BIT 6113

Database Management System

Saroj Ghimire

saroj.ghimire2@texascollege.edu.np

Lincoln University College

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 efficiently 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) have 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.

Packet Switching

Packet Switching uses Store and Forward technique while switching the packets; while forwarding the packet each hop first stores that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of sources and destinations. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different paths possible over an existing network.

**Modes of Packet Switching :**

**1. Connection-oriented Packet Switching (Virtual Circuit) :**

Before starting the transmission, it establishes a logical path or virtual connection using signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by

switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended

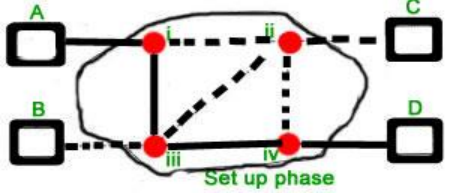
with help of sequence numbers. Overall, three phases take place here- The setup, data transfer and tear down phase.

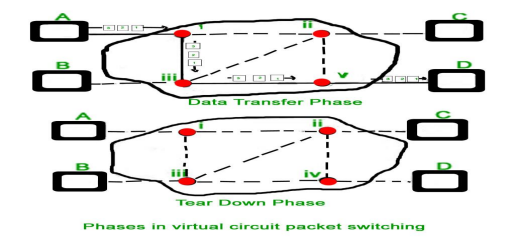
**Modes of Packet Switching:**

All address information is only transferred during the setup phase. Once the route to a destination is discovered, entry is added to the switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number, etc.

Connection-oriented switching is very useful in switched WAN. Some popular protocols which use the Virtual Circuit Switching

approach are X.25, Frame-Relay, ATM, and MPLS(Multi-Protocol Label Switching).

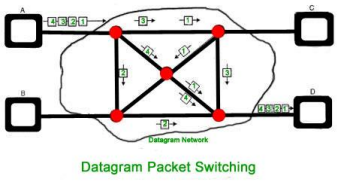
**Modes of Packet Switching:** ---



**Modes of Packet Switching:**

**2. Connectionless Packet Switching (Datagram) :** Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers, etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at the destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.

Packet delivery is not guaranteed in connectionless packet switching, so reliable delivery must be provided by end systems using additional protocols.

**Modes of Packet Switching: **

To send a packet from A to B there are delays since this is a Store and Forward network.

**Delays in Packet switching :**

Transmission Delay

Propagation Delay

Queuing Delay

Processing Delay

Circuit Switching

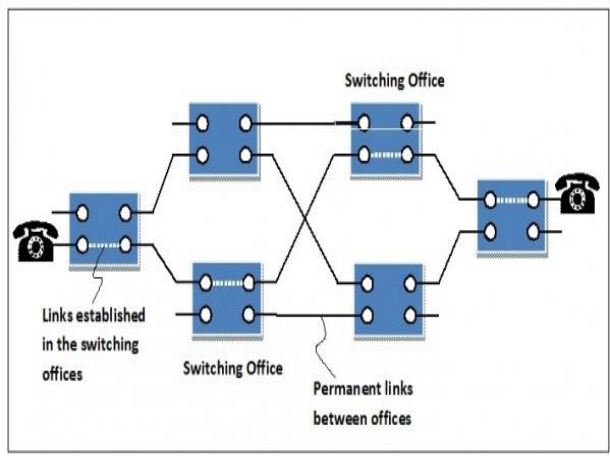
Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.

**Phases of Circuit Switch Connection**

**Circuit Establishment** : In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centers. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.

**Data Transfer** : Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.

**Circuit Disconnection** : When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all intermediate links from the sender to the receiver.



**Circuit Switching Packet Switching In circuit switching there are 3 phases:**

**i) Connection Establishment.**

**ii) Data Transfer.**

**iii) Connection Released.**

**In circuit switching, each data unit know the entire path address which is provided by the source.**

**In Packet switching directly data transfer takes place.**

**In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.**

**In Circuit switching, data is processed at source system only In Packet switching, data is processed at all intermediate node including source system.**

**Delay between data units in circuit switching is uniform. Delay between data units in packet switching is not uniform.**

**Resource reservation is the feature of circuit switching because path is fixed for data transmission.**

**There is no resource reservation because bandwidth is shared among users.**

**Circuit switching is more reliable. Packet switching is less reliable.**

**Wastage of resources are more in Circuit Switching Less wastage of resources as compared to Circuit Switching It is not a store and forward technique. It is a store and forward technique.**

**Transmission of the data is done by the source. Transmission of the data is done not only by the source, but also by the intermediate routers.**

**Congestion can occur during the connection establishment phase, because there might be a case where a request is being made for a channel but the channel is already occupied.**

**Congestion can occur during data transfer phase, large number of packets comes in no time.**

**Circuit switching is not convenient for handling bilateral traffic. Packet switching is suitable for handling bilateral traffic.**

**In Circuit switching, charge depend on time and distance, not on traffic in the network.**

**In Packet switching, charge is based on the number of bytes and connection time.**

**Recording of packet is never possible in circuit switching. Recording of packet is possible in packet switching.**

**In Circuit Switching there is a physical path between the source and the destination**

**In Packet Switching there is no physical path between the source and the destination**

**Circuit Switching does not support store and forward transmission Packet Switching supports store and forward transmission**

Forwarding a Packet

Packet forwarding is the process of directing the packet towards its destination. As we know that Internet is a combination of several networks. A

packet may belong to the same network as of source host or it may be for the destination host in a different network. So, a packet from a source host may have to travel many networks before reaching the destination.

Packet forwarding is the responsibility of the router where the router has to accept the packet from the source host or a router in the path of the packet and place it on the route heading towards the destination host.

Packet Forwarding

Forwarding Based on Destination Address

Forwarding Techniques

Forwarding Process(we shall cover later)

Forwarding Based on Label(we shall cover later)

**Forwarding Based on Destination Address**

Packet forwarding based on the destination address requires the source host and routers in the path of the packet to have the routing table. Whenever the host is ready with the packet to be sent or the router receives a packet to forward it to the

next router or the destination host, they look up the routing table to decide the route of the packet toward the destination host.

But nowadays Internet has grown too far, so many entries in routing make the table lookup inefficient. There are several techniques to minimize the size of the routing table and also manage the security of the routing table.

Forwarding Techniques

**1. Next-Hop Method**

The next-hop method minimizes the size of the routing table by just keeping the details of the **next hop** or next router in the path of the packet. Here the routing table does not involve the information about the entire route the packet has to follow. **2. Network-Specific Method**

Here the routing table does not have an entry for all the destination hosts in the network connected to the router. Instead, it has an entry of the destination networks itself connected to the router.

**3. Host-Specific Method**

It is the reverse of the network-specific method. Here the routing table has an entry for all the destination hosts in the destination network. It reduces the efficiency of the routing table as the size of the routing table is increased. It is usually used for checking the routes and for security purposes.

**4. Default Method**

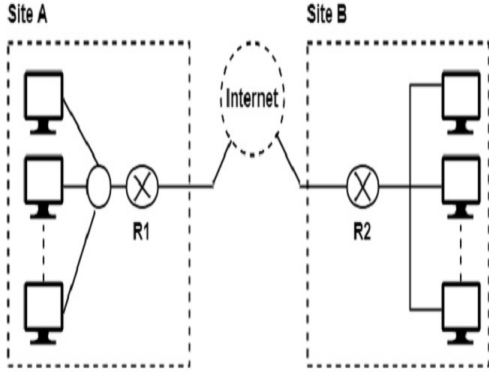
Consider the situation that a host in a network N1 is connected to two routers where one router R1 is connected to the network N2 and another router R2 connects it to the rest of the internet. So here the routing table has only one entry for the router R2 as a default entry.

VPN(Virtual Private Network)

• **VPN** stands for Virtual Private Network. It allows you to connect your computer to a private network, creating an encrypted connection that masks your IP address to securely share data and surf the web, protecting your identity online.

• A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

• VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.



VPN(Virtual Private Network)

• A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

• **Secure encryption:** To read the data, you need an encryption key . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.

• **Disguising your whereabouts :** VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

• **Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With VPN location spoofing , you can switch to a server to another country and effectively “change” your location.

• **Secure data transfer:** If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Types of VPN

**SSL VPN**

• A virtual private network (VPN) is a service that allows a user to establish a secure, encrypted connection between the public internet and a corporate or institutional network.

• A secure sockets layer VPN (SSL VPN) enables individual users to access an organization's network, client-server applications, and internal network utilities and directories without the need for specialized software. SSL VPNs provide safe, secure communication via an encrypted connection for all types of devices, regardless of whether access to the network is via the public internet or another secure network.

• All traffic between a web browser and an SSL VPN device is encrypted with either the SSL or transport layer security (TLS) protocol. Individual users of the SSL VPN do not have to decide which protocol to use for the VPN to do its job. Instead, the SSL VPN automatically uses the newest, most updated cryptographic protocol that has been installed on the user's browser. Users do not need to worry about updating the protocol on their browser either. Whenever a browser or an operating system (OS) is updated, the newest version of the protocol is updated along with it.

Types of VPN

Site-to-Site VPN

• A site-to-site virtual private network (VPN) refers to a connection set up between multiple networks. This could be a corporate network where multiple offices work in conjunction with each other or a branch office network with a central office and multiple branch locations.

• Site-to-site VPNs are useful for companies that prioritize private, protected traffic and are particularly helpful for organizations with more than one office spread out over large geographical locations. These businesses often have to access resources housed on a primary network, which could include servers that facilitate email or store data. In some instances, a server may be the operational hub of an application essential to the company’s business. A site-to-site VPN can, in that case, give all sites full access to the application— as if it were housed within their physical facility.

Types of VPN

• A site-to-site VPN is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

• A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

• Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

VPN(Virtual Private Network)

• VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private “tunnel” to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

• VPN (Virtual Private Network) is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunneled through an otherwise unsecured or untrusted network. Instead of using a dedicated connection, such as leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections.

• VPN transmits data by means of tunneling. Before a packet is transmitted, it is encapsulated (wrapped) in a new packet, with a new header. This header provides routing information so that it can traverse a shared or public network, before it reaches its tunnel endpoint. This logical path that the encapsulated packets travel through is called a tunnel. When each packet reaches the tunnel endpoint, it is “decapsulated” and forwarded to its final destination. Both tunnel endpoints need to support the same tunneling protocol. Tunneling protocols are operated at either the OSI (Open System Interconnection) layer two (data-link layer), or layer three (network layer). The most commonly used tunneling protocols are IPsec, L2TP, PPTP and SSL. A packet with a private non-routable IP address can be sent inside a packet with globally unique IP address, thereby extending a private network over the Internet.

VPN(Virtual Private Network)

• VPN uses encryption to provide data confidentiality. Once connected, the VPN makes use of the tunneling mechanism described above to encapsulate encrypted data into a secure tunnel, with openly read headers that can cross a public network. Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission. VPN can also provide a data integrity check. This is typically performed using a message digest to ensure that the data has not been tampered with during transmission. By default, VPN does not provide or enforce strong user authentication. Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. Nevertheless, VPN does support add-on authentication mechanisms, such as smart cards, tokens and RADIUS.

Network System

• A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

• A computer network comprises two or more computers that are connected—either by cables (wired) or WiFi (wireless)—with the purpose of transmitting, exchanging, or sharing data and resources. You build a computer network using hardware (e.g., routers, switches, access points, and cables) and software (e.g., operating systems or business applications).

• Geographic location often defines a computer network. For example, a LAN (local area network) connects computers in a defined physical space, like an office building, whereas a WAN (wide area network) can connect computers across continents. The internet is the largest example of a WAN, connecting billions of computers worldwide.

• You can further define a computer network by the protocols it uses to communicate, the physical arrangement of its components, how it controls traffic, and its purpose. • Computer networks enable communication for every business, entertainment, and research purpose. The internet, online search, email, audio and video sharing, online commerce, live-streaming, and social networks all exist because of computer networks.

Autonomous System

• An autonomous system is a collection of network prefixes within the internet. A collection of network prefixes are grouped into an autonomous system (AS). An AS is an individual network on the internet. Each network, or AS, has an autonomous system number (ASN).

• To understand a bit further, we can explain where an AS fits in the composition of the internet. The internet comprises internet protocols (IPs), network prefixes and autonomous systems. IPs are grouped into network prefixes and network prefixes are grouped into autonomous systems. Autonomous systems are then owned by internet service providers (ISPs).

• In the early days of the internet, an AS was only able to be owned by one entity. For example, one ISP would own one AS. This is no longer the case. An ISP can own multiple AS’s and they will use border gateway protocol (BGP) to communicate between them.

• Autonomous systems communicate between each other through BGP. For one AS to communicate to another, they identify with autonomous system numbers.

• Autonomous system numbers (ASNs) are the unique identifiers that are given to an AS. The identifier allows an AS to communicate both externally and internally. An AS can have a private ASN and a public ASN.

• Private ASN: A private ASN is a unique identifier for an AS that is used for communicating an AS to one entity.

• Public ASN: A public ASN is a unique identifier that is advertised to the public internet. This is also used to communicate between ASNs.

**The backbone of the Autonomous System**

• The backbone consists of those networks not contained in any area, their attached routers, and those routers that belong to multiple areas. The backbone must be contiguous.

• It is possible to define areas in such a way that the backbone is no longer contiguous. In this case the system administrator must restore backbone connectivity by configuring virtual links.

• Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. On the graph of the backbone, two such routers are joined by arcs whose costs are the intra-area distances between the two routers. The routing protocol traffic that flows along the virtual link uses intra- area routing only.

• The backbone is responsible for distributing routing information between areas. The backbone itself has all of the properties of an area. The topology of the backbone is invisible to each of the areas, while the backbone itself knows nothing of the topology of the areas.