted decimal notation (same like IP address).
  - Example: 255.255.255.0
  - In binary: 11111111 11111111 11111111 00000000
  - Value 1 in the subnet mask represents bit position of the network portion.
  - Value 0 in the subnet mask represent bit position of the host portion.

Subnet Mask


Network and Host Portions of an IP Address
These values are in the network portion of the address. They can be "0" or "1".
These values are in the host portion of the address.They can be "0" or "1".
IP Address
172 . 16 . 4 . 1
10101100 00010000 00000100 00000001
Subnet Mask
255 . 255 . 255 . 0
111111111 1111111111 111111111 00000000
Prefix /24 (24 high order bits)
A "1" in these positions indicates that these positions are part of the network portion of the address.
NETWORK
HOST
A "0" in these positions indicates that these positions are part of the host portion of the address.

Subnet Mask

- Recall that a router forwards packets using its routing table.
  - The routing table contains a list of destination networks and the router interface that the packet should be forwarded to in order to reach that destination network.
- When a packet comes in, the router needs to find the destination network from the destination IP address inside the packet's header.
- This is done by ANDing the IP address with the subnet masks of potential routes.
  - This yields a network address that is compared to the route from the routing table whose subnet mask was used.

Subnet Mask

- Example:
  - Given the IP address **172.16.4.35** and subnet mask **255.255.255.224**, find the network address on which this IP address is located.
- Since subnet mask and prefix length can both be used to represent the same information, the question can also be rephrased like this:
  - Find the network address of the IP address 172.16.3.35/27.

255.255.255.224 = /27

Dot-decimal notation Slash notation

Subnet Mask

Answer:

1. Convert the host address and Mask to binary
2. ANDing host address with Mask
3. Convert the answer to decimal

	Dotted Decimal				Binary Octets			
Host	172	16	4	35	10101100	00010000	00000100	00100011
Mask	255	255	255	224	11111111	11111111	11111111	11100000
Network	172	16	4	32	10101100	00010000	00000100	00100000

ANDing

Network address : 172.16.4.32

Public and Private Addresses

- **Public IP** addresses are addresses that are publicly accessible from the Internet.
  - Most of the addresses in the IP address range are public IP addresses.
  - A host using a public IP address can be accessed by any other host in the Internet.
- **Private IP** addresses are addresses that only valid within a certain private network.
  - These addresses cannot be accessed directly by other hosts in the Internet.
  - Used by hosts that require limited or no Internet access.

Public and Private Addresses

- The IP address ranges below have been reserved be used as private IP addresses:
  - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- A public IP address must be unique throughout the whole Internet.
- A private IP address must be unique only within the private network in which it is used.
  - A private IP address can be used by multiple hosts, as long as they are located in different private networks.

Public and Private Addresses

- Private IP addresses are not valid within the public Internet.
  - If an Internet routers receives a packet with destination IP address 10.10.10.100, it cannot forward this packet.
- This can cause problem when a host with a private IP address wants to communicate with an Internet host using a public IP address.
  - The problem occurs when the Internet host wants to reply back to the host with the private IP address.
  - The reply cannot be sent because destination address is a private IP address.

Public and Private Addresses

- A solution to this would be to use the network address translation (NAT) service.
  - This allows packets with a private IP address to have its source IP address (which is initially a private IP address) converted to a public IP address at the edge router.
    - This IP address would be the address of the edge router.
  - The packet would then travels the Internet with a public IP address as the source address.
  - When the receiving host wants to send a reply, this reply will be sent to the edge router of the private network.
  - The edge router would then convert back the destination IP address to a private address belonging to the sending host.

Special Unicast IPv4 Addresses

- There are addresses in the IPv4 address range that are not normally assigned to hosts, but instead reserved for special purposes.
- These addresses are:
  - Default route
  - Loopback address
  - Link-local address
  - Test-net addresses

Default Route

- Default route refers to the address 0.0.0.0.
  - The use of this address also reserves all addresses in the range 0.0.0.0/8 (0.0.0.0 – 0.255.255.255).
  - None of the addresses in this range can be assigned to an Internet host.
- Default route is used by routers in their routing tables to define a “catch all” route when a more specific route is not available.

Loopback Address

- IPv4 loopback addresses are the addresses in the range of 127.0.0.1 to 127.255.255.255.
- Loopback address is used by hosts to direct traffic to themselves.
  - If a host sends a packet with a loopback address as the destination IP address, the packet will be delivered to itself.
  - This address cannot be assigned to any Internet host.
- The loopback address is mainly used for testing.
  - To test the TCP/IP configuration of a host.
  - Used by developers to test network applications.

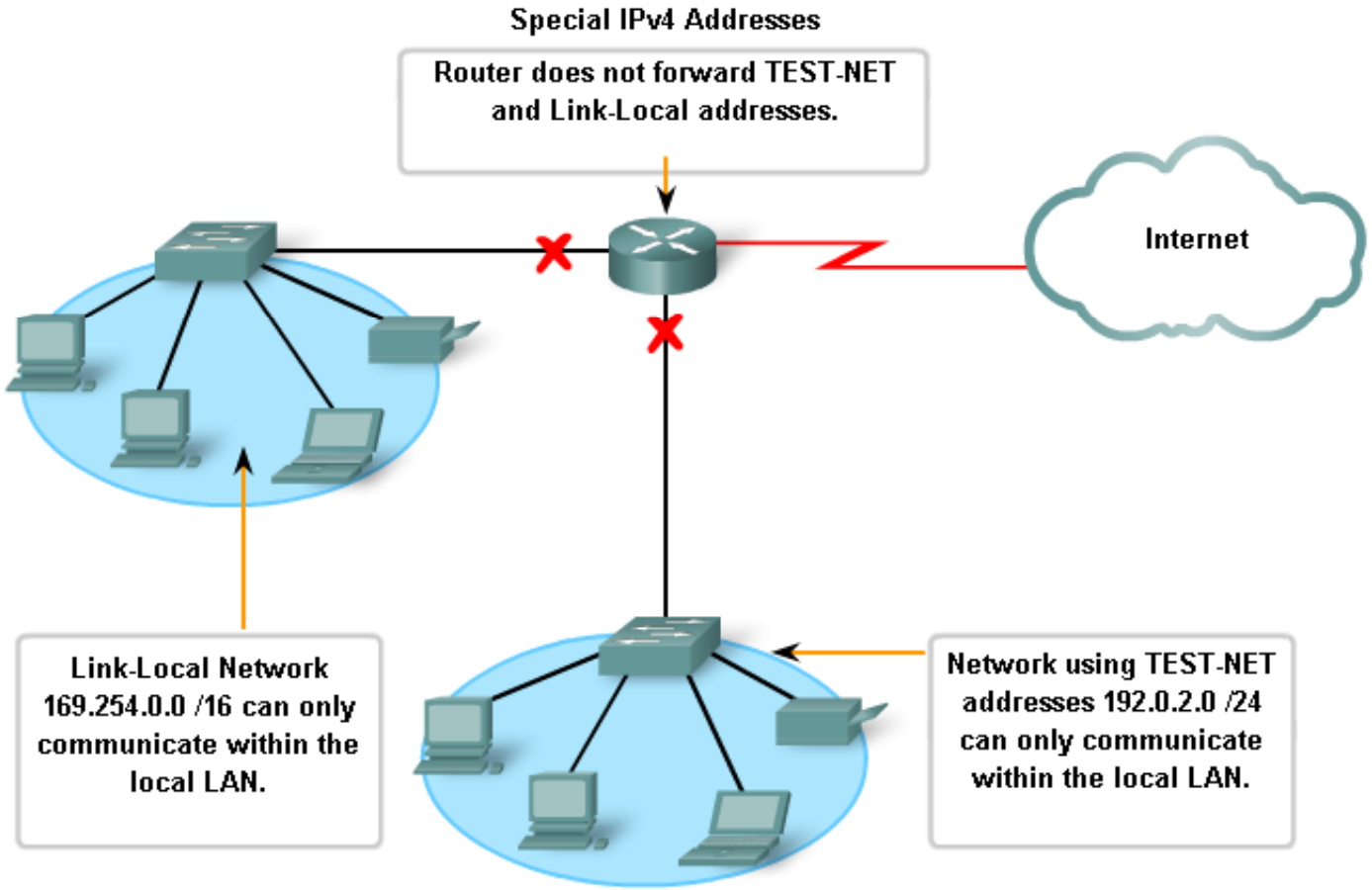
Link-local Address

- IPv4 link-local addresses are the addresses in the range of 169.254.0.0 to 169.254.255.255 (169.254.0.0/16).
- Link-local addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available.
- Link-local addresses are only valid within the local network.
  - Routers do not forward packets with link-local address as the source address.

Test-net Addresses

- IPv4 test-net addresses are the addresses in the range of 192.0.2.0 to 192.0.2.255 (192.0.2.0/16).
- Test-net addresses are set aside for teaching and learning purposes.
- Test-net addresses can actually be assigned to hosts in the network.
  - However, these addresses are only valid within the local network.
  - Routers do not forward packets with test-net address as the source address.

Link-local and Test-net Addresses



Legacy IPv4 Addressing

- In the early 1980s, IPv4 addressing range was divided into several classes (defined in RFC 1700):
  - Class A, Class B and Class C for unicast.
  - Class D for multicast.
  - Class E for experiment.
- Each unicast class represents networks of a specific size.
  - The number of bits for the network portion is different for each of the unicast class.
- Each class has its own address range.
  - The classes can be identified by examining the higher order bits.

Legacy IPv4 Addressing

IP Address Classes

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

** All zeros (0) and all ones (1) are invalid hosts addresses.

Legacy IPv4 Addressing

- In those days, companies / organizations who request for an address block will be given an entire Class A, B or C address block.
  - The use of IP address space this way is called classful addressing.
- The use of classful addressing can be a waste of address space.
  - Example: Say that your company has 2000 computers to be connected to the network.
    - Using class C, you can only support 254 hosts.
    - So you have to use class B.
    - But class B can support 65534 hosts. So the extra addresses are wasted.

Classless Addressing

- The addressing system that we are currently using is referred to as classless addressing.
- With classless addressing, the network portion of an address block can be of any length.
  - No longer restricted to having the network portion only be 8,16 or 24 bits as in classful addressing.
  - Organizations that ask for an IP address block will be given an address block appropriate for the number of hosts that it has.
- Referring back to the previous example, the company can be given an IP address block with /21.

Assigning addresses

Planning to Address the Network

- When assigning IP addresses to a network, it should be properly planned and documented.
- This is important because:
  - To prevent duplication of addresses.
  - To make it easier to provide and control access to certain hosts.
  - To make it easier to monitor the security and performance of the network.
- Other considerations in planning network addressing:
  - Which hosts should be given private / public addresses.
  - Which hosts should be given static / dynamic addresses.

Static or Dynamic Addressing for End-user Devices

- With the static assignment, the network information for a host must be manually configured.
- Commonly used for network devices that need to be accessed by other hosts in the network.
  - Servers, printers, etc.
  - For these devices, it would cause a service disruption if the IP address keeps changing.
- Static assignment of addressing information can provide increased control of network resources.
- However it can be time consuming to enter the information on each host.

Static or Dynamic Addressing for End-user Devices

- Dynamic addressing is done by using DHCP.
  - Hosts will automatically get network configuration information once it is connected to the network.
  - Require a DHCP server to be set up in the network.
- Addresses to the hosts on large networks.
  - Reduce the burden on network staff and virtually eliminates the entry errors.
- Address assigned using DHCP is not permanent.
  - If the host is powered down or taken off from the network the address is available for other hosts.

Selecting Device Addresses

- Within a network, there can be different types of hosts. For example:
  - End devices for users
  - Servers and peripherals
  - Hosts that are accessible from the Internet
  - Intermediary devices
- End devices for users are normally given private IP addresses assigned using DHCP.
  - These devices are not accessed by other hosts.
  - It does not matter what IP address they use.

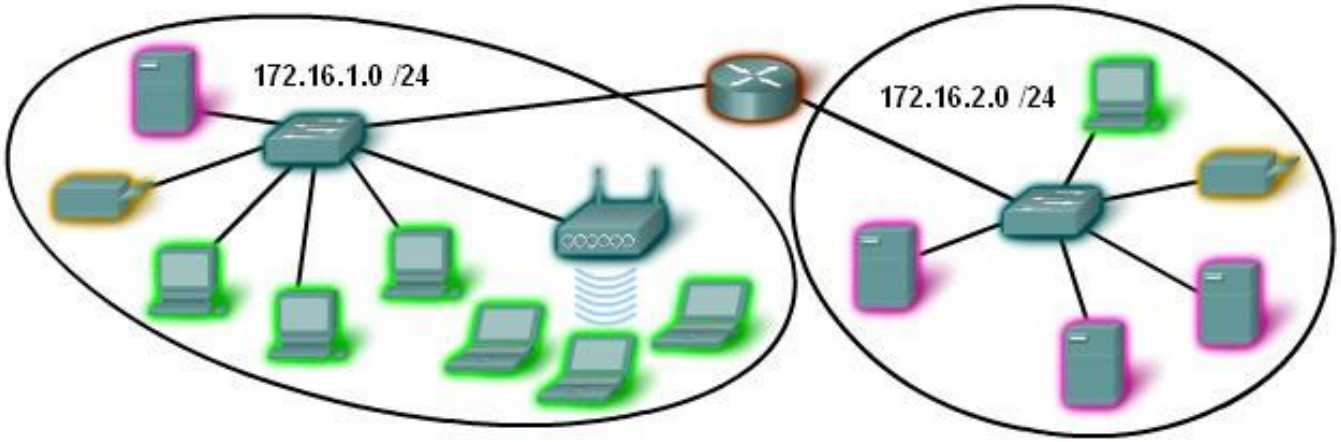
Selecting Device Addresses

- Servers and peripherals should be given a static IP address.
  - This will make it easier for other hosts to access them.
- Hosts that are accessible from the Internet must be given a static, public IP address.
  - Public IP address is important to enable them to be accessible by hosts in the Internet.
- Intermediary devices (switches, routers, firewalls) should be given a static IP address.
  - This will make it easier for them to be accessed by network administrators.

Selecting Device Addresses

Devices IP Address Ranges

Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



Internet Assigned Numbers Authority (IANA)

- The use of public IP addresses is managed by the Internet Assigned Number Authority (IANA).
  - http://www.iana.net
- However, the actual assignment of IP addresses is done by the regional Internet registries:
  - AfriNIC (African Network Information Centre)
  - APNIC (Asia Pacific Network Information Centre)
  - ARIN (American Registry for Internet Numbers)
  - LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  - RIPE NCC (Reseaux IP Europeans)

ISPs

- Users get their IP addresses from Internet Service Providers (ISPs).
- Home users are normally given just one IP address.
  - This address can be fixed or dynamic, depending on the package offered by the ISP.
- Companies and organizations are normally given a block of IP addresses.
  - The number of IP addresses given depends on the number of hosts in the company.
  - If a company requires 200 IP addresses, the ISP may give an address block with prefix length /24.
    - Example: 169.20.34.0/24

ISPs

- To provide Internet connectivity and related services, ISPs have their own set of internal data network.
  - Routers, DNS server, DHCP server, e-mail server, etc.
- Similar to IP address, ISPs are also hierarchical.
  - Tier 1 ISPs – Large national or international ISPs that are directly connected to the Internet backbone.
  - Tier 2 ISPs – Subscribe their Internet connection from Tier 1 ISPs and normally focus on business customers.
  - Tier 3 ISPs – Subscribe their Internet connection from Tier 2 ISPs and provide service to home users.

Calculating the addresses

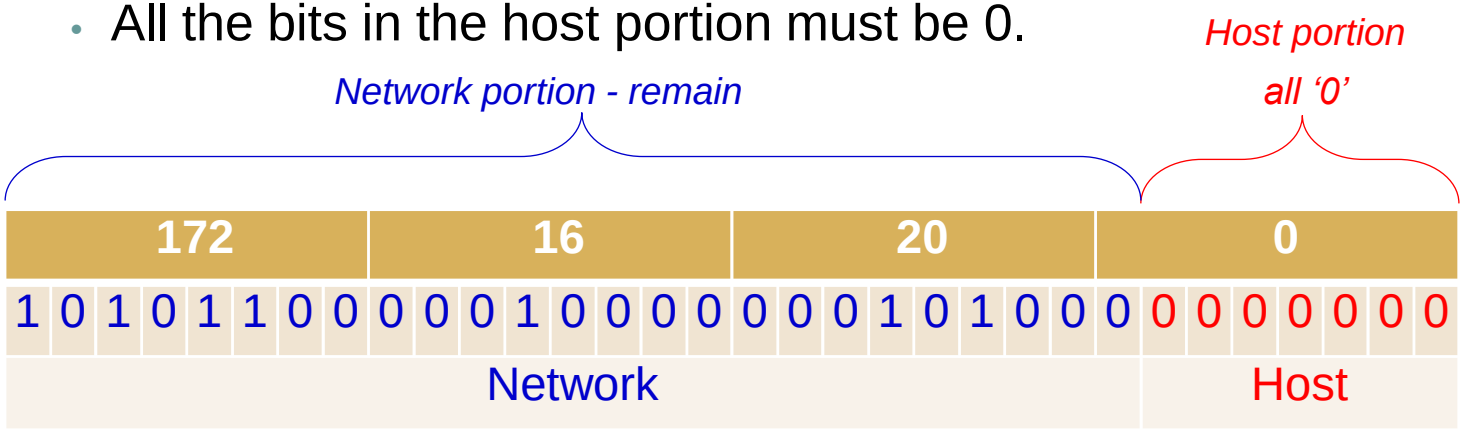
Calculating the Network, Host and Broadcast Addresses

- As discussed earlier, companies or organizations get a block of IP addresses from an ISP.
  - These addresses would then need to be assigned to hosts in the network.
- In assigning IP addresses to hosts in a network, it is important to figure out the following addresses:
  - Network address
  - Range of host addresses
  - Broadcast address
- **Example**: Say that a company is given the address block 172.16.20.0/25. Find the Network Address, Range of host addresses and Broadcast address

Calculating the Network, Host and Broadcast Addresses

Step 1: Calculate the Network address.

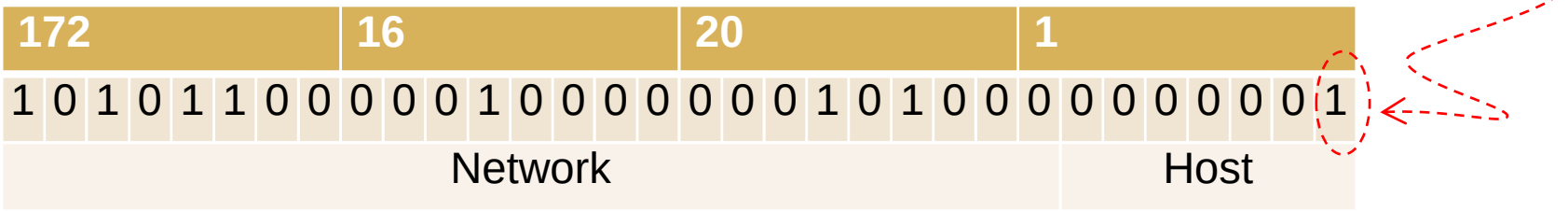
- Network address = the lowest address in the address block.
- The address block given has a prefix length of /25. This means the network portion has 25 bits and the host portion has 7 bits.
- All the bits in the host portion must be 0.



Therefore, the **Network address is 172.16.20.0**

Calculating the Network, Host and Broadcast Addresses

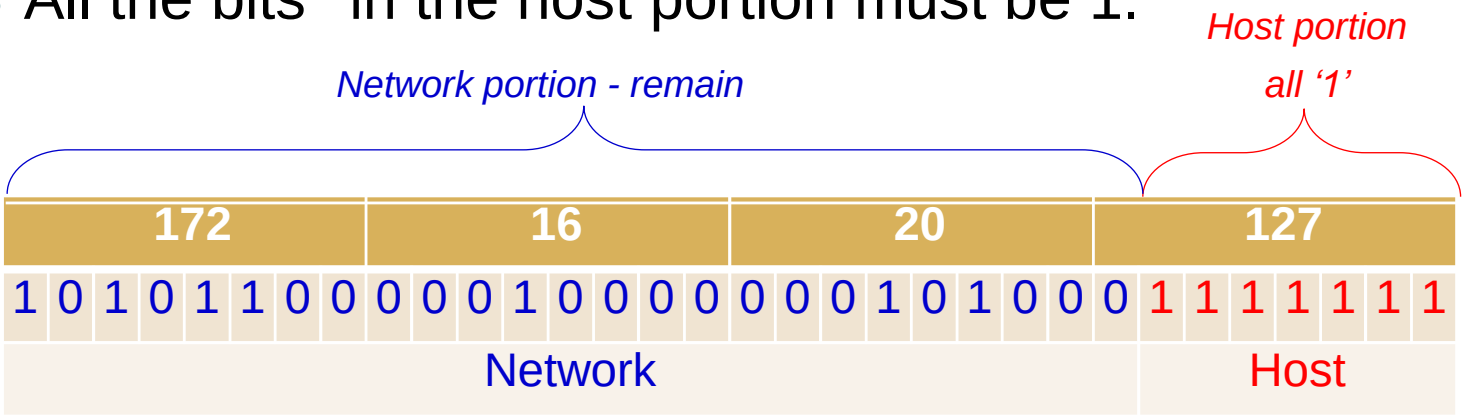
- **Step 2: Calculate the lowest host address.**
  - The lowest host address is always 1 greater than the network address.
  - The last host bit must be equal to binary 1.



Therefore, the lowest host address is **172.16.20.1**

Calculating the Network, Host and Broadcast Addresses

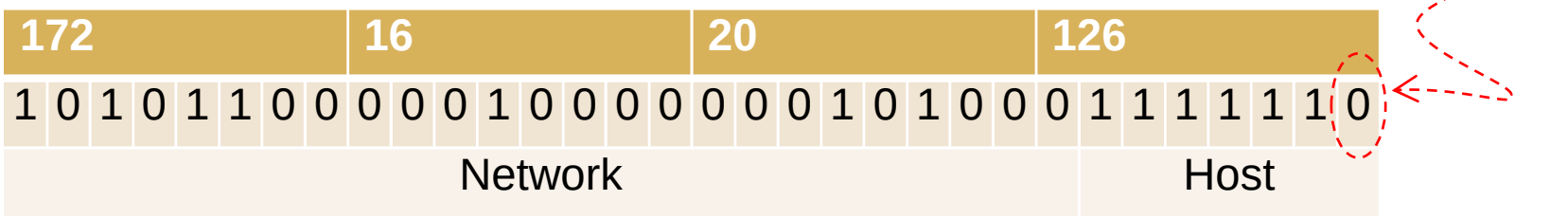
- **Step 3: Calculating the Broadcast address.**
  - Broadcast address = the highest address in the address block.
  - All the bits in the host portion must be 1.



Therefore, the **Broadcast address is 172.16.20.127**

Calculating the Network, Host and Broadcast Addresses

- **Step 4: Calculating the highest host address.**
  - The highest host address is 1 less than the broadcast address.



Therefore, the highest host address is **172.16.20.126**

Calculating the Network, Host and Broadcast Addresses

- **Step 5: Determine the host address range.**
  - The host address range refers to the addresses that can be assigned to hosts.
  - This range should be from the lowest host address (calculated in Step 2) to the highest host address (calculated in Step 4).
  - For this example, the host address range for the address block 172.16.20.0/25 is from 172.16.20.1 to 172.16.20.126.

Range of host addresses

= Lowest → Highest host addresses

= 172.16.20.1 → 172.16.20.126

PART 2

Week 7

(Page 65 → 93)

Basic Subnetting

- Subnetting refers to the technique used to create multiple logical networks (subnets) from a single address block.
- The main idea is to use one or more host bits in the address block as network bits.
- The more host bits used, the more subnets can be created.
- However, with each host bits borrowed, fewer host addresses are available per subnet.

Basic Subnetting

- Example 1: Create two subnets from the address block 192.168.1.0/24.
- Step 1: Find out how many host bits need to be used.
  - Formula: Number of subnets = 2^n (where *n* is the number of host bits required)
  - Since we need to create 2 subnets, $2 = 2^n$.
    - Therefore $n = 1$.
  - The leftmost bit of the host portion is now used to differentiate between the two subnets.
    - Subnet 0: **0**0000000 (0)
    - Subnet 1: **1**0000000 (128)

Basic Subnetting

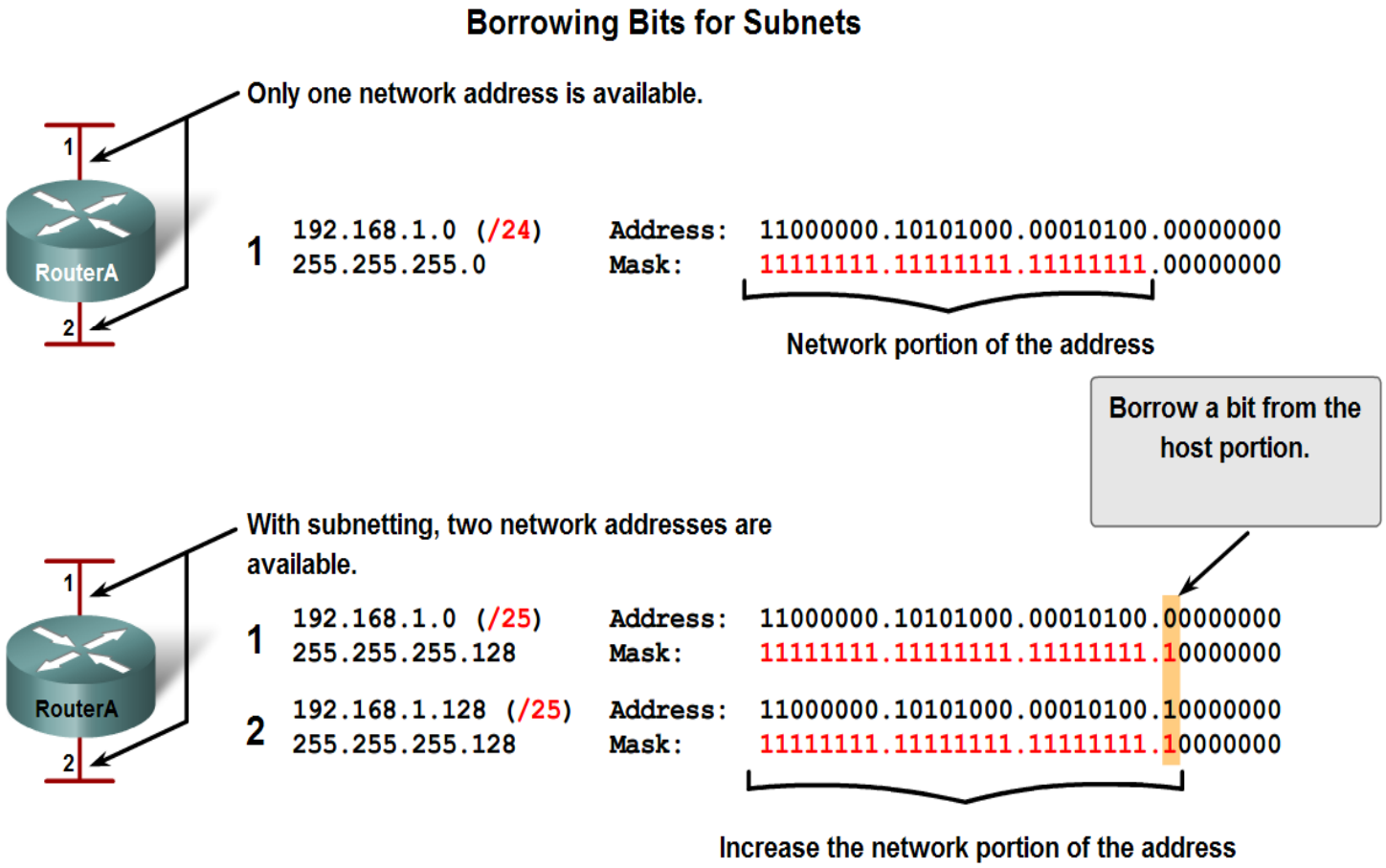
- Step 2: Find out the number of hosts per network.
  - Formula: Number of hosts = $2^n - 2$ (where n is the number of bits in the host portion).
    - Why need to minus 2?
      - Because the lowest address in the range is used for the network address and the highest address in the range is used for the broadcast address.
  - Since we have borrowed 1 bit, the host portion now only has 7 bits ($n = 7$).
  - Number of hosts = $2^7 - 2 = 128 - 2 = 126$.

Basic Subnetting

- Step 3: Identify the subnet mask, network address, host address range and broadcast address.
  - The two new subnets now has 25 bits for network portion and 7 bits for host portion.
    - Therefore, the subnet mask is 255.255.255.128 (prefix /25).
  - The network address, host address range and broadcast address can be calculated using the technique discussed earlier.

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0 /25	192.168.1.1 to 192.168.1.126	192.168.1.127
1	192.168.1.128 /25	192.168.1.129 to 192.168.1.254	192.168.1.255

Basic Subnetting



Basic Subnetting

- Example 2: Create eight subnets from the address block 192.168.1.0/24.
- Step 1: Find out how many host bits need to be used.
  - $2^n = 8$, therefore $n = 3$.
  - The three leftmost bits of the host portion is now used to differentiate between the eight subnets.
    - Subnet 0: **000**00000 (0)
    - Subnet 1: **001**00000 (32)
    - Subnet 2: **010**00000 (64)

Basic Subnetting

- Subnet 0: **000**00000 (0)
- Subnet 1: **001**00000 (32)
- Subnet 2: **010**00000 (64)
- Subnet 3: **011**00000 (96)
- Subnet 4: **100**00000 (128)
- Subnet 5: **101**00000 (160)
- Subnet 6: **110**00000 (192)
- Subnet 7: **111**00000 (224)

- Step 2: Find out the number of hosts per network.
  - Since we have borrowed 3 bits, the host portion now only has 5 bits ($n = 5$).
  - Number of hosts = $2^5 - 2 = 32 - 2 = 30$

Basic Subnetting

- Step 3: Identify the subnet mask, network address, host address range and broadcast address.
  - The two new subnets now has 27 bits for network portion and 5 bits for host portion.
    - Therefore, the subnet mask is 255.255.255.224 (prefix /27).
  - The network address, host address range and broadcast address are as follows:

Basic Subnetting

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0 /27	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32 /27	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64 /27	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96 /27	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128 /27	192.168.1.129 to 192.168.1.158	192.168.1.159
5	192.168.1.160 /27	192.168.1.161 to 192.168.1.190	192.168.1.191
6	192.168.1.192 /27	192.168.1.193 to 192.168.1.222	192.168.1.223
7	192.168.1.224 /27	192.168.1.225 to 192.168.1.254	192.168.1.255

Basic Subnetting

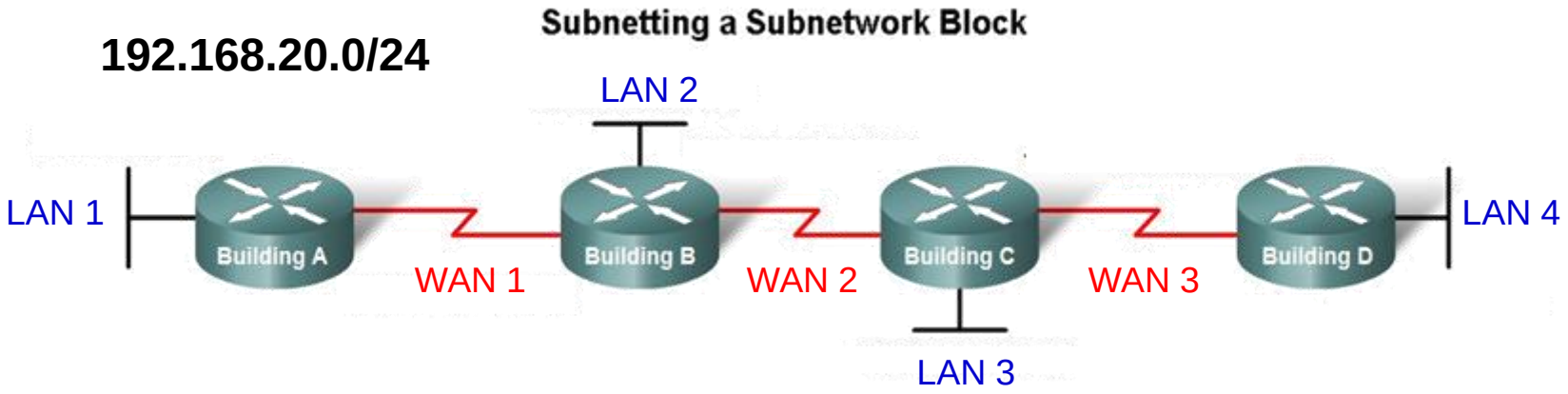
- In the second example, eight subnets have been created from a single address block.
- However, the last subnet cannot be used.
  - The last subnet is the broadcast subnet.
  - Its broadcast address is actually the broadcast address of all the other seven subnets.
- The first subnet is also not commonly used in practice.
- Therefore, in the previous example, only six subnets (subnet 1 – subnet 6) can actually be used.

Subnetting a Subnet

- In the previous examples, we have learned how to divide an address block into multiple equal-sized subnets.
- If all the subnets have the same requirements for the number hosts, these fixed size address blocks would be efficient.
- However, there can be situations where the number of hosts required per subnet is not the same.

Subnetting a Subnet

- Consider the following example: Given the address block 192.168.20.0/24, create 7 subnets.
  - Four for LANs
  - Three for WANs



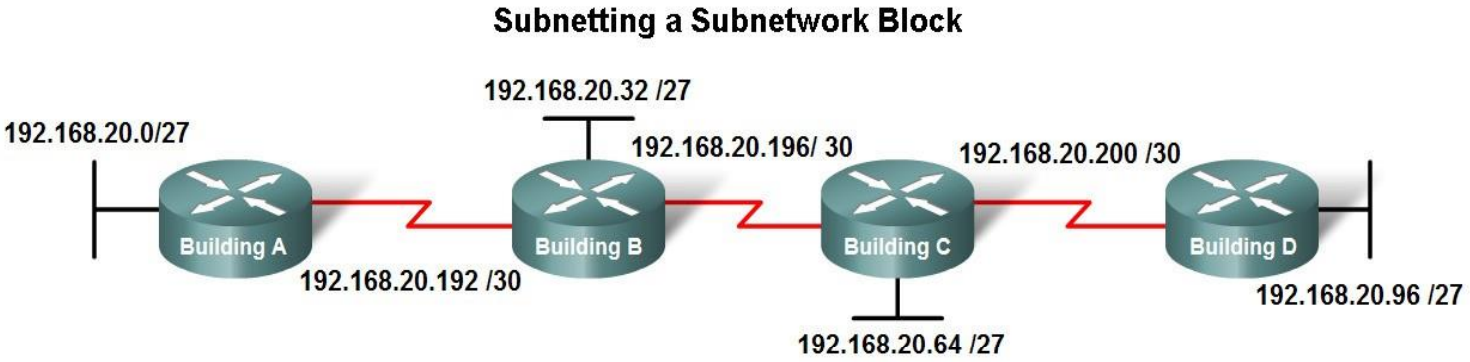
Subnetting a Subnet

- Using the subnetting technique learned previously, we will need to use 3 bits from the host portion.
  - This left 5 bits for the host portion of each subnet.
  - Each subnet then can accommodate 30 hosts.
- For the LAN subnets, 30 hosts per subnet would be okay.
- But for the WAN subnets, 30 hosts per subnet would be a waste of IP address space.
  - A WAN only need two IP addresses.
  - The other 28 addresses would then be unused and wasted.

Subnetting a Subnet

- To make a more efficient use of IP address space, a technique called Variable Length Subnet Mask (VLSM) can be used.
  - Allows allocating IP addresses to subnets according to the need of the subnet (in terms of number of hosts required).
- The idea is to divide one of the subnets created earlier to create additional, smaller subnets.
  - Each smaller subnets is only able to support two hosts.
  - This leaves the original subnets free to be allotted to other devices.
  - Prevents many addresses from being wasted.

Subnetting a Subnet



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.20/30

Testing the network layer

Testing the Network Layer

- Once the network interface of a host has been configured, the host should have network connectivity.
- However, things can always go wrong.
  - You though that you have configured the network correctly, but there is still no network connectivity.
- To make it easier to debug the problem, the network layer provides several utilities such as ping and traceroute.

Ping

- Ping is a utility for testing connectivity between hosts.
- Ping uses a layer 3 protocol called ICMP (Internet Control Message Protocol).
- When a host performs a ping to another host, a datagram called ICMP Echo Request will be sent to the other host.
- When the other host receives the echo request, it will reply with an ICMP Echo Reply datagram.
- For each packet sent, ping measures the time taken to receive the reply.

Ping

- As each response is received, ping provides a display of the time between the ping being sent and the response received.
  - This can be used to measure network performance.
- Ping has a timeout value for the response.
  - If a response is not received within that timeout, ping gives up and provides a message indicating that a response was not received.
- After all the requests are sent, the ping utility provides an output with the summary of the responses.
  - This output includes the success rate and average round-trip time to the destination.

Ping 127.0.0.1 – Testing the Local Stack

- Recall that 127.0.0.1 is a loopback address.
  - Meaning that send the packet to the host itself.
- By sending a ping to 127.0.0.1, you can test the internal configuration of IP on the local host.
  - This indicates whether IP is properly installed on the host or not.
- It does not, however, indicate whether the addresses, subnet mask and gateway are properly configured.
- If this test gives an error, that means TCP/IP is not operational on the host.

Ping Gateway – Testing Connectivity to the Local LAN

- To test whether the host can communicate with the local network, you can ping the IP address of the gateway.
  - This will test whether the host and router's interface serving as the gateway are both operational on the local network.
- You can also test the LAN connectivity by pinging the other hosts in the same LAN.
- If the host responds but the gateway does not, this indicates a problem with the router's interface serving as the gateway.
  - In this case, check the IP address of the gateway and make sure that it is correct.

Ping Remote Host – Testing Connectivity to Remote LAN

- To test whether the host can communicate with another host on a remote LAN, you can try to ping a remote host.
- Testing connectivity to remote LAN should be done after verifying that the host can communicate with the local LAN.
  - Need to make sure that the gateway is working.
- A failure here may indicate several things:
  - There may be routers or links outside that local LAN that is not working. Try to ping another host (preferably on another network than the first one).
  - The routing table of the host is not configured properly. Make sure the gateway IP address is configured correctly.

Traceroute (tracert): Testing the Path

- Ping is used to indicate the connectivity between two hosts.
- Traceroute (tracert) is a utility that allows us to observe the path between these hosts.
- The trace generates a list of hops that were successfully reached along the path.
- Similar to ping, traceroute also uses the ICMP protocol.

ICMPv4: The Protocol Supporting Testing and Messaging

- ICMP is actually used to send error messages between routers and hosts in the network.
- Among the use of ICMP are as follows:
  - Host confirmation
    - Determines if a host is operational.
  - Unreachable destination or service
    - Notifies a host that the destination or service is unreachable.
    - The packet will contain codes that indicate why the packet could not be delivered (0 = net unreachable; 1 = host unreachable; 2 = protocol unreachable; 3 = port unreachable).

ICMPv4: The Protocol Supporting Testing and Messaging

- Time exceeded
  - Indicates that a packet cannot be forwarded because the TTL field of the packet has expired.
- Route redirection
  - Notifies the hosts on a network that a better route is available for a particular destination.
  - This message may only be used when the source host is on the same physical network as both gateways.
- Source quench
  - Tells the source to temporarily stop sending packets.

Overview of IPv6

- In the early 1990s, the Internet Engineering Task Force (IETF) grew concerned about the exhaustion of the IPv4 network addresses.
- This led to the development of the next version of IP, called IPv6.
- The key feature of IPv6 is that it has a much larger address space.
  - In IPv4, the address is only 32-bit long.
    - Total IPv4 addresses = 2^{32} = 4,294,967,296 ~ 4.3 billions
  - In IPv6, the address is 128-bit long.
    - Total IPv6 addresses = 2^{128}
    - = 340,282,366,920,938,463,463,374,607,431,768,211,456

Overview of IPv6

- Other improvements made to IPv6:
  - Simpler header format
    - To improve packet handling.
  - Improved support for extensions and options
    - To increase scalability/longevity and improve packet handling.
  - Flow labeling capability
    - To provide QoS mechanism.
  - Authentication and privacy capability
    - To integrate security.

KEMENTERIAN PENDIDIKAN MALAYSIA

UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

http://ftmk.utem.edu.my