

Explores how the multiple networks are interconnected to form the Internet

6.7.1 Learning Outcomes:

Learning Outcomes:

- Explains the role of a gateway device in inter connecting two LANs
- Explain the need for a uniform, MAC protocol independent addressing scheme and how IP addresses play that role
- Describes the role of subnet masks
- Calculates subnet masks and IP address ranges given a block of IP addresses and network sizes
- Describes the how DHCP is used to dynamically assign IP addresses
- Describes the role of routers in finding a suitable path from the sender to the receiver
- Explains packet switching and best effort delivery in IP networks

Contents:

- A device connected two or more networks – gateway
- Need for globally unique uniform addressing independent of MAC addresses and LAN technology
 - IPv4 addresses
 - Assigning IPs to networks
 - ❖ Sub-netting
 - ❖ Subnet masks
 - ❖ CIDR notation
 - ❖ Private IP addresses
 - ❖ DHCP
 - Scarcity of IPv4 addresses and IPv6 as a solution (an overview)
 - Finding the path to the destination
 - Routing and routers
 - Packet switching
- Best effort delivery

Classless Inter Domain Routing (CIDR)

- It replaces the old system based on classes A, B, and C.
- This scheme also helped greatly extend the life of IPv4 as well as slow the growth of routing tables.
- The old method of IP addressing came with inefficiencies that exhausted the availability of IPv4 addresses faster than it needed to.
- **Class A** - Over 16 million host identifiers
- **Class B** - 65,535 host identifiers
- **Class C** - 254 host identifiers
- The problem would commonly occur when an organization required more than 254 host machines and therefore would no longer fall into class C but rather class B.
- This means that the organization would use a class B license even though they had far less than 65,535 hosts.
- Therefore if an organization only required 2,500 hosts, they would be wasting about 63,000 hosts by holding a class B license which would greatly decrease the availability of IPv4 addresses unnecessarily

- CIDR is based on variable-length subnet masking (VLSM).
- CIDR IP addresses are composed of two sets of numbers
- The network address is written as a prefix
 1. Normal IP address (e.g. 192.255.255.255)
 2. Suffix which indicates how many bits are in the entire address (e.g. /12)

CIDR IP address would look like the following:

192.168.17.15 /18



192.168.17.15

11111111 11111111 11000000 00000000



/18

Subnet mask is 255.255.192.0

CIDR			
CIDR	Class	Hosts*	Mask
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1 C	256	255.255.255.000
/23	2 C	512	255.255.254.000
/22	4 C	1024	255.255.252.000
/21	8 C	2048	255.255.248.000
/20	16 C	4096	255.255.240.000
/19	32 C	8192	255.255.224.000
/18	64 C	16384	255.255.192.000
/17	128 C	32768	255.255.128.000
/16	256 C, 1 B	65536	255.255.000.000

Private IP Addresses and Public IP address

Private IP

- Any IP address that falls specified ranges is a private IP address and is non-routable on the Internet.
- These addresses are reserved for use only within private/corporate network and cannot be seen outside the private networks.
- These private addresses are translated at the company's firewall into an external (public) IP address, which will be some address that does 'not' fall within these ranges.
- Private IP address do not connect to the internet.
- Private IP address use in local area network (LAN)

Private IP

10.0.0.0/8	=	10.0.0.0	– 10.255.255.255
192.168.0.0/16	=	192.168.0.0	– 192.168.255.255
172.16.0.0/12	=	172.16.0.0	– 172.31.255.255

An address is Private if it starts with:

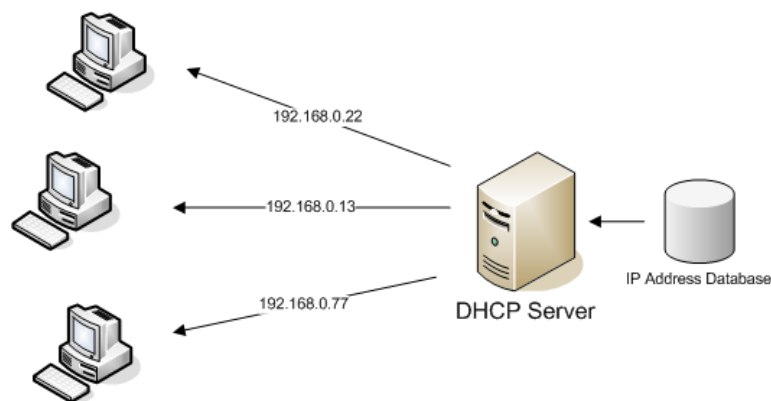
1. 10
2. 172. [16-31]

Public IP address

- A public IP address is the address that is assigned to a computing device to allow direct access over the Internet.
- A web server, email server and any server device directly accessible from the Internet are candidate for a public IP address.
- A public IP address is globally unique, and can only be assigned to a unique device.

A DHCP Server

- It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.
- DHCP is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.
- DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices.
- A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices.
- DHCP can be implemented on small local networks, as well as large enterprise networks.



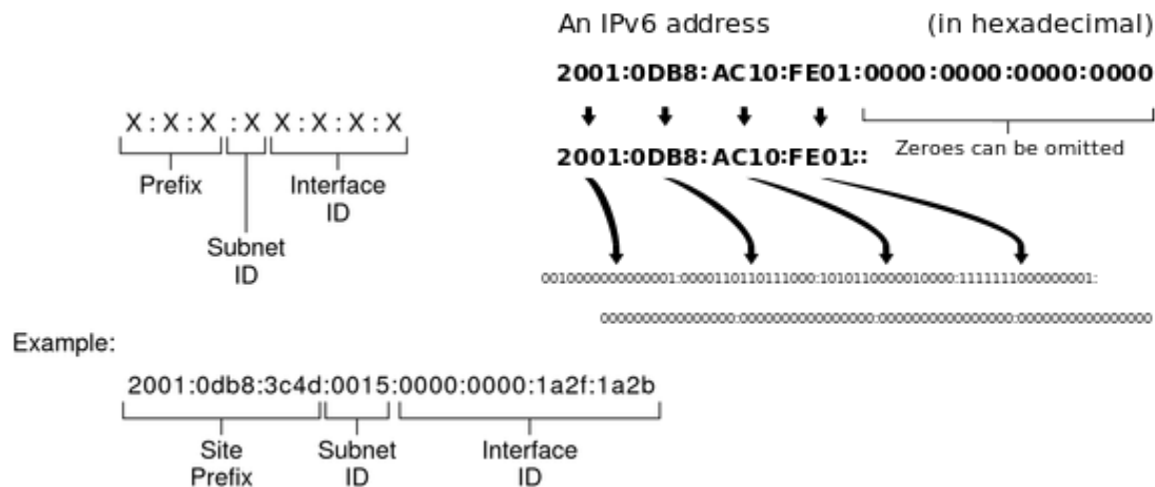
IPv6 Addressing

- IPv6 is the latest version of the Internet Protocol, which identifies devices across the internet so they can be located. Every device that uses the internet is identified through its own IP address in order for internet communication to work
- The previous version, IPv4, uses a 32-bit addressing scheme to support 4.3 billion devices, which was thought to be enough. However, the growth of the internet, personal computers, smartphones and now Internet of Things devices proves that the world needed more addresses. The Internet Engineering Task Force (IETF) recognized this 20 years ago.

- In 1998 it created IPv6, which instead uses 128-bit addressing to support approximately 340 trillion (or 2 to the 128th power).
- Instead of the IPv4 address method of four sets of one- to three-digit numbers, IPv6 uses eight groups of four hexadecimal digits, separated by colons.
- An Internet Protocol Version 6 address is a numerical label that is used to identify a network interface of a computer or a network node participating in an IPv6 computer network, and locate it in the network.
- IP addresses are included in the packet header to indicate the source and the destination of each packet.

Parts of the IPv6 Address

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses



IPv6 Address type

• **Global Unicast Address-**

Equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

• **Link-Local Address-**

Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0

• **Unique-Local Address**

This type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



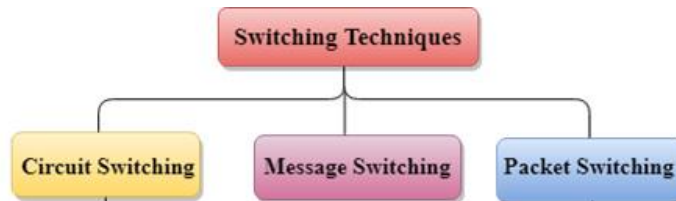
Switching

Switching is process to forward packets coming in from one port to a port leading towards the destination.

The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication

Classification Of Switching Techniques

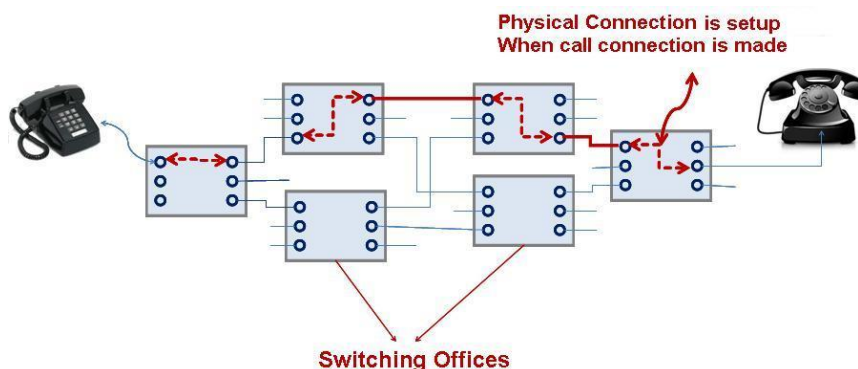


In A/L syllabus you are going to learn only

- **Circuit Switching**
- **Packet Switching**

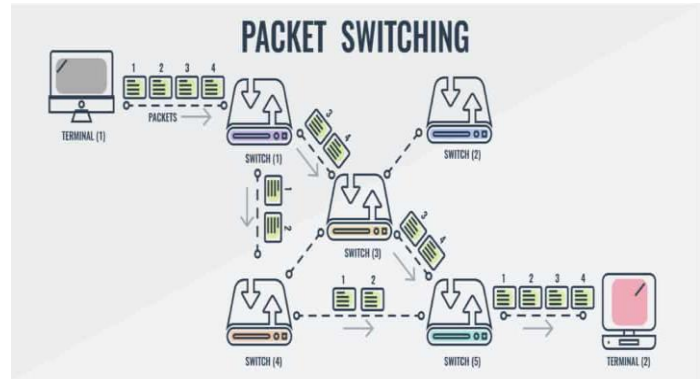
- **Circuit Switching**

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.



Packet switching

- **Packet switching** is a method of transferring the data to a network in form of packets.
- In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**.
- At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file
- . A packet composes of payload and various control information.
- No pre-setup or reservation of resources is needed.



Advantage of Packet Switching over Circuit Switching:

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
- Cost effective and comparatively cheaper to implement.

Disadvantage of Packet Switching over Circuit Switching

- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but large message Circuit Switching is better.

Feature	Circuit Switching	Packet Switching
Dedicated Path	Yes	No
Path Formation	Path dedicated for one conversation	Route is established on a per packet basis of the conversation using datagram (or per conversation with virtual circuit)
Delay	Call setup delay	Packet transmission delay (call setup delay for virtual circuit)
Bandwidth Type	Fixed Bandwidth	Dynamic bandwidth
Overload Effects	Stops call establishment	Increases packet delay (can block call establishment and increase packet delay with virtual circuit)

6.7.3

- **Find the details about**(At least 1full Page of CR Book)
 - Repeaters
 - Hub
 - Bridges
 - Switch
 - Routers
 - NIC
 - RJ45
 - BNC(Bayonet Neill –Concelman)

Network troubleshooting Commands

- Network performance troubleshooting is the process of identifying a network problem, establishing and testing a theory of probable cause, constructing a plan of action and implementing a functional resolution.
- This process requires adept tools that support a network administrator to troubleshoot network issues effectively.
- The multiple tools involved in this remediation process are identified as network analysis and troubleshooting tools.

Types of network troubleshooting tools

- These network troubleshooting tools range from simple command line based troubleshooting utilities to more comprehensive and robust solutions that allows for a systematic, efficient and proactive approach to network troubleshooting,
 - Ping
 - Tracert/ Trace Route
 - Ipconfig/ ifconfig
 - TTL
 - LOST
 - MINIMUM
 - MAXIMUM
 - AVERAGE

1. **Ping**

- **Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network.
- It is available for virtually all operating systems that have networking capability, including most embedded network administration software.
- Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.
- Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply.
- The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sanjeeva>ping www.google.lk

Pinging www.google.lk [216.58.199.163] with 32 bytes of data:
Reply from 216.58.199.163: bytes=32 time=76ms TTL=117
Reply from 216.58.199.163: bytes=32 time=108ms TTL=117
Reply from 216.58.199.163: bytes=32 time=102ms TTL=117
Reply from 216.58.199.163: bytes=32 time=61ms TTL=117

Ping statistics for 216.58.199.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 108ms, Average = 86ms

C:\Users\sanjeeva>
```

2. Tracert/ Trace Route

- Tracert (Windows) or trace route (Linux) is a network diagnostic and troubleshooting tool to view the route and measure transit delays of data packets in a network.
- It displays the number of hops between the source and destination devices based on the hop limit concept, modifying the Time To Live (TTL) values.

3. Ipconfig (Windows) and Ifconfig (Linux / Unix)

- When we need to know the IP address of the host that we're working on, these are the utilities to use.
- Not only will it provide IPv4 information, but it will also provide IPv6 addresses, MAC addresses, DNS servers, default gateways and data with regard to how much traffic is flowing over the interface along with errors and dropped packets.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sanjeeva>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2cba:fe9b:95ef:7a38%13
    IPv4 Address. . . . . : 192.168.8.194
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.8.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

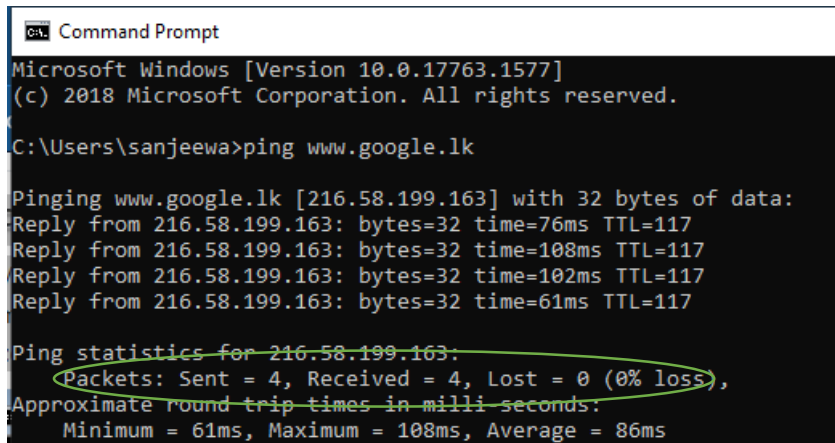
C:\Users\sanjeeva>
```


Time to live (TTL)

- Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.
- When a packet of information is created and sent out across the Internet, there is a risk that it will continue to pass from router to router indefinitely.
- To mitigate this possibility, packets are designed with an expiration called a time-to-live or hop limit.
- Packet TTL can also be useful in determining how long a packet has been in circulation, and allow the sender to receive information about a packet’s path through the Internet.
- Each packet has a place where it stores a numerical value determining how much longer it should continue to move through the network.
- Every time a router receives a packet, it subtracts one from the TTL count and then passes it onto the next location in the network.
- If at any point the TTL count is equal to zero after the subtraction, the router will discard the packet and send an ICMP message back to the originating host.
- This value can be between 1 to 255

Lost

Shows host, which the number of damaged packets during transmission.



```
Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sanjeewa>ping www.google.lk

Pinging www.google.lk [216.58.199.163] with 32 bytes of data:
Reply from 216.58.199.163: bytes=32 time=76ms TTL=117
Reply from 216.58.199.163: bytes=32 time=108ms TTL=117
Reply from 216.58.199.163: bytes=32 time=102ms TTL=117
Reply from 216.58.199.163: bytes=32 time=61ms TTL=117

Ping statistics for 216.58.199.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli seconds:
        Minimum = 61ms, Maximum = 108ms, Average = 86ms
```

Maximum

The Maximum time used in transmission of data

Minimum

The Minimum time used in transmission of data

Average

Value shown here is obtained by dividing the total of the time elapsed for the transmitted data packets by the number of packets.