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 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 borrowed, fewer bits 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

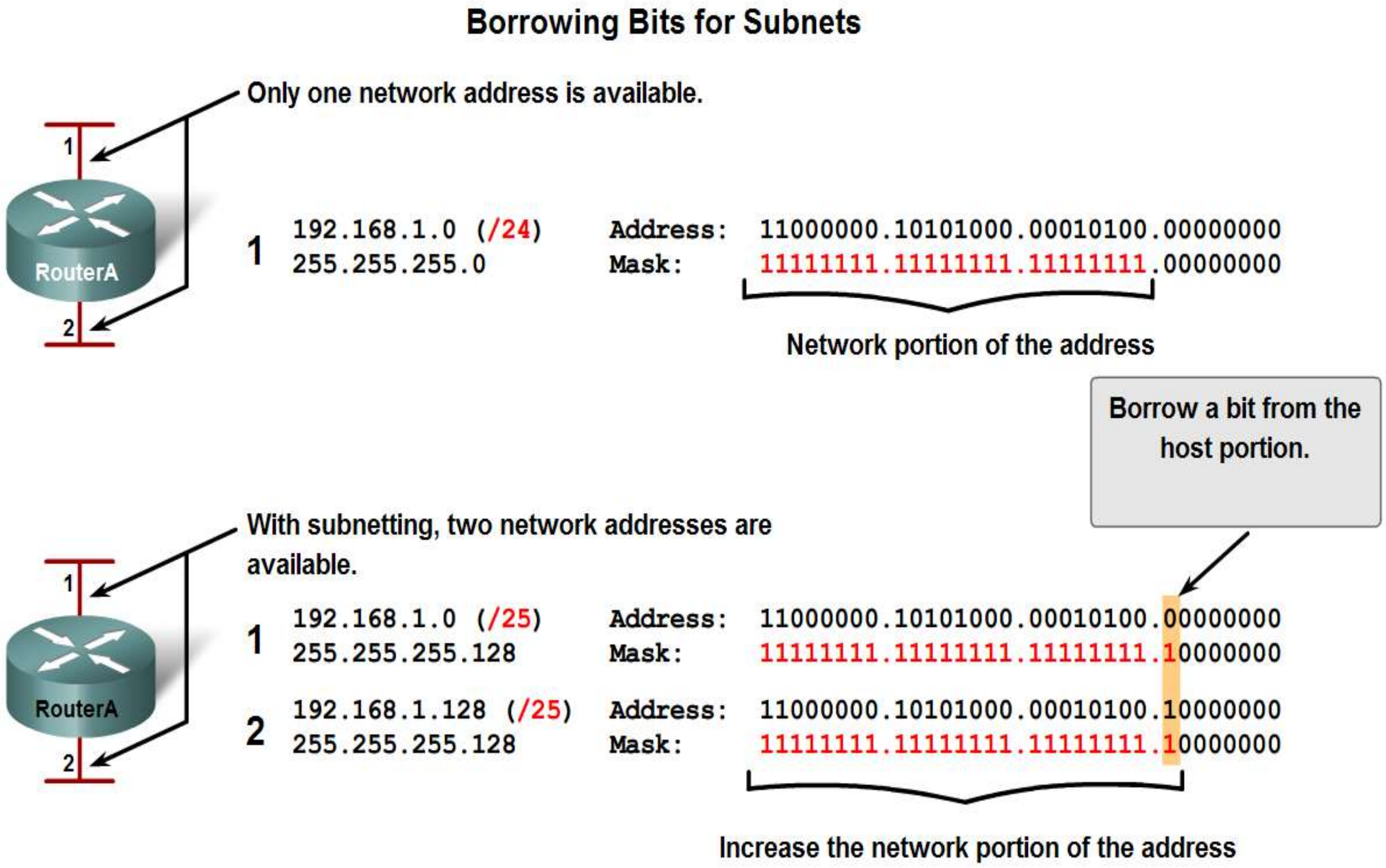
- Step 2: Find out the number of hosts per network.
  - Formula: Number of hosts = $2^n – 2$ (where n is the number of bits in the host portion).
    - Why need to minus 2?
    - Because the lowest address in the range is used for the network address and the highest address in the range is used for the 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



Borrowing Bits for Subnets

Only one network address is available.

```
1  192.168.1.0 (/24)      Address:  11000000.10101000.00010100.00000000
   255.255.255.0          Mask:     11111111.11111111.11111111.00000000
```

Network portion of the address

Borrow a bit from the host portion.

With subnetting, two network addresses are available.

```
1  192.168.1.0 (/25)      Address:  11000000.10101000.00010100.00000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000

2  192.168.1.128 (/25)    Address:  11000000.10101000.00010100.10000000
   255.255.255.128        Mask:     11111111.11111111.11111111.10000000
```

Increase the network portion of the address

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

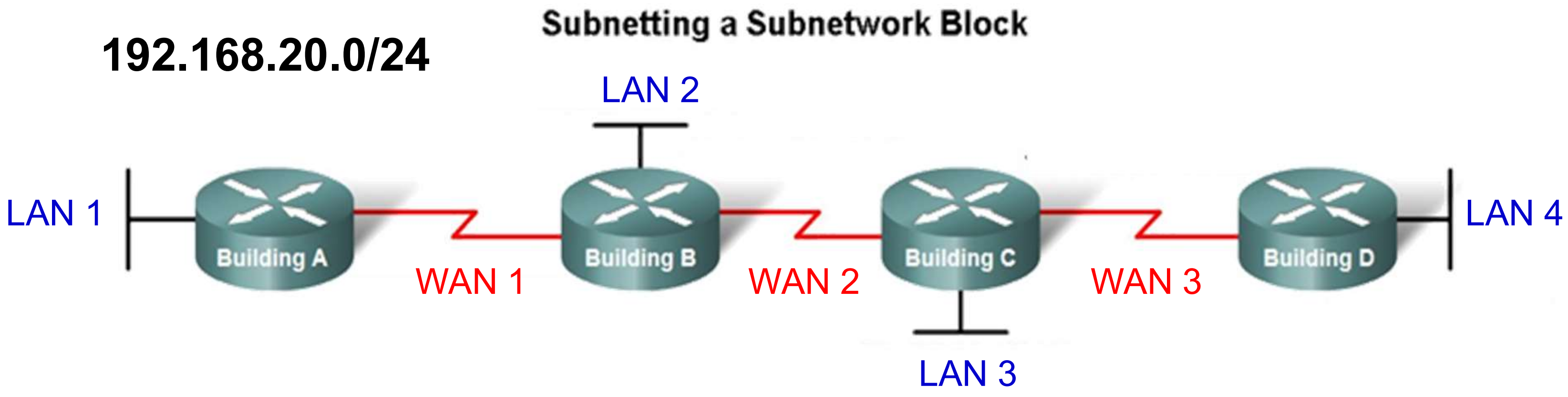
Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0 /27	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32 /27	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64 /27	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96 /27	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128 /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

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

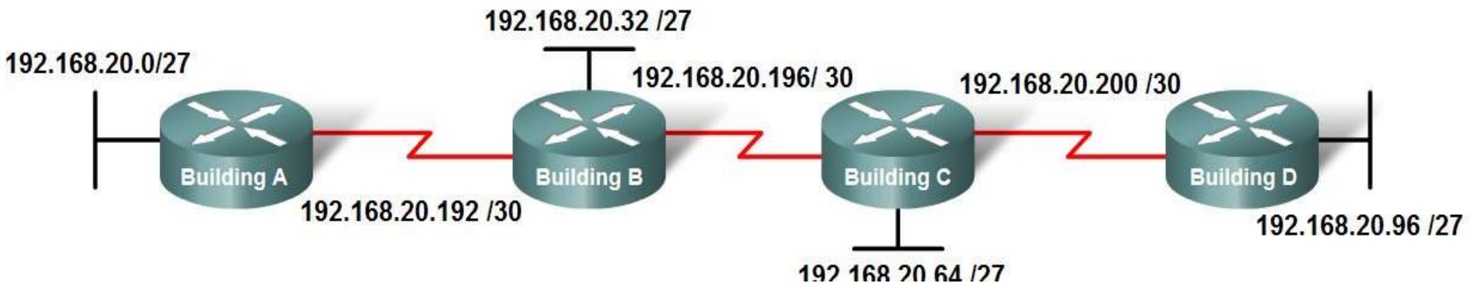
- Using the subnetting technique learned previously, we will need to use 3 bits from the host portion.
  - This left 5 bits for the host portion of each subnet.
  - Each subnet then can accommodate 30 hosts.
- For the LAN subnets, 30 hosts per subnet would be okay.
- But for the WAN subnets, 30 hosts 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.

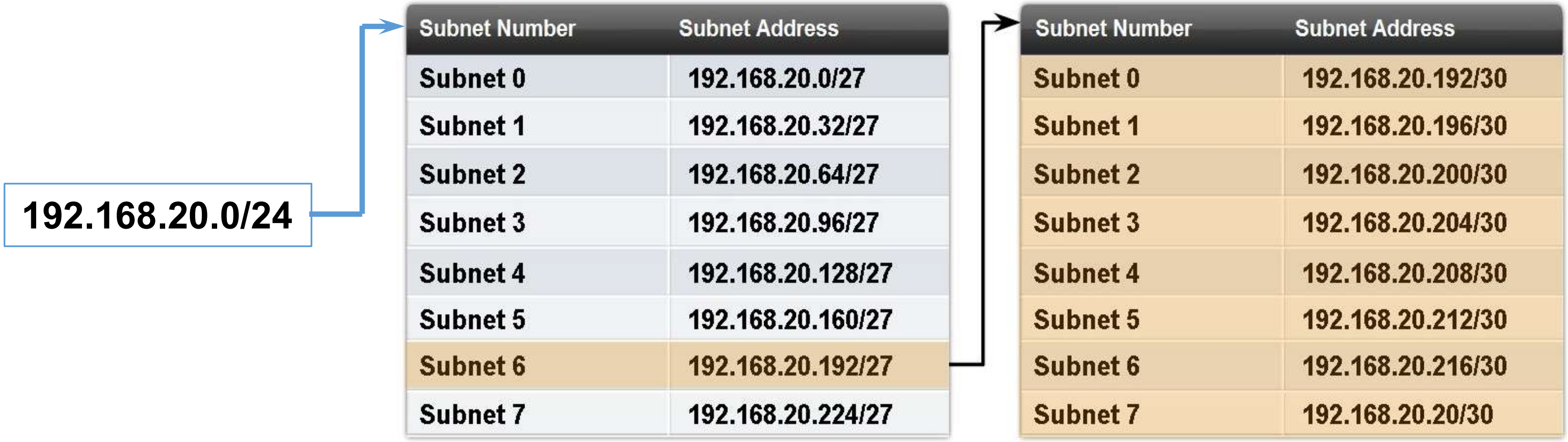
Subnetting a Subnet

- 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

Subnetting a Subnetwork Block




192.168.20.0/24

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.

Text Representation of Addresses

- “Preferred” form:
  - 1080:0:FF:0:8:800:200C:417A
- Compressed form:
  - FF01:0:0:0:0:0:0:43
- becomes
  - FF01::43

KEMENTERIAN
PENDIDIKAN
MALAYSIA

UTeM

اونيۏرسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FTMK

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

/ myftmk

http://ftmk.utem.edu.my