This course is designed to impart knowledge about detailed knowledge of computer network architecture, various protocols used in communication, Managing and configuring Cisco Switches and Routers, and various WAN Technologies.

Switching and Routing

Study Material

Department of Cyber Science & Technology, Brainware University

Table of Contents

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Module I
Network Models, IP Addressing and Routing Basics

What are Network Models?

In the context of computer networks, network models are abstract representations that define the structure, components, and operations of a network. These models provide a framework for understanding how different network elements interact and communicate. They are crucial for designing, implementing, managing, and troubleshooting computer networks.

Purpose of Network Models?

Standardization

- **Interoperability**: Network models provide a common framework that ensures devices and systems from different manufacturers can work together seamlessly.
- **Consistency**: They establish consistent protocols and procedures, making it easier to develop and maintain networked systems.

Design and Implementation

- **Structured Design**: Network models offer a systematic approach to designing networks, breaking down complex processes into manageable layers or components.
- **Modular Development**: They facilitate modular development, allowing individual network components to be designed and implemented independently before being integrated into the larger system.
- **Troubleshooting and Maintenance**

- **Layered Problem-Solving**: The layered structure of network models helps in isolating and identifying issues within specific layers, simplifying the troubleshooting process.
- **Efficient Maintenance**: They provide a clear understanding of network operations, making it easier to perform maintenance tasks and ensure network reliability.

Scalability and Flexibility

- **Ease of Expansion**: Network models support scalable designs, making it easier to expand the network by adding new components without disrupting existing services.
- **Adaptability**: They provide flexibility to accommodate new technologies and protocols, allowing the network to evolve with changing requirements.

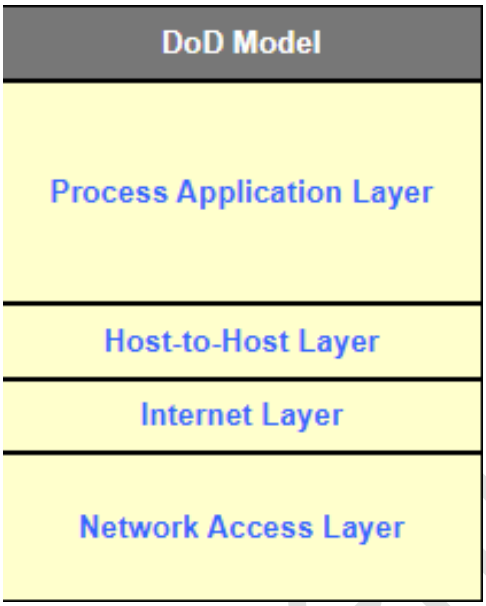
Security

- **Layered Security**: Implementing security measures at different layers of the network model enhances overall security, providing multiple defenses against threats.
- **Policy Enforcement**: Network models help define and enforce security policies, ensuring consistent protection across the network.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

What is DOD model?

The Department of Defense (DoD) Model, also known as the DoD Reference Model, is a conceptual framework used in networking to describe the functions and protocols used in the development and implementation of network communication systems. It is similar to the OSI (Open Systems Interconnection) model but with fewer layers. The DoD Model is sometimes referred to as the TCP/IP model because it is based on the TCP/IP protocol suite. The model consists of four layers.

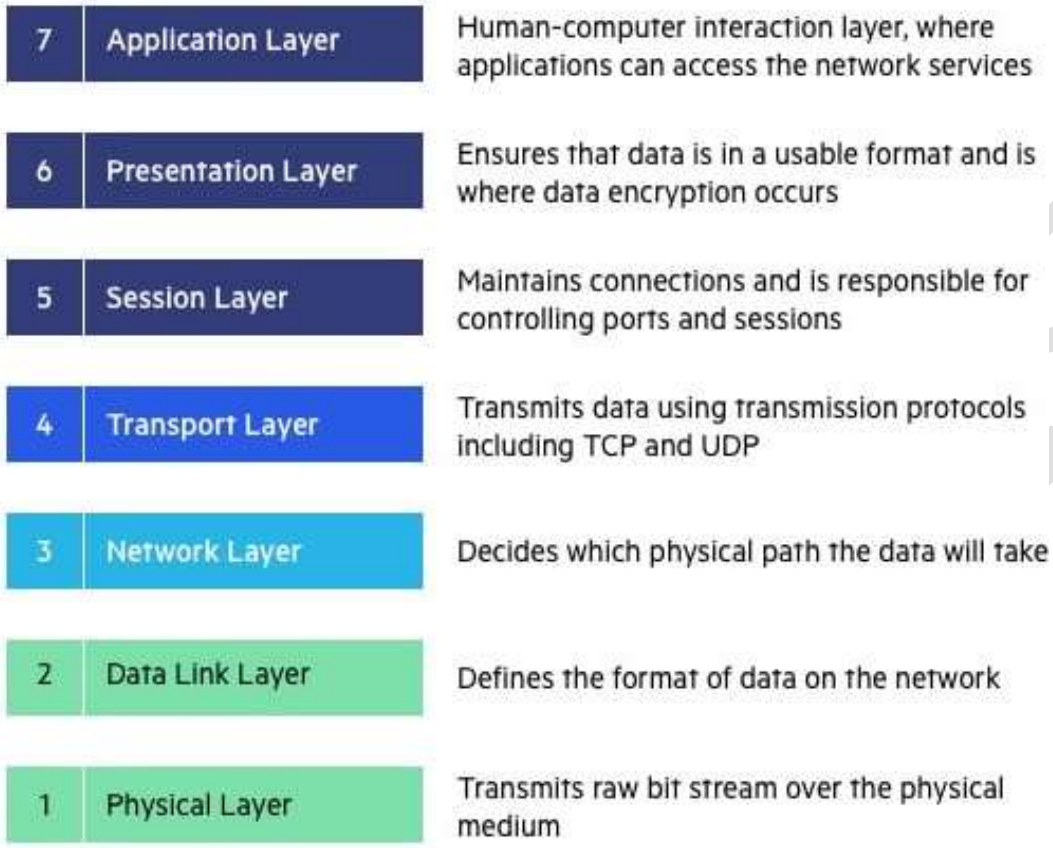


What is OSI model?

OSI stands for Open Systems Interconnection, where open stands to say non-proprietary. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe. The OSI reference model was developed by **ISO – 'International Organization for Standardization** ', in the year 1984.

The OSI model provides a theoretical foundation for understanding network communication. However, it is usually not directly implemented in its entirety in real-world networking hardware or software. Instead, specific protocols and technologies are often designed based on the principles outlined in the OSI model to facilitate efficient data transmission and networking operations.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



Physical Layer:

- Deals with the physical connection between devices.
- Transmits raw bit streams over a physical medium.
- Includes hardware components like cables, switches, and network interface cards.
- Manages bit rate control, modulation, and signal transmission.

Data Link Layer:

- Ensures node-to-node data transfer.
- Provides error detection and correction.
- Divided into two sublayers: Media Access Control (MAC) and Logical Link Control (LLC).
- Controls frame synchronization, flow control, and error checking.

Network Layer:

- Handles routing of data packets between nodes and networks.
- Manages logical addressing (IP addresses).
- Facilitates packet forwarding and routing.
- Uses protocols like Internet Protocol (IP).

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Transport Layer:

- Ensures end-to-end communication and reliability.
- Manages segmentation, error correction, and data reassembly.
- Uses protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Provides flow control and data integrity.

Session Layer:

- Manages sessions or connections between applications.
- Establishes, maintains, and terminates sessions.
- Ensures proper synchronization and recovery of data.
- Handles session establishment, maintenance, and termination.

Presentation Layer:

- Translates data between network and application formats.
- Provides data encryption, decryption, and compression.
- Ensures that data is readable by the receiving system.
- Handles character encoding, data formatting, and conversion.

Application Layer:

- Provides network services directly to end-user applications.
- Facilitates communication between software applications and network services.
- Uses protocols like Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).
- Manages application-specific network operations and user interfaces.

Explain OSI layer Briefly?

Functions of the Physical Layer

- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number **of bits sent per second.**
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (**MAC addresses**) of the sender and/or receiver in the header of each frame.
- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Functions of the Session Layer

- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Functions of the Application Layer

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

What Is Data Encapsulation and Decapsulation Process?

Data Encapsulation
Data Encapsulation is the process in which some extra information is added to the data item to add some features to it.

Process: -

Application Layer:

- The data originates from the application layer.
- No encapsulation is done here; it provides the raw data to the presentation layer.

Presentation Layer:

- The data is translated, encrypted, or compressed as needed.
- The presentation layer adds its header (if any) and passes the data to the session layer.

Session Layer:

- The session layer manages sessions and controls dialogues.
- It adds its own header (if any) and passes the data to the transport layer.

Transport Layer:

- The transport layer segments the data into smaller pieces if necessary.
- It adds a transport header, which includes information like sequence and port numbers (e.g., TCP or UDP header).
- The resulting segment or datagram is passed to the network layer.

Network Layer:

- The network layer encapsulates the data with an IP header, creating a packet.
- This header includes logical addressing (source and destination IP addresses) and other routing information.
- The packet is then passed to the data link layer.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Data Link Layer:

- The data link layer encapsulates the packet with a frame header and trailer.
- The frame header includes physical addressing (MAC addresses) and error-checking information.
- The frame trailer typically includes a Frame Check Sequence (FCS) for error detection.
- The resulting frame is passed to the physical layer.

Physical Layer:

- The physical layer converts the frame into a bitstream of 0s and 1s for transmission over the physical medium.
- It deals with the electrical, optical, or radio signals that represent the bits.
- The bits are transmitted to the receiving device.

Decapsulation Process: -

Physical Layer: This is the actual hardware that transmits the raw bitstream over a physical medium, such as cables or radio waves. No headers or footers are added or removed here.

Data Link Layer: When data arrives at this layer, the physical layer's raw bits are assembled into frames. The data link layer removes the frame header and trailer added by the data link layer of the sender.

Network Layer: The data is then passed up to the network layer, where the network layer header (containing source and destination IP addresses, etc.) is removed. This layer works with packets.

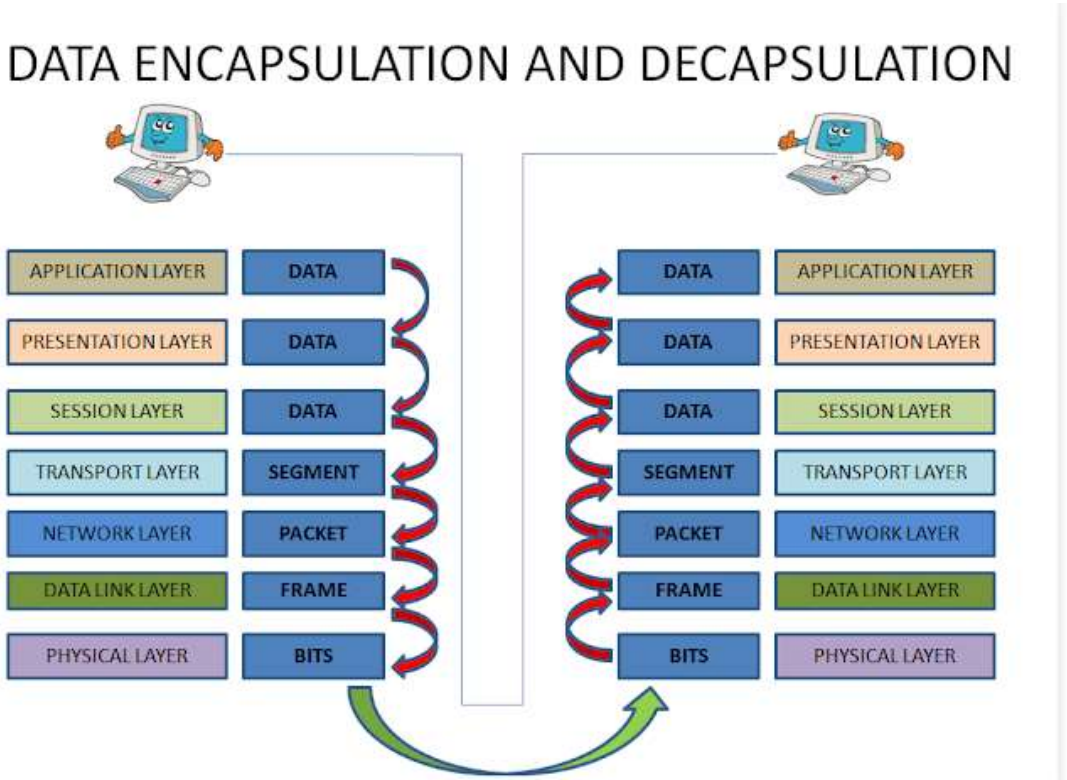
Transport Layer: The transport layer header, which includes information such as source and destination port numbers, sequence, and acknowledgment numbers, is removed. This layer works with segments (TCP) or datagrams (UDP).

Session Layer: This layer manages sessions and dialogs. It establishes, maintains, and terminates connections between applications. Session layer information is processed, but there are no specific headers or trailers to be removed.

Presentation Layer: This layer translates data between the application layer and the network format. It handles data encryption, compression, and translation. Decapsulation involves converting the data to a format that the application layer can understand.

Application Layer: Finally, the data reaches the application layer, where it is used by end-user applications such as web browsers, email clients, and file transfer programs.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



Difference Between OSI and TCP/IP model

OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
It has 7 layers.	It has 4 layers.
It is low in usage.	It is mostly used.
It is vertically approached.	It is horizontally approached.
Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Key Component of Ethernet Networking

Ethernet Cables:
Twisted Pair Cables: Most commonly used in modern networks, especially Cat5e and Cat6 cables, which consist of twisted pairs of wires to reduce electromagnetic interference.
Coaxial Cables: Used in older Ethernet networks but largely replaced by twisted pair cables.
Fiber Optic Cables: Used for high-speed and long-distance connections, transmitting data as light pulses.

Network Interface Cards (NICs):
Hardware installed in computers and devices to enable Ethernet communication.
Provides the physical connection to the network medium (e.g., Ethernet cable) and handles data framing and error checking.

Switches and Hubs:
Switches: Central devices that connect multiple devices within an Ethernet network, using MAC addresses to forward data only to the intended recipient.

Hubs: Older technology that broadcasts data to all connected devices, resulting in more network collisions and inefficiency.

Routers:
Devices that connect multiple networks, such as connecting a LAN to the internet.
Routes data packets based on IP addresses.

Ethernet Frames:
The data packet structure used in Ethernet networks.
Contains the destination and source MAC addresses, payload (actual data), and error-checking information.

Ethernet Standards

Ethernet standards are defined by the IEEE (Institute of Electrical and Electronics Engineers) and designated as IEEE 802.3. Key standards include:

- **10BASE-T**: Operates at 10 Mbps using twisted pair cables.
- **100BASE-TX (Fast Ethernet)**: Operates at 100 Mbps using twisted pair cables.
- **1000BASE-T (Gigabit Ethernet)**: Operates at 1 Gbps using twisted pair cables.
- **10GBASE-T**: Operates at 10 Gbps using twisted pair cables.
- **100GBASE-T**: Operates at 100 Gbps, typically using fiber optic cables.

Key Component of Wireless Networking?

1. **Wireless Access Points (APs)**:
    - Devices that broadcast and receive radio signals to connect wireless devices to a wired network.
    - Often integrated into routers.
2. **Wireless Routers**:

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- Combine the functions of a router and an access point, providing both wireless connectivity and network routing.

3. **Network Interface Cards (NICs)**:
   - Built into devices or available as external adapters, these enable devices to connect to wireless networks.

Wireless Standards

Defined by the IEEE 802.11 family, common standards include:

- **802.11n**: Up to 600 Mbps.
- **802.11ac**: Up to several Gbps, better range and speed.
- **802.11ax (Wi-Fi 6)**: Improved performance in congested areas, higher data rates, better energy efficiency.

Operation

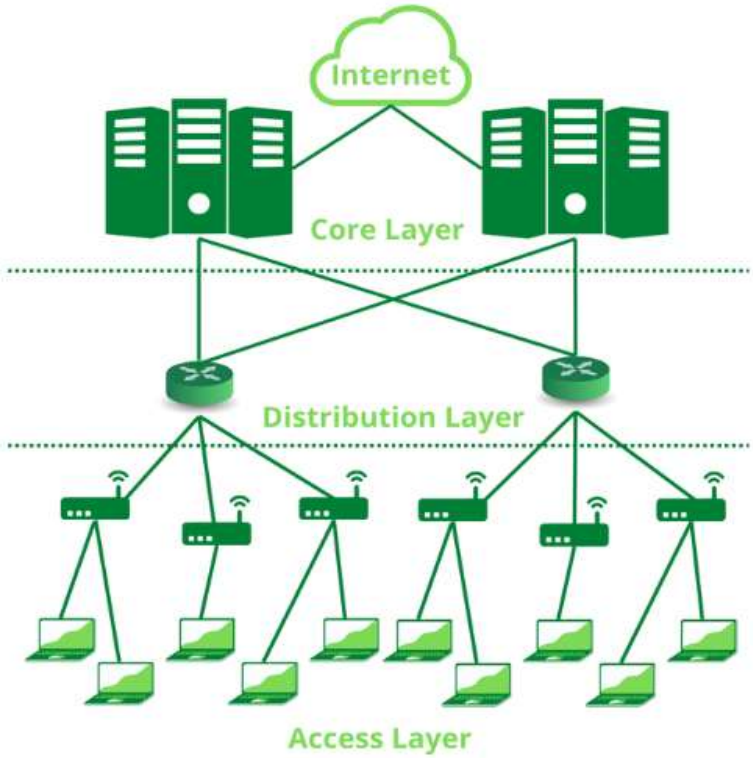
1. **Data Transmission**:
   - Uses radio frequencies (typically 2.4 GHz and 5 GHz bands) to transmit data.
   - Devices communicate with the AP, which routes data to the network or internet.
2. **Security**:
   - Common protocols include WEP, WPA, and WPA2, with WPA3 being the latest standard for enhanced security.

Advantages

- **Mobility**: Devices can connect from anywhere within the network's range.
- **Convenience**: No need for physical cables.
- **Scalability**: Easy to add new devices to the network. Considerations
- **Interference**: Radio signals can be affected by other electronic devices, physical obstacles, and other Wi-Fi networks.
- **Range**: Limited by the power of the AP and environmental factors.
- **Security**: Wireless networks are more vulnerable to unauthorized access, requiring robust encryption methods.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Cisco Three Layer Hierarchical Model



- **Access** – controls user and workgroup access to the resources on the network. This layer usually incorporates Layer 2 switches and access points that provide connectivity between workstations and servers. You can manage access control and policy, create separate collision domains, and implement port security at this layer.
- **Distribution** – serves as the communication point between the access layer and the core. Its primary functions are to provide routing, filtering, and WAN access and to determine how packets can access the core. This layer determines the fastest way that network service requests are accessed – for example, how a file request is forwarded to a server – and, if necessary, forwards the request to the core layer. This layer usually consists of routers and multilayer switches.
- **Core** – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high speed devices, like high end routers and switches with redundant links.

What is broadcast and collision domains?

- **Broadcast Domain**

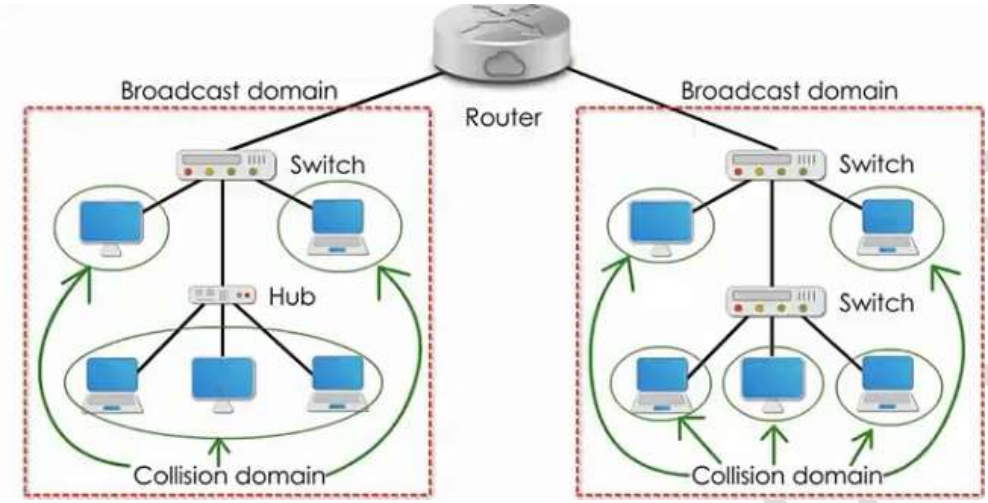
A Broadcast Domain is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain have to pay attention to it. This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

- **Collision Domain**

A Collision Domain is a scenario in which when a device sends out a message to the network, all other devices

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

which are included in its collision domain have to pay attention to it, no matter if it was destined for them or not. This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time. Remember, it happens only in the case of a half-duplex mode.



Introduction to Cisco IOS: -

IOS (Internetwork Operating System) is a multitasking operating system used on most Cisco Systems routers and switches. IOS has a command-line interface with a predetermined number of multiple-word commands. The IOS operating system is used to configure routing, switching, internetworking and other features supported by Cisco IOS devices.

There are three most common ways to access the Cisco IOS:

1. Console Access – This type of access is usually used to configure newly acquired devices. These devices usually don't have an IP address configured, and therefore cannot be accessed through the network. Most of the Cisco devices have a physical console port. This port can be connected to a computer using a rollover cable, a special type of cable with pins on one end and reversed on the

Telnet Access – this type of access used to be a common way to access network devices. Telnet is a terminal emulation program that enables you to access IOS through the network and configure the device remotely. The device that is being configured needs to have a Telnet server installed and an IP address configured.
Telnet uses a well-known TCP port 23. One of the biggest disadvantages of this protocol is that it sends all data as clear text, which includes the passwords! This is the reason why this type of access is usually not used anymore. Instead, SSH is usually used.

SSH Access – like Telnet, this access type enables you to configure devices remotely, but it adds an extra layer of security by encrypting all communications using public-key cryptography. SSH uses the well-known TCP port 22.

IOS has many different modes. There are three main modes and many sub-modes. We will describe the three main modes and one sub-mode.

- **User EXEC Mode** – the default mode for the IOS CLI. This is the mode that a user is placed in after accessing the IOS. Only basic commands (like ping or telnet) are available in this mode.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Steps of Router Boot Sequence:

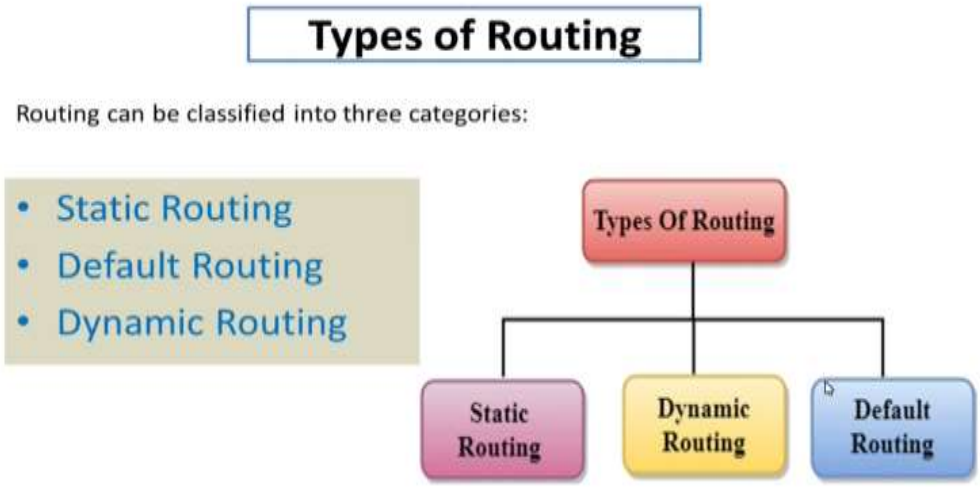
1. When the router is turned on it performs the POST (Power On Self-Test) program. The POST program tests the present hardware and checks it is operational or not. The POST programs are stored and run from the ROM.
2. The bootstrap program present in the ROM checks the Configuration Register value to find where to load the IOS. The default value of configuration register 0x2102 indicates that the router should load the Cisco IOS Operating System software image from the flash memory and load the startup configuration.
3. The Bootstrap Program looks for and loads the IOS program to the configuration register. This program is also responsible for initializing the hardware and finding the IOS program location and loading the IOS image from the flash memory.
4. If the Bootstrap program does not find the IOS image it will act as ROM Monitor. It supports a command line that is used to perform configuration tasks.
5. The IOS finds the valid configuration file stored in NVRAM. This file is called startup-config.
6. If the Startup configuration(startup-config) is present in NVRAM the router loads the file into RAM and applies the startup-config file. If the file is not present in NVRAM it tries to load a file from TFTP. If no TFTP server responds it enters the Setup mode.
7. When the Startup Configuration is loaded IOS will display CLI mode in user mode.

Router memory type

- **Read-Only Memory (ROM):** ROM stores the bootstrap startup program of the router along with the operating system software and other test programs like POST programs (Power On Self-Test).
- **Flash Memory:** Flash memory generally called flash holds the IOS images. The flash content is used by the router at the time of reload. Flash is erasable and reprogrammable ROM.
- **Random Access Memory (RAM):** RAM stores information such as routing tables and running configuration files. RAM is volatile hence; its content is lost during router power down and reload.
- **Non-volatile RAM (NVRAM):** NVRAM stores the startup configuration files. It is non-volatile RAM; hence contents are not lost during router power down and reload.

What Is Routing?

Routing in a router is the process by which a router determines the best path for data packets to travel across a network. This involves examining the destination address of the packets, consulting a routing table, and forwarding the packets to the appropriate next hop or destination. Here's a detailed explanation of routing in routers.



Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

What is routing Table?

Routing Table: A router maintains a routing table that contains information about the various paths to different network destinations. The table includes:

- Destination network addresses
- Subnet masks
- Next hop addresses (the next router in the path)
- Interface through which the packet should be forwarded
- Metrics to determine the best path (e.g., hop count, bandwidth, latency)

What is Static Routing: -

Static routing is a method of network routing where routes are manually entered into the routing table by an administrator. This involves specifying fixed paths for data packets to travel through the network. These routes do not change unless they are manually updated by the network administrator.

How Static Routing Works

- **Manual Configuration**: Network administrators manually configure routes using commands on routers.
- **Fixed Paths**: Once set, these routes remain constant unless manually modified.
- **No Dynamic Adjustments**: Unlike dynamic routing protocols, static routes do not adapt to network changes automatically.

Advantages of Static Routing

1. **Simplicity**:
   - Static routes are straightforward to configure and manage in small networks with limited routing paths.
2. **Predictability**:
   - Because the routes do not change automatically, network behavior is predictable, making troubleshooting easier.
3. **Security**:
   - Since static routes do not rely on dynamic routing protocols, there is less risk of routing information being intercepted or altered by malicious actors.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **Network A**: 192.168.1.0/24, connected to R1
- **Network B**: 192.168.2.0/24, connected to R2

To enable communication between these networks:

- On R1:

```arduino
R1(config)# ip route 192.168.2.0 255.255.255.0 <Next-hop IP address of R2>
```

- On R2:

```arduino
R2(config)# ip route 192.168.1.0 255.255.255.0 <Next-hop IP address of R1>
```

What is Dynamic Routing: -

Dynamic routing is a method used in networking where routers automatically adjust the paths that data packets take to reach their destination based on the current state of the network. Unlike static routing, which requires manual configuration, dynamic routing uses routing protocols to exchange information about network topology changes and automatically update routing tables.

Key Features of Dynamic Routing

1. **Automatic Updates**:
   - Routers dynamically share routing information and update their routing tables based on changes in the network, such as link failures or topology changes.
2. **Routing Protocols**:
   - Dynamic routing relies on specific protocols to facilitate the exchange of routing information. Common dynamic routing protocols include:
     - **RIP (Routing Information Protocol)**
     - **OSPF (Open Shortest Path First)**
     - **EIGRP (Enhanced Interior Gateway Routing Protocol)**
     - **BGP (Border Gateway Protocol)**
3. **Path Selection**:
   - Routers use metrics such as hop count, bandwidth, delay, and cost to determine the best path to a destination.
4. **Scalability**:
   - Dynamic routing is scalable and suitable for large and complex networks where manual configuration of static routes would be impractical.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Advantages of Dynamic Routing

1. **Automatic Adaptation**:
   - Routers automatically adapt to changes in the network, such as link failures or congestion, ensuring optimal routing without manual intervention.
2. **Scalability**:
   - Dynamic routing protocols can handle large and complex network topologies, making them suitable for enterprise and ISP networks.
3. **Reduced Administrative Overhead**:
   - Less manual configuration is needed compared to static routing, reducing the burden on network administrators.
4. **Efficient Network Utilization**:
   - Dynamic routing protocols can find the best paths based on real-time network conditions, leading to efficient use of network resources.

What Is The Difference Between Static And Dynamic Routing?

Static Routing	Dynamic routing
1. The network administrator must do the route entry in the routing table. 2. More overhead to a network administrator. 3. Less CPU utilization. 4. It does not use a complex algorithm. 5. Implemented in a small network. 6. Additional resources are not required.	1. Routing entry is done by routing protocol. 2. Less overhead to a network administrator. 3. High CPU utilization 4. It uses a complex algorithm. 5. Implemented in a large network. 6. Additional resources are required.

What is default routing and why it need:

Default routing is a technique used in network routing where a router is configured to send all packets destined for unknown networks to a single, specific next-hop address or exit interface. This "default route" serves as a catch-all path for any packets that do not have a more specific match in the router's routing table.

Why Default Routing is Needed

1. **Simplifies Routing Table**:
   - In networks with many potential destinations, maintaining specific routes for each possible destination can be cumbersome and resource-intensive. A default route simplifies the routing table by reducing the number of routes that need to be maintained.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

2. **Connects to Unknown Networks**:
    - Default routing is particularly useful for stub networks, which have only one route to the outside world (e.g., a small branch office connecting to a larger corporate network). It allows these networks to send traffic to any unknown destination through a single route without needing specific routes for each external network.

Configuration of Default Routing

Syntax

The syntax for configuring a default route on a Cisco router is:

```plaintext
ip route 0.0.0.0 0.0.0.0 <next-hop IP address or exit interface>
```

IP version 6 addressing

Necessity of IPv6

Here are some valid reasons why companies are beginning to migrate to an IPv6 environment:

- Currently more than 1 billion people are connected to the Internet, and this is exponentially increasing based on fast-emerging technical markets such as China and India.
- More than 1 billion mobile phones are currently on the market, most of which support limited data services, and this is expected to grow not only in numbers, but also with the enhanced offerings of data services these phone and providers are capable of delivering.
- More than 30 million PDAs and similar devices offer common data services such as e-mail and web browsing, and this number is expected to grow as more and more businesses implement mobile applications.
- More data services are being offered on consumer products, such as automobiles, household appliances, and industrial devices, and this number is expected to grow into the billions.

IPv6 Features

- **Very large address space** IPv6's large address space deals with global growth, where route prefixes can be easily aggregated in routing updates. Support for multihoming to ISPs with a single address space is easily accomplished. Autoconfiguration of addressing information, including the capability of including MAC addresses in the IP address, as well as plug and play options, simplifies address management. Renumbering and modification of addresses is easily accommodated, as well as public-to-private readdressing without involving address translation.
- **Security** IP security (IPSec) is built into IPv6, whereas it is an awkward add-on in IPv4. With IPv6, two devices can dynamically negotiate security parameters and build a secure tunnel between them with no user intervention.
- **Mobility** With the growth of mobile devices, such as PDAs and smart phones, devices can roam between wireless networks without breaking their connections.
- **Streamlined encapsulation** The IPv6 encapsulation is simpler than IPv4, providing faster forwarding rates by routers and better routing efficiency. No checksums are included, reducing processing on endpoints. No

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

broadcasts are used, reducing utilization of devices within the same subnet. QoS information is built into the IPv6 header, where a flow label identifies the traffic; this alleviates intermediate network devices from having to examine contents inside the packet, the TCP/UDP headers, and payload information to classify the traffic for QoS correctly.

Transition capabilities Various solutions exist to allow IPv4 and IPv6 to successfully coexist when migrating between the two. One method, dual stack, allows you to run both protocols simultaneously on an interface of a device. A second method, tunneling, allows you to tunnel IPv6 over IPv4 and vice versa to transmit an IP version of one type across a network using another type. Cisco supports a third method, referred to as Network Address Translation-Protocol Translation (NAT-PT), to translate between IPv4 and IPv6 (sometimes the term *Proxy* is used instead of Protocol).

IPv6 Address Format

Here are some important items concerning IPv6 addresses:

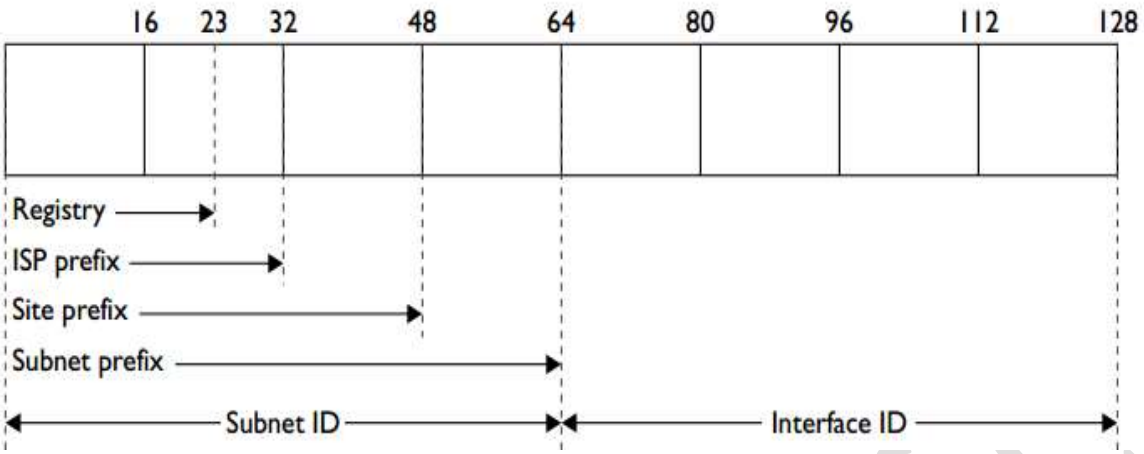
- Hexadecimal values can be displayed in either lower- or upper-case for the numbers A–F.
- A leading zero in a set of numbers can be omitted; for example, you could either enter *0012* or *12* in one of the eight fields—both are correct.
- If you have successive fields of zeroes in an IPv6 address, you can represent them as two colons (: :). For example, *0:0:0:0:0:0:0:5* could be represented as:*5*; and *ABC:567:0:0:8888:9999:1111:0* could be represented as *ABC:567::8888:9999:1111:0*. However, you can only do this *once* in the address: *ABC:567::891::00* would be invalid since *::* appears more than once in the address. The reason for this limitation is that if you had two or more repetitions, you wouldn't know how many sets of zeroes were being omitted from each part.
- An unspecified address is represented as *::*, since it contains all zeroes.

Types of IPv6 Addresses

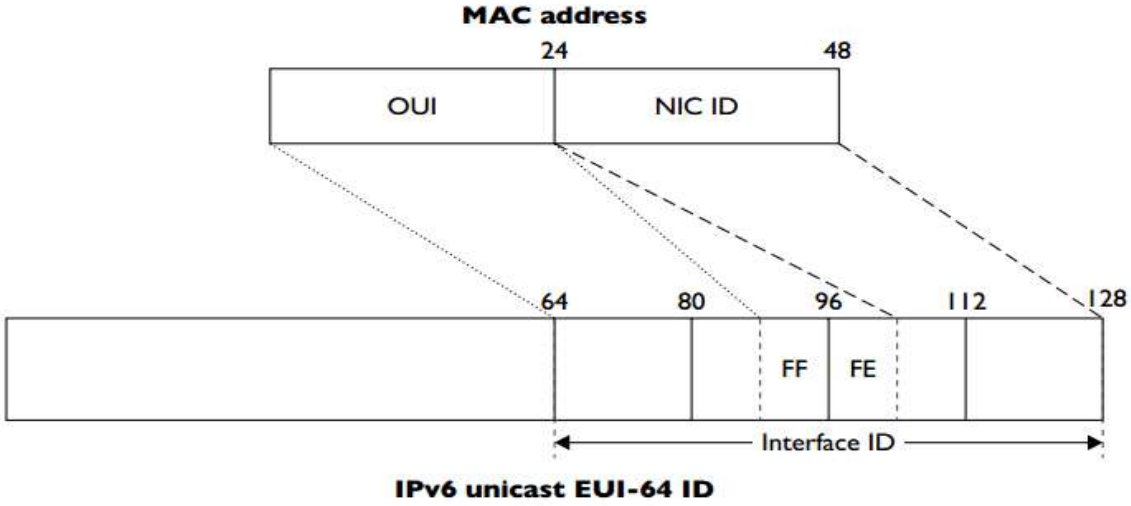
- **Anycast** Very different from an IPv4 broadcast—one-to-the-nearest interface, where many interfaces can share the same address
- **Multicast** Similar to a multicast in IPv4—one to a group of devices
- **Unicast** Represents a single interface

Global Addresses With the exception of the multicast address space of FF00: :/8, unicast and anycast addresses make up the rest. However, IANA has currently assigned only 2000: :/3 addresses to the global pool, which is about 1/6th of the available IPv6 addresses. Of these addresses, only 2001: :/16 are assigned to various Internet address registries. Global unicast addresses are made up of two components, shown in Figure 24-2: subnet ID (64 bits) and an interface ID (64 bits). The subnet ID contains the registry of the address (which is responsible for assigning it, such as IANA), the ISP prefix (which ISP is associated with the address), the site prefix (which company is assigned the address space), and a subnet prefix (subnets within the site). ISPs are assigned an ISP prefix range that allows them easily to aggregate their prefixes, advertising just a single route to the Internet backbone; this alleviates one main problem today with how the Internet grew and how ISPs, initially, were assigned IPv4 address spaces that could not easily be summarized. Another advantage of this address allocation is that the subnet prefix is 16 bits in length. Therefore, with a single global site address, a company can address up to 65,536 subnets.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



The last half of the IPv6 address, the interface ID, represents a particular interface within the site. One requirement with addresses from 2000::/3 through E000::/3 is that the interface ID must have a 64-bit value in it to be considered valid. Therefore, addresses that have 0s for the last 64 bits are considered invalid IPv6 unicast addresses. For example, 2004:1234:5678:90AB:: is invalid, since the interface ID (the last 64 bits—that is, the last four sets of numbers) are binary zeroes.



IPv6 unicast EUI-64 ID

Address Assignment

You can use four methods to assign an interface an IPv6 address: two are done statically and two dynamically. The following three

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Suggestive Questions

Multiple-choice Questions

1. **Which layer of the OSI model is responsible for data encryption and decryption?**

   A. Physical
   B. Data Link
   C. Network
   D. Presentation

2. **At which layer of the OSI model does routing occur?**

   A. Physical
   B. Data Link
   C. Network
   D. Transport

3. **Which of the following is NOT a function of the Data Link layer in the OSI model?**

   A. Error detection and correction
   B. Frame sequencing
   C. Path determination
   D. Media access control

4. **What is the primary purpose of the Transport layer in the OSI model?**

   A. Addressing
   B. Data encapsulation
   C. Reliable data transfer
   D. Data representation

5. **Which protocol operates at the Network layer of the OSI model?**

   A. TCP
   B. IP
   C. FTP
   D. Ethernet

IP Addressing

6. **What is the default subnet mask for a Class B IP address?**

   A. 255.0.0.0
   B. 255.255.0.0
   C. 255.255.255.0
   D. 255.255.255.255

7. **Which of the following IP addresses is a loopback address?**

   A. 10.0.0.1
   B. 169.254.0.1
   C. 127.0.0.1
   D. 192.168.0.1

8. **What is the purpose of a subnet mask in IP addressing?**

   A. To identify the network portion of an IP address
   B. To identify the host portion of an IP address
   C. To identify the default gateway
   D. To identify the broadcast address

9. **Which of the following is a private IP address range?**

   A. 172.32.0.0 - 172.33.255.255
   B. 192.168.0.0 - 192.168.255.255
   C. 200.0.0.0 - 200.0.0.255
   D. 224.0.0.0 - 224.0.0.255

10. **What does CIDR stand for?**

    A. Classless Internet Domain Routing
    B. Classful Inter-Domain Routing
    C. Classless Inter-Domain Routing
    D. Classful Internet Domain Routing

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Routing Basics

11. **What is the primary function of a router?**

A. Connect multiple devices within the same network
B. Forward data packets between different networks
C. Provide IP addresses to devices
D. Translate domain names into IP addresses

12. **Which of the following routing protocols is a distance vector protocol?**

A. OSPF
B. EIGRP
C. RIP
D. BGP

13. **What does the acronym BGP stand for?**

A. Border Gateway Protocol
B. Basic Gateway Protocol
C. Border Group Protocol
D. Backbone Gateway Protocol

14. **Which metric does OSPF use to determine the best path to a destination?**

A. Hop count
B. Bandwidth
C. Delay
D. Cost

15. **Which type of routing protocol is OSPF?**

A. Distance vector
B. Link state
C. Path vector
D. Static

16. **In EIGRP, what is the feasible successor?**

A. The best path to a destination
B. A backup path to a destination
C. The path with the highest bandwidth
D. The path with the lowest delay

17. **Which command would you use to view the routing table on a Cisco router?**

A. show ip route
B. show ip interface
C. show version
D. show interfaces

18. **What is a characteristic of dynamic routing?**

A. Requires manual configuration
B. Automatically adapts to network changes
C. Uses a fixed path for data packets
D. Suitable for small networks only

19. **Which of the following is a link-state routing protocol?**

A. RIP
B. OSPF
C. EIGRP
D. BGP

20. **What is the main advantage of using a hierarchical network design in OSPF?**

A. Simplifies IP address management
B. Reduces the size of routing tables
C. Increases network latency
D. Eliminates the need for routers

21. What is the purpose of the OSI model in networking?

A. To define the architecture for network protocols
B. To establish a framework for software development
C. To specify the physical network infrastructure
D. To manage network security

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

22. **Which layer of the OSI model is responsible for end-to-end communication and provides services like encryption and decryption?**

A. Transport Layer
B. Presentation Layer
C. Application Layer
D. Session Layer

23. **What is the primary function of the Network Layer in the OSI model?**

A. Error detection and correction
B. Data link control
C. Routing and addressing
D. Session establishment and termination

24. **Which addressing scheme is used by IPv6?**

A. 32-bit
B. 128-bit
C. 64-bit
D. 16-bit

25. **What is the purpose of ARP (Address Resolution Protocol)?**

A. To map IP addresses to MAC addresses
B. To discover the default gateway
C. To resolve domain names to IP addresses
D. To establish a secure connection

26. **In networking, what is the function of a router?**

A. Connects devices within the same network
B. Filters and forwards packets between different networks
C. Manages network security
D. Assigns IP addresses dynamically

27. **Which protocol is used for secure communication over a computer network?**

A. HTTP
B. FTP
C. SSH
D. SNMP

28. **What is the primary purpose of DNS (Domain Name System)?**

A. Assigning IP addresses to devices
B. Resolving domain names to IP addresses
C. Encrypting network communication
D. Managing network resources

29. **Which subnet mask is associated with the Class B IP address range?**

A. 255.255.255.0
B. 255.0.0.0
C. 255.255.0.0
D. 255.255.255.255

30. **What is the purpose of ICMP (Internet Control Message Protocol)?**

A. To encapsulate data for transmission
B. To manage network traffic congestion
C. To diagnose network-related issues
D. To establish a secure connection

31. **What does NAT (Network Address Translation) do in networking?**

A. Assigns unique IP addresses to devices
B. Maps private IP addresses to a public IP address
C. Encrypts network traffic
D. Manages network security policies

32. **Which of the following is a layer-2 device in a network?**

A. Router
B. Switch
C. Hub
D. Firewall

Correct Answer:

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Sl. No.	Right Answer
1.	D. Presentation
2.	C. Network
3.	C. Path determination
4.	C. Reliable data transfer
5.	B. IP
6.	B. 255.255.0.0
7.	C. 127.0.0.1
8.	A. To identify the network portion of an IP address
9.	B. 192.168.0.0 - 192.168.255.255
10.	C. Classless Inter-Domain Routing
11.	B. Forward data packets between different networks
12.	C. RIP
13.	A. Border Gateway Protocol
14.	D. Cost
15.	B. Link state
16.	B. A backup path to a destination
17.	A. show ip route
18.	B. Automatically adapts to network changes
19.	B. OSPF
20.	B. Reduces the size of routing tables
21.	A. To define the architecture for network protocols
22.	B. Presentation Layer
23.	C. Routing and addressing
24.	B. 128-bit
25.	A. To map IP addresses to MAC addresses
26.	B. Filters and forwards packets between different networks
27.	C. SSH
28.	B. Resolving domain names to IP addresses
29.	C. 255.255.0.0
30.	C. To diagnose network-related issues
31.	B. Maps private IP addresses to a public IP address
32.	B. Switch

Short Answer Types Questions

Network Models

1. What is the primary function of the Network Layer in the OSI model?
2. Which layer of the OSI model is responsible for error detection and recovery?
3. Name two protocols that operate at the Transport Layer of the OSI model.
4. What is the primary purpose of the Physical Layer in the OSI model?
5. Explain the difference between the OSI model and the TCP/IP model.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

IP Addressing

6. What is the difference between IPv4 and IPv6 addressing?
7. How many bits are there in a subnet mask for a Class C IPv4 address?
8. What is the purpose of a subnet mask in IP addressing?
9. Define private IP addresses and give an example of a private IP address range.
10. What is a loopback IP address and what is its purpose?

Routing Basics

11. What is the primary function of a router in a network?
12. Explain the concept of routing tables.
13. What is the difference between static and dynamic routing?
14. Name two common dynamic routing protocols.
15. What is the purpose of the default gateway in a network?

Long Answer Types Questions

Network Models

1. Describe the functions of the Data Link Layer in the OSI model and name two sublayers.
2. Compare and contrast the OSI model with the TCP/IP model in terms of layers and functionality.
3. Explain the role of the Session Layer in the OSI model and provide two examples of protocols that operate at this layer.

IP Addressing

4. Differentiate between classful and classless IP addressing, providing examples for each.
5. Explain the concept of CIDR (Classless Inter-Domain Routing) and its advantages over traditional IP addressing methods.
6. Describe the process of subnetting and its benefits in network management.

Routing Basics

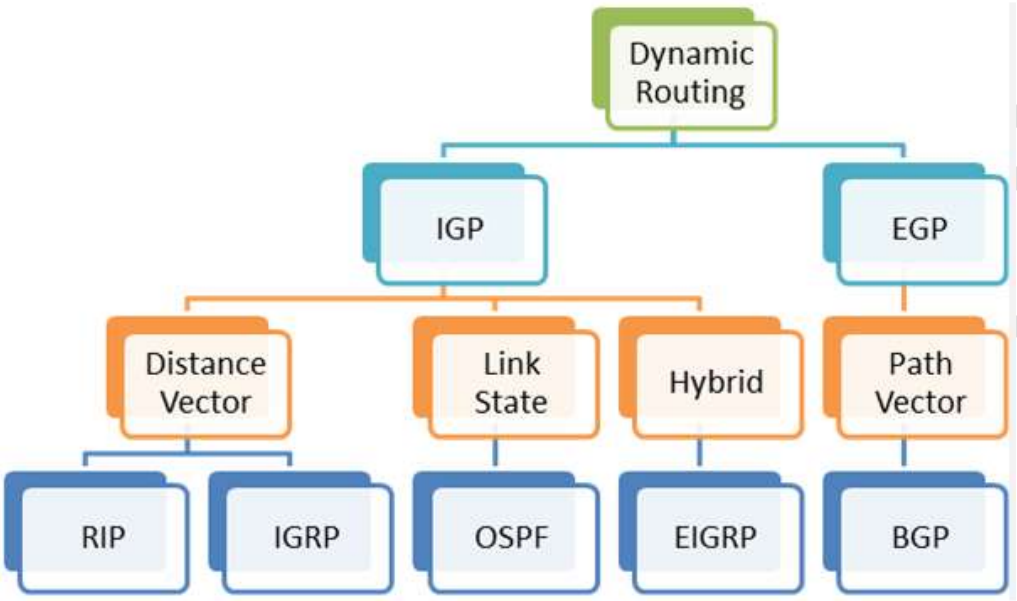
7. Explain how a router determines the best path for forwarding packets in a network.
8. Compare and contrast link-state and distance-vector routing protocols, providing examples of each.
9. Describe the purpose and process of the Address Resolution Protocol (ARP) in n etworking.
10. Explain the difference between interior and exterior routing protocols, providing examples of each.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Module II

Dynamic Routing

Dynamic Routing Protocol Types. :-



IGP Routing Protocol: -

IGP stands for Interior Gateway Protocol, which is a type of routing protocol used within an autonomous system (AS) or a single administrative domain. An IGP is responsible for exchanging routing information between routers within the same AS

EGP Routing Protocol: -

EGP stands for Exterior Gateway Protocol. Unlike IGP (Interior Gateway Protocol), which operates within a single autonomous system (AS), EGP is used for routing between different autonomous systems in the context of the Internet or interconnected networks.

IGP	EGP
• Interior Gateway Protocol • Routing protocols used within an autonomous system • All routers will be routing within the same Autonomous boundary • RIP, IGRP, EIGRP, OSPF, IS-IS	• Exterior Gateway Protocol • Routing protocol used between different autonomous systems • Routers in different AS need an EGP • Border Gateway Protocol is extensively used as EGP

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Distance Vector Routing Protocols:

These protocols determine the best path to a destination based on the number of hops (distance) between routers. Examples include:

RIP (Routing Information Protocol): RIP uses hop count as the metric and employs the Bellman-Ford algorithm.

IGRP (Interior Gateway Routing Protocol): Cisco's proprietary distance vector protocol, which uses a composite metric including bandwidth, delay, reliability, and load.

EIGRP (Enhanced Interior Gateway Routing Protocol): Also developed by Cisco, EIGRP is an advanced distance vector protocol that includes features like partial updates and convergence optimization.

Link State Routing Protocols:

These protocols build a detailed map of the network by exchanging information about network links and their states. Examples include:

OSPF (Open Shortest Path First): OSPF is a link state routing protocol that uses a link state database and the Dijkstra algorithm to calculate the shortest path tree.

IS-IS (Intermediate System to Intermediate System): IS-IS is another link state protocol commonly used in larger service provider networks and also uses the Dijkstra algorithm.

Hybrid Routing Protocols:

Hybrid protocols combine features of both distance vector and link state protocols. They are designed to offer the advantages of both types while minimizing their limitations. An example is:

EIGRP (Enhanced Interior Gateway Routing Protocol): EIGRP, despite being classified as a distance vector protocol, incorporates some link state characteristics, such as maintaining a topology table.

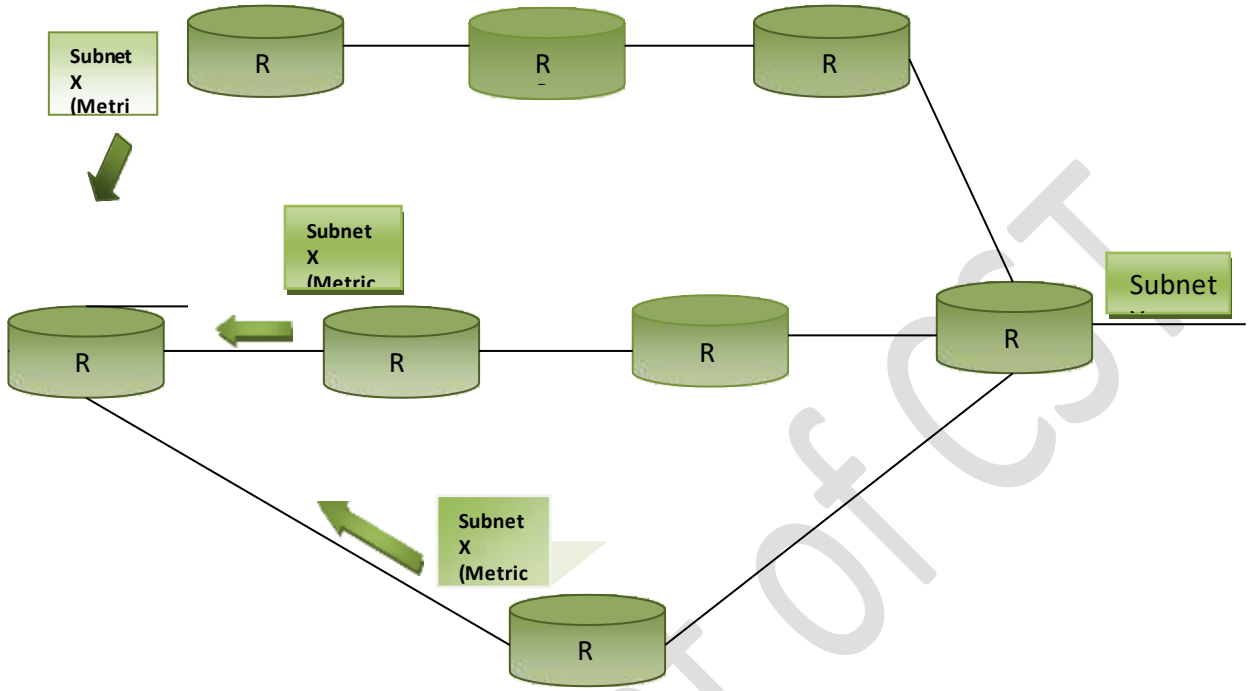
Path Vector Routing Protocols:

- These protocols are similar to distance vector protocols but maintain more information about the path to each destination. The main example is:
  - **BGP (Border Gateway Protocol)**: BGP is the core routing protocol of the Internet and operates by exchanging routing and reachability information with other BGP systems (peers). It is unique in its use of policy-based routing decisions and path attributes.

Routing Information Protocol:

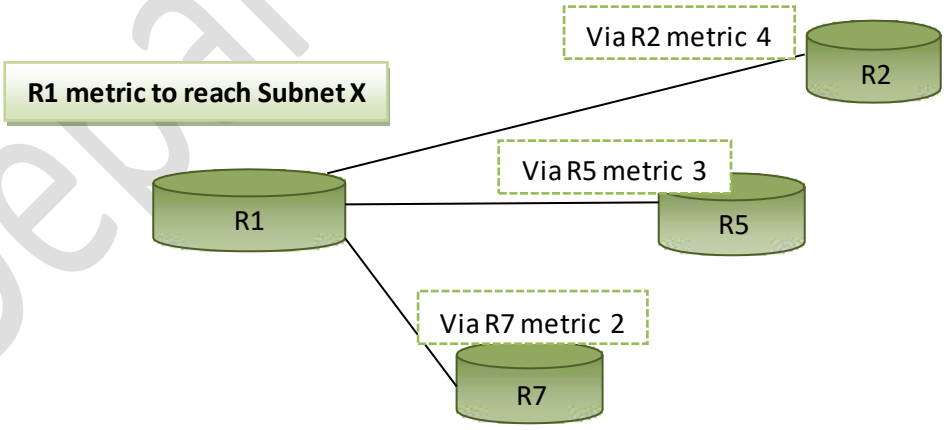
RIP is usually known as **DISTANCE VECTOR ROUTING PROTOCOL**. Here **Distance** is referring to thenumber of Hops which is calculated by the router to reach a specific destination. **Vector** means direction, i.e. the path that the router chooses to reach the subnet.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



In the above scenario if R1 want to build communication with Subnet –X then, R1 has got three different paths (via R2, via R5 and via R7) to reach Subnet X. To choose the best path, R1 will calculate the metric for each path. As according to the diagram if R1 wants to reach Subnet X via R2, then the metric for the route will 4. Similarly if R1 choose the route via R5 to reach Subnet X the metric for the route will be 3 and if R1 choose the route via R7 to reach Subnet X the metric for the route will be 2.
So the best route for R1 to reach Subnet X will be via R7 as it is having lowest metric than the other two routes i.e. via R2 and R5.

Graphical Representation of the Distance Vector Concept

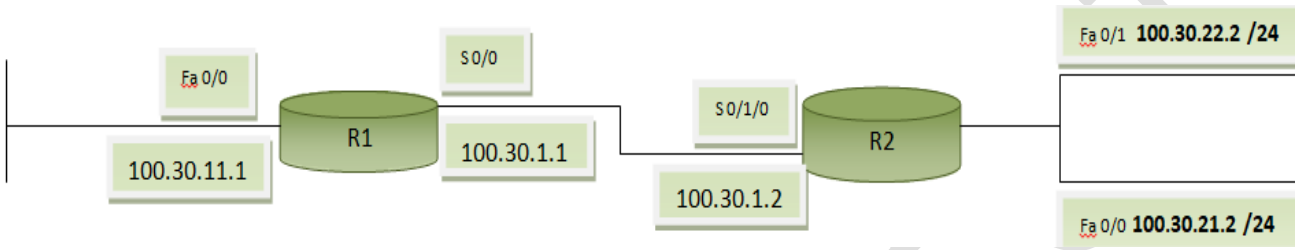


R1 knows that are three routes to reach Subnet X. If R1 choose the route via R2 the metric is 4. That means there are 4 hops via R2 or we may say that there are 4 routers between R1 and subnet X. Similarly, if R1 choose the route via R5 to reach subnet X there is 3 hops or 3 routers and 2 hops or 2 routers via R7. R1 can calculate the

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

number of hops/routers by the value of the metric, but in distance vector protocol concept the router does not have the total information of the entire topology. It only contains information about the directly connected neighbors (routers). Though it knows that there is other routers present in the topology. As in the above scenario R1 is only aware about its directly connected neighbors (i.e. R2, R5, R7). R1 does not have any information about R3, R4, R5 and R8.

Concept of Learning Route by Distance Vector Protocol



The Route Learning Process Took Place Between R1 and R2

Subnet 100.30.11.0 and 100.30.1.0 are the directly connected subnets of R1. So, their metric is considered to be 0 for R1. Similarly, subnet 100.30.1.0, 100.30.21.0 and 100.30.22.0 are the directly connected subnets of R2. So, their metric will be considered as 0 for R2.

Subnets that need to be advertise by R1 to R2 is 100.30.11.0 and the subnet that need to be advertise by R2 to R1 are 100.30.21.0 and 100.30.22.0. Subnet 100.30.1.0 is directly connected by both the routers. So, none of the routers need to advertise the route to each other.

When a router advertises any route from its routing table it adds 1 to the present metric value of the route.

When R1 receives Rip update from R2, R1 adds those Rip updates in its routing table. As R1 has got no other alternate path to reach those subnets, so the Rip update receives from R2 is the best possible route to reach the subnets.

For the learned route, R1 uses an outgoing interface S0/0 as R1 has received routing update from R2 on R1's S0/0 interface.

For the learned route, R1 will use the next hop IP address 100.30.1.2 of router R2, because in the Rip update sent by R2, the source IP address was 100.30.1.2.

R1 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Rip	100.30.21.0/24	S 0/0	100.30.1.2	1
Rip	100.30.22.0/24	S 0/0	100.30.1.2	1
Conn	100.30.1.0/24	S 0/0	N/A	0
Conn	100.30.11.0/24	FA 0/0	N/A	0

R2 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Conn	100.30.21.0/24	FA0/0	N/A	0
Conn	100.30.22.0/24	FA0/1	N/A	0
Conn	100.30.1.0/24	S0/1/0	N/A	0
Rip	100.30.11.0/24	S0/1/0	100.30.1.1	1

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Important Fasts of Distance Vector Routing Protocol

Periodic: In Distance Vector Routing the routing updates are sent in regular intervals. The default interval timer is 30 sec.

Full updates: The routers sends full updates each and every time, instead of sending changed or new routing information.

Full updates limited by Split Horizon rule: The router omits some routes in routing table because of the split horizon rule. This rule is implemented for loop avoidance in the network.

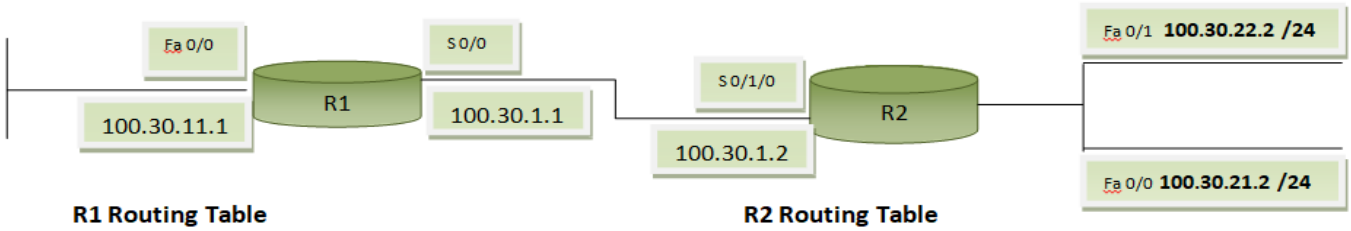
What is Routing Loop

It is the process where a router forwards a packet towards the destination and the packets repeatedly returns to the source and the process continue to go on. This result in wastage of unnecessary bandwidth and generation of useless traffic. Distance Vector Protocol is very simple and due its simplicity it introduces the possibility of routing loop.

Factors of loop prevention

- **Split Horizon Rule**
- **Route Poison**
- **Poison Reverse**
- **Hold Down Process and Hold Down Timer**

Split Horizon Rule: This rule says that router will not add those routes in its routing update whose outgoing interface is same from where the routing update is forwarded



R1 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Rip	100.30.21.0/24	S 0/0	100.30.1.2	1
Rip	100.30.22.0/24	S 0/0	100.30.1.2	1
Conn	100.30.1.0/24	S 0/0	N/A	0
Conn	100.30.11.0/24	FA 0/0	N/A	0

R2 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Conn	100.30.21.0/24	FA0/0	N/A	0
Conn	100.30.22.0/24	FA0/1	N/A	0
Conn	100.30.1.0/24	S0/1/0	N/A	0
Rip	100.30.11.0/24	S0/1/0	100.30.1.1	1

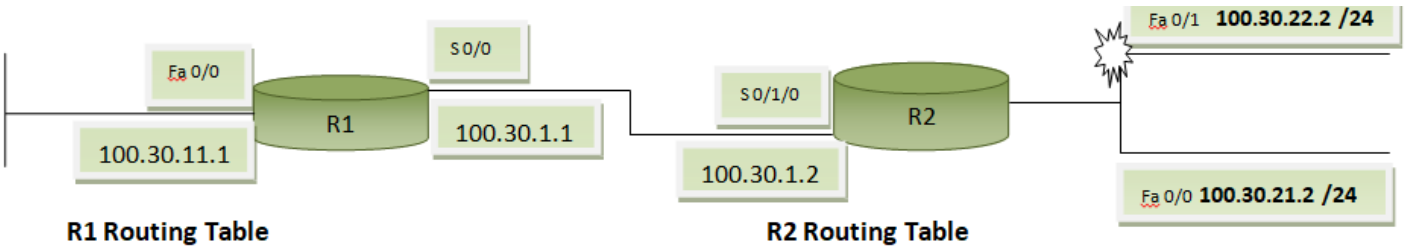
- In this scenario, in the routing table of R1 is having information of four subnets. But at the time of sending routing update it only sends information about the subnet 100.30.11.0, because the outgoing interface of all the other subnet is same with the interface from where the routing update is advertised (i.e. interface s 0/0).

- Similarly, R2 is also having information of four subnets in its routing table. At the time of sending routing update through interface S0/1/0, the router will omit those routes whose outgoing interface is S0/1/0 in the

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

routing table.

Route Poison: When any link or subnet of a router goes down, the router immediately reacts with the change and also informs the other router about the change. This helps the other routers in the network to know about the poison route and update the information in its routing table.



R1 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Rip	100.30.21.0/24	S 0/0	100.30.1.2	1
Rip	100.30.22.0/24	S 0/0	100.30.1.2	16
Conn	100.30.1.0/24	S 0/0	N/A	0
Conn	100.30.11.0/24	FA 0/0	N/A	0

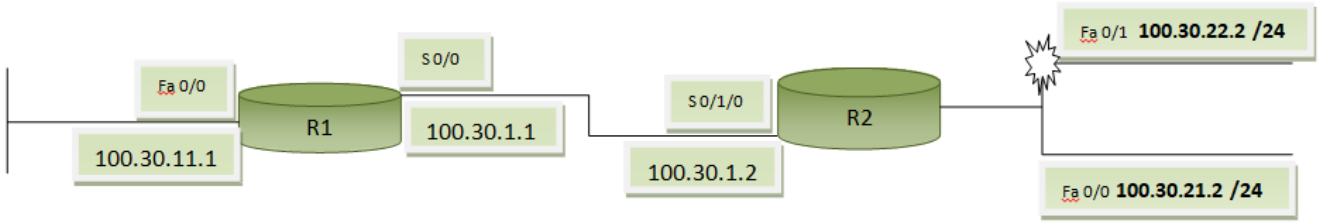
R2 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Conn	100.30.21.0/24	FA0/0	N/A	0
Conn	100.30.22.0/24	FA0/1	N/A	0
Conn	100.30.1.0/24	S0/1/0	N/A	0
Rip	100.30.11.0/24	S0/1/0	100.30.1.1	1

- In the above scenario of route poison, a subnet (100.30.22.0) of R2 goes down, the router R2 immediately reactwith the change and remove the link information from the routing table.
- As R1 receives the information update about the poison route from R2, R1 immediately mark the route as an infinite route in its routing table.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Poison Reverse: It is the process where, when a router receives a poison route message, the router suspends thesplit horizon rule and forward back the message towards the source.



R1 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Rip	100.30.21.0/24	S 0/0	100.30.1.2	1
Rip	100.30.22.0/24	S 0/0	100.30.1.2	16
Conn	100.30.1.0/24	S 0/0	N/A	0
Conn	100.30.11.0/24	FA 0/0	N/A	0

R2 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Conn	100.30.21.0/24	FA0/0	N/A	0
Conn	100.30.22.0/24	FA0/1	N/A	0
Conn	100.30.1.0/24	S0/1/0	N/A	0
Rip	100.30.11.0/24	S0/1/0	100.30.1.1	1

PROCESS-1

100.30.22.0, Metric-16
Triggered partial update

PROCESS-2

100.30.22.0, Metric-16
Triggered partial update

R1 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Rip	100.30.21.0/24	S 0/0	100.30.1.2	1
Rip	100.30.22.0/24	S 0/0	100.30.1.2	16
Conn	100.30.1.0/24	S 0/0	N/A	0
Conn	100.30.11.0/24	FA 0/0	N/A	0

R2 Routing Table

Source	Subnet	Out int.	Next Hop	Metric
Conn	100.30.21.0/24	FA0/0	N/A	0
Conn	100.30.22.0/24	FA0/1	N/A	16
Conn	100.30.1.0/24	S0/1/0	N/A	0
Rip	100.30.11.0/24	S0/1/0	100.30.1.1	1

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Hold-down Process and Hold-down Timer

When a subnet or link is considered to be in down state the routers hold it down for a while so that,other routers know and ensure that a link has gone down. This process is called Hold-down process.

When a router hears a poison route advertisement from the other router, the router starts a Hold-down timer for that route. Until the timer expires, the router does not believe any routing advertisement for that route. However, if the router gets any information from the primary source,the router believes the update information, before the Hold-down timer expires.

Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP.

What Is Administrative Distance:

Administrative distance is crucial in scenarios where a router receives routing information about the same network from multiple sources. The router will prefer the route with the lowest administrative distance.

- **Internal EIGRP Routes:** Routes learned within the same Autonomous System (AS) using EIGRP have an administrative distance of **90**.
- **External EIGRP Routes:** Routes learned from another AS (external routes redistributed into EIGRP) have an administrative distance of **170**.

What Is Autonomous System:

In EIGRP (Enhanced Interior Gateway Routing Protocol), an Autonomous System (AS) refers to a collection of IP networks and routers under the control of a single organization or administration that presents a common routing policy to the internet.

Neighbor Discovery:

It is the process where the router generates or sends Hello messages to discover potential EIGRP routers and perform a routine check to accept the discovered router as neighbor.

The router checks the following setting to determine if the router should be allowed to be a neighbor:

- The routers must pass the authentication process.
- The routers must use the same configured AS number.
- The source IP address used by the neighbor Hello must be in the same subnet.

Topology Exchange:

Here the neighbor exchanges the full topology database and partial updates are sent as needed based on changes to the network topology.

Choosing Routes:

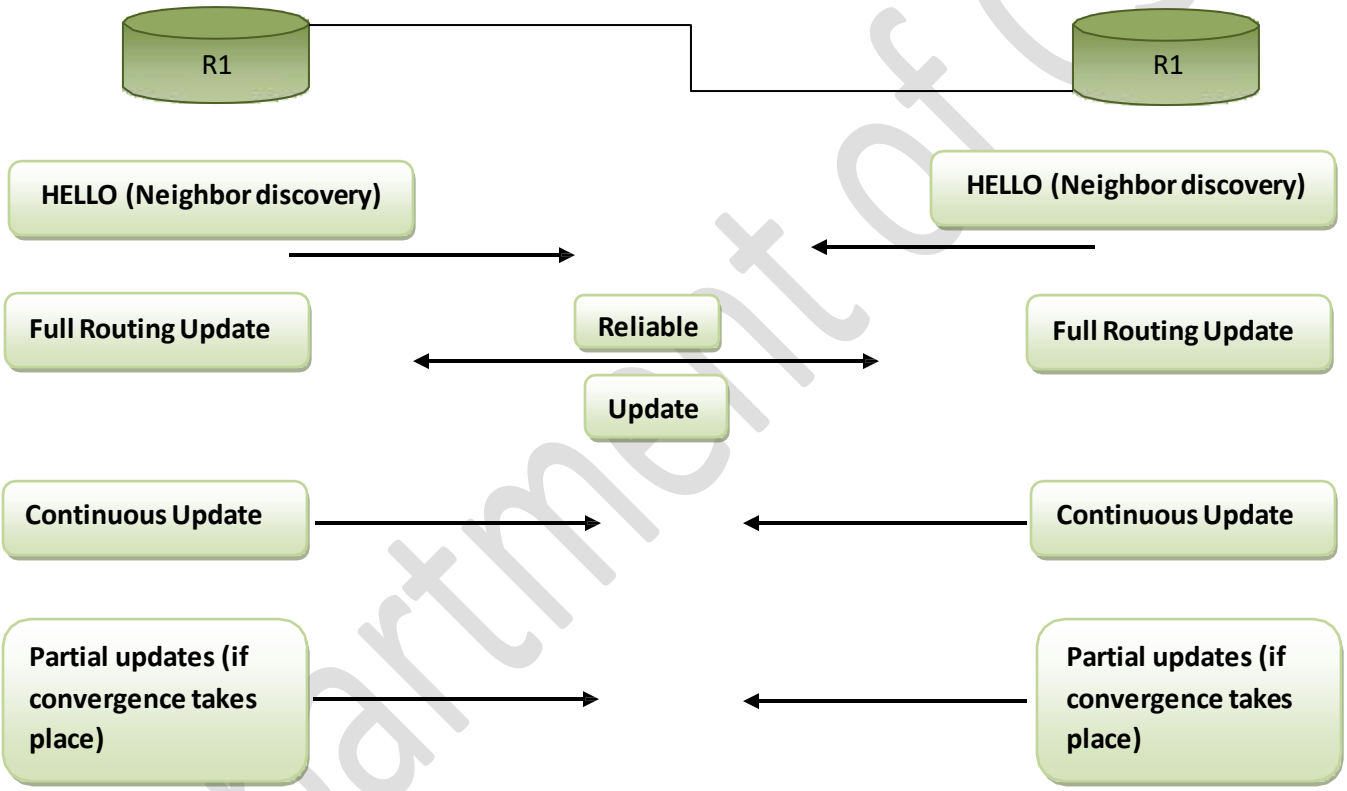
Each router analyzes its respective EIGRP topology table so that the routers can choose the lowest metric route to reach each subnet.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Messages in EIGRP

1. Hello
2. Update ---------- RTP
3. Query ----------RTP
4. Reply ----------RTP
5. Acknowledgement

Full and Partial EIGRP updates:



EIGRP metric calculation formula

METRIC = [(10^7 / Least-bandwidth) + cumulative Delay] x 256

Here: bandwidth is in kbps.

- Least- bandwidth: Represents the lowest bandwidth link in the route.
- The Cumulative-Delay value used in formula is the sum total of all the delay value for all links in the in the route. The default Delay in serial link is 20,000ms and the default Delay in fast ethernet link is 100 ms.
- Unlike OSPF there is no concept of DR and BDR.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Feasible Distance & Reported Distance

Feasible Distance:

The metric of the best route to reach a subnet, as calculated on a EIGRP router.

Reported Distance / Advertised Distance:

The metric as calculated on a neighboring router and then reported and learned in an EIGRP update.

EIGRP Successor and Feasible Successor

EIGRP calculates the metric for each subnet and find out the best route for a particular subnet, the best metric route is selected and is called the Successor. The routing table select the Successor route entry to reach a particular subnet. (This router metric is called the feasible distance).

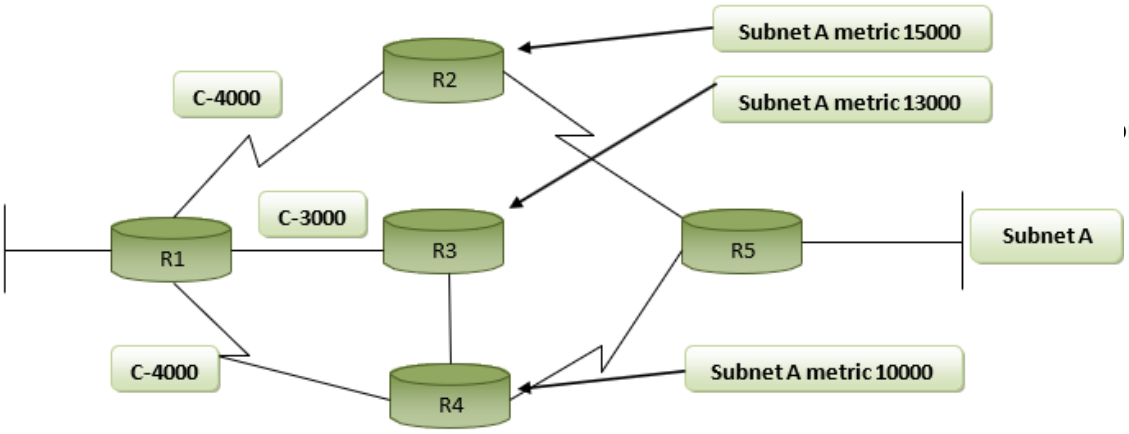
The rest of the routes discovered by the router to reach the same subnet – routes whose metric was larger than the FD, EIGRP needs to determine which can be used immediately if the currently best route fails., without causing routing loop.

These immediate alternative free backup usable routes are called Feasible Successor

Condition of becoming Feasible Successor

If a non-successor routes RD is less than the FD, the route is a Feasible Sucessor route.

called Diffusing
n. When the new



R1 calculate FD for each subnet:

Route through Router R2 – 19000
Route through Router R3 – 16000
Route through Router R4 - 14000

R1 routing table: Subnet A metric 14000 through R4

R1 topology table for subnet A

Route through R4 – SUCCESSOR
Route through R3 – FEASIBLE SUCCESSOR (as because R3 RD is 13000 which is less than R1's metric)

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Difference Between RIP and EIGRP

SR.NO	RIP	EIGRP
1.	RIP stands for Routing Information Protocol.	EIGRP stands for Enhanced Interior Gateway Routing Protocol.
2.	RIP works on Bellman Ford algorithm.	EIGRP works on DUAL (Diffusing Update Algorithm) Algorithm.
3.	It is a industry standard dynamic routing protocol.	It is a Cisco standard routing protocol.
4.	It is basically use for smaller size organization.	It is basically use for larger size organization as compared to RIP.
5.	RIP is a distance vector protocol.	EIGRP is derived from Integrated Gateway Routing Protocol.
6.	It allows maximum hop count upto 15.	It allows maximum hop count upto 255.
7.	It's administrative distance is 120.	It's administrative distance is 90.
8.	It is not a more intelligent dynamic routing protocol.	It is a more intelligent routing protocol than RIP.

Summarization in EIGRP (Enhanced Interior Gateway Routing Protocol) is a process used to reduce the size of routing tables by combining a group of contiguous networks into a single summarized route. This helps in minimizing the amount of routing information that needs to be exchanged and processed, leading to more efficient routing and reduced bandwidth usage.

Key Points of EIGRP Summarization

1. **Automatic Summarization**:
   - By default, EIGRP performs automatic summarization at classful network boundaries. This means it summarizes routes based on the major network boundaries (e.g., 192.168.0.0/16).
2. **Manual Summarization**:
   - Network administrators can configure manual summarization on EIGRP-enabled interfaces to create custom summary routes. This is typically done at the interface level.
3. **Configuration**:

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- To configure manual summarization, use the ***ip summary-address eigrp*** command followed by the EIGRP autonomous system number and the summary address with its subnet mask.

4. **Benefits**:
   - **Reduces Routing Table Size**: Summarization helps in reducing the size of routing tables, making them easier to manage.
   - **Decreases Routing Updates**: Fewer routes are advertised, which reduces the bandwidth used for routing updates.
   - **Improves Convergence**: With fewer routes, the network can converge faster in the event of topology changes.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e., the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

OSPF Terms

Router Id – It is the highest active IP address present on the router. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

Router priority – It is an 8-bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

Designated Router (DR) – It is elected to minimize the number of adjacencies formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers share their DBD. In a broadcast network, the router requests for an update to DR, and DR will respond to that request with an update.

Backup Designated Router (BDR) – BDR is a backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

DR and BDR election – DR and BDR election takes place in the broadcast network or multi-access network. Here are the criteria for the election:
The router having the highest router priority will be declared as DR.
If there is a tie in router priority then the highest router I'd be considered. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

OSPF States

The device operating OSPF goes through certain states. These states are:

Down – In this state, no hello packets have been received on the interface.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Note – The Downstate doesn't mean that the interface is physically down. Here, it means that the OSPF adjacency process has not started yet.

INIT – In this state, the hello packets have been received from the other router.

2WAY – In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.

Note – In between the 2WAY state and Ex-start state, the DR and BDR election takes place.

Ex-start – In this state, NULL DBD are exchanged. In this state, the master and slave elections take place. The router having the higher router I'd become the master while the other becomes the slave. This election decides Which router will send its DBD first (routers who have formed neighborship will take part in this election).

Exchange – In this state, the actual DBDs are exchanged.

Loading – In this state, LSR, LSU, and LSA (Link State Acknowledgement) are exchanged.

Important – When a router receives DBD from another router, it compares its own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.

Full – In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

OSPF Topology Database exchange

This is process where the OSPF routers exchange their LSDB between each other, so that both the neighbors have the exact copy of their database. This is the basic fundamental how the link-state protocol works.

When the LSA list are exchanged the LSA contain serial number. If any changes take place the LSA number get change. This determines the routers to decide when to send partial updates. So, it exchanges only missing LSA.

Choosing a Designated Router

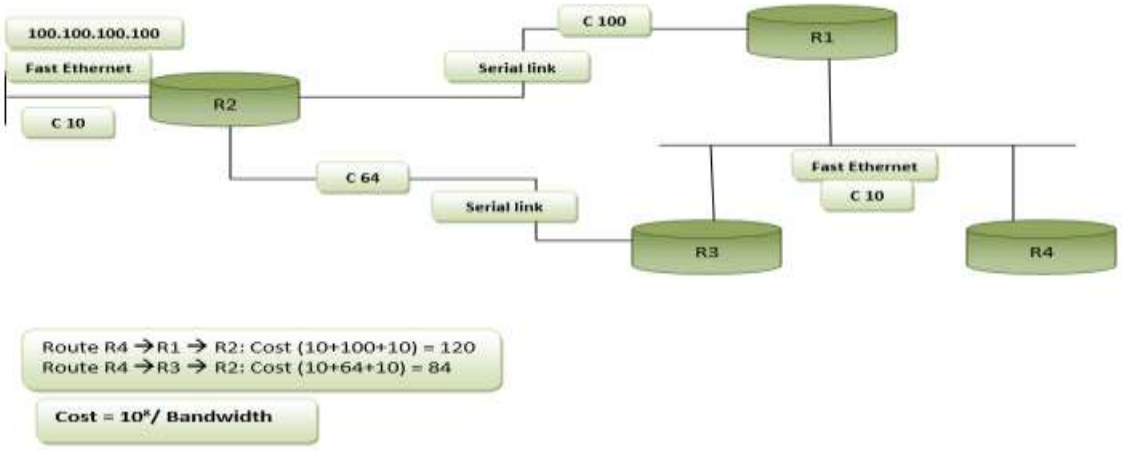
- The routers that are sending HELLO's with the highest priority is elected as DR.
- If two or more tie with the highest priority, then the router with the highest RID becomes the DR.
- Not for every time but the router having the second highest priority becomes the BDR.
- If any router having a priority setting of 0 means, that router does not participate in the election and can never become a DR or BDR.
- The range of the priority value that allows a router to become a DR or BDR are 1 through 255.
- If a new better router is added within the topology with a better priority value after DR and BDR have been elected, the new candidate does not preempt the existing DR and BDR.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Maintaining the LSDB while being fully adjacent

When the routers are in full state, still they do some maintenance work. They keep sending Hello messages at regular Hello interval. At any instance of time if the Hello message is absent for atime equal to the Dead interval means that the connection to the neighbor has failed. Also if any
topology convergence takes place then the neighbor send new copies of the changed LSA's to each neighbors so that the neighbors can change LSDB's. Each router then uses the SPF to recalculate andfind to see any routes affected by network convergence.

Sample OSPF network with Cost shown:



for each area it

Inter-Area Routing: The ABR routes traffic between different OSPF areas. It summarizes the routing information from one area and advertises it to other areas, helping to contain the size of the link-state database within each area.

LSA (Link-State Advertisement) Management: ABRs generate and propagate Type 3 (Summary LSA) and Type 4 LSAs. These LSAs help disseminate information about routes between areas and ensure that all areas have the necessary routing information without sharing every detail of each area's topology.

What Is ASBR

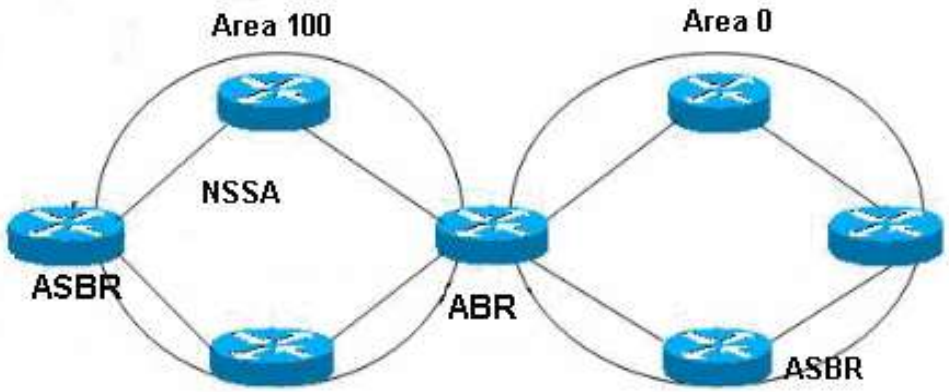
An ASBR is a router that connects an OSPF autonomous system (AS) to external networks or other autonomous systems. It redistributes routes learned from these external sources into the OSPF domain.

Role of ASBR in OSPF:

Route Redistribution: The primary function of an ASBR is to take routes learned from other routing protocols (e.g., BGP, EIGRP, RIP) or other OSPF autonomous systems and inject them into the OSPF domain. This process is known as route redistribution.

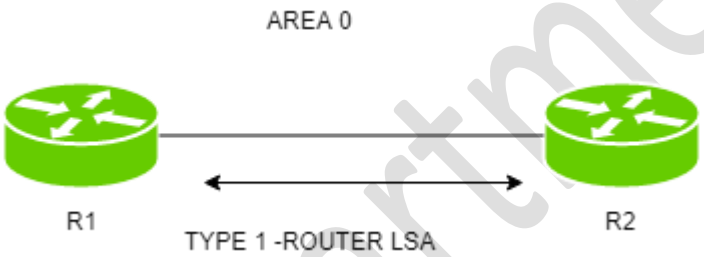
External LSAs: ASBRs generate Type 5 LSAs (External LSAs) for routes that are external to the OSPF domain and Type 7 LSAs (NSSA External LSAs) if they are located in a Not-So-Stubby Area (NSSA). These LSAs contain the external route information and are flooded throughout the OSPF network to inform all routers about the external routes.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

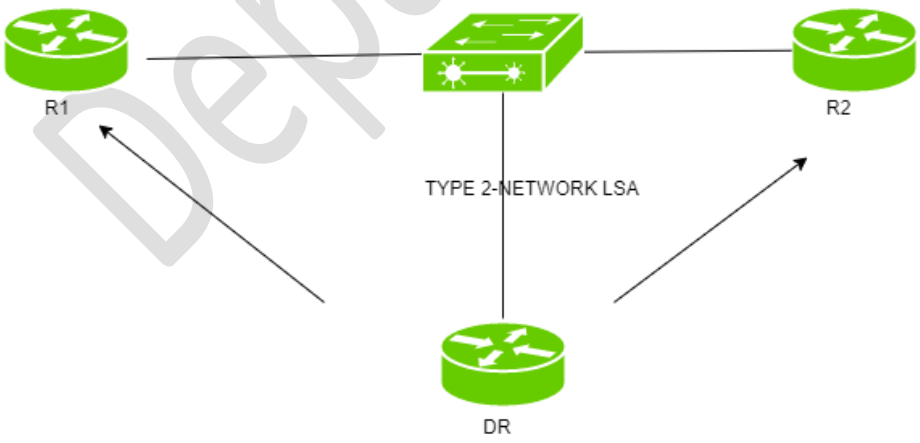


OSPF LSA Types

Router LSA	LSA Type 1
Network LSA	LSA Type 2
Summary LSA	LSA Type 3
Summary ASBR LSA	LSA Type 4
Autonomous System external LSA	LSA Type 5
Multicast OSPF LSA	LSA Type 6
NSSA External LSA	LSA Type 7



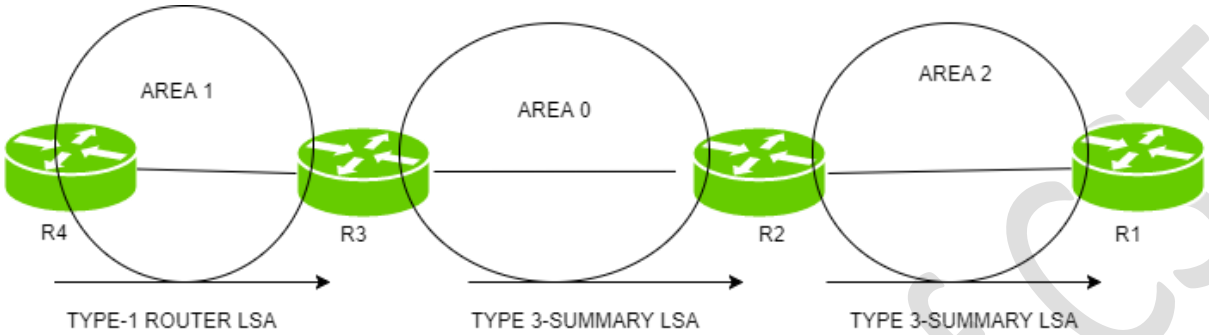
Type-1 (Router Link Advertisement) – This is a Type-1 LSA exchanged by the routers which belongs to a same area. The router contains status of link, Router I'd, IP information and current interface state. If a router is connected to multiple areas then separate Type 1 LSA is exchanged.



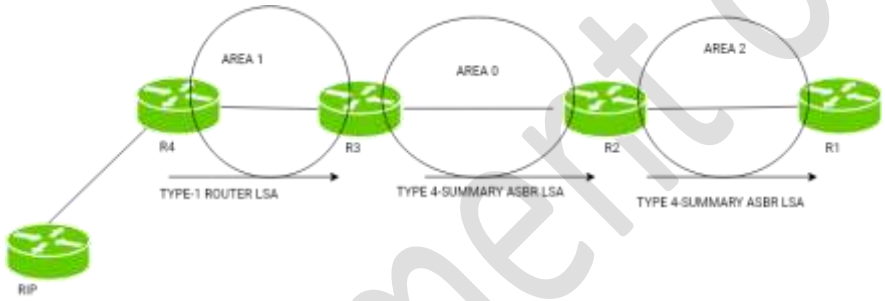
Type-2 (Network Link Advertisement) – This is a Type-2 LSA which is send by DR (Designed Router) only to all the other routers present in the same area (broadcast or multi-access network) . These contain the DR and BDR IP information and also the state of other routers that are part of same network. Remember DR is responsible for distributing routing information to all other routers present in same broadcast area.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

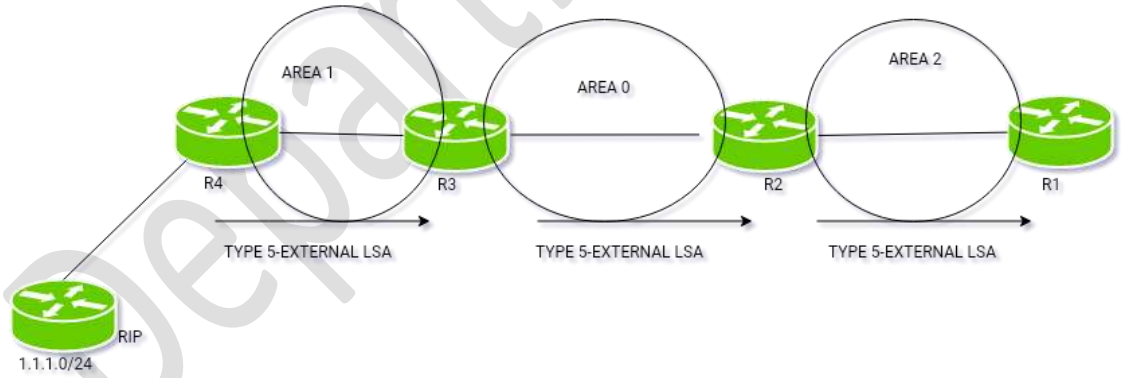
Type-3 (Summary LSA) – This is a Type-3 LSA which are generated by ABRs to areas other than in which it resides. The topological database which ABR receives from other areas are injected into the backbone area. This includes the IP information and Router I'd of ABR that is advertising these LSA.



Type-4 (Summary ASBR LSA) – ABR send these Type 4 LSA towards the area other than the area in which they are generated. These LSAs are generated by ABR to tell others the route to ASBR.



Type-5 AS external link advertisement – These LSAs are generated by ASBR to advertise routes of other Autonomous System than OSPF.



Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Difference Between EIGRP and OSPF

S. No.	Comparison	EIGRP	OSPF
1.	Stands for	Enhanced Interior Gateway Protocol.	Open Shortest Path First.
2.	Protocol type	Hybrid.	Link State.
3.	Administrative distance	90 (Internal) 170 (External).	110
4.	Algorithm	DUAL distance vector.	Dijkstra link state.
5.	Standards-based on	Cisco Proprietary.	IETF Open Standard.
6.	Routing metrics	Combination of bandwidth, reliability, load and delay.	Interface bandwidth.
7.	CPU requirements	Lower CPU and memory needs.	Require high CPU and memory.
8.	Ease of implementation	Easy but no provision of auto-summary.	Complicated.
9.	Organized as	It lacks a hierarchical structure.	It is hierarchically organized.
10.	Used by	It is primarily utilized by medium-sized to large-sized networks.	It primarily serves larger organizations in networks.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Suggestive Questions

Multiple-choice Questions

1. RIP uses which type of metric for route determination?
   a) Bandwidth
   b) Delay
   c) Hop count
   d) MTU

2. What is the maximum hop count for RIP?
   a) 15
   b) 16
   c) 31
   d) 32

3. RIP operates at which layer of the OSI model?
   a) Network
   b) Data Link
   c) Transport
   d) Application

4. Which port number does RIP use for its operations?
   a) 80
   b) 110
   c) 520
   d) 8080

5. How often does RIP send out routing updates by default?
   a) Every 15 seconds
   b) Every 30 seconds
   c) Every 60 seconds
   d) Every 90 seconds

6. EIGRP is a hybrid routing protocol that uses characteristics of which two types of routing protocols?
   a) Distance-vector and link-state
   b) Distance-vector and path-vector
   c) Link-state and path-vector
   d) None of the above

7. What algorithm does EIGRP use for finding the shortest path?
   a) Bellman-Ford
   b) Dijkstra
   c) DUAL (Diffusing Update Algorithm)
   d) A* algorithm

8. Which multicast address does EIGRP use to send updates?
   a) 224.0.0.9
   b) 224.0.0.5
   c) 224.0.0.10
   d) 224.0.0.7

9. EIGRP maintains a copy of its neighbour's routing tables. What is this table called?
   a) Routing table
   b) Topology table
   c) Neighbor table
   d) Link-state table

10. By default, EIGRP uses which metrics to calculate its metric?
    a) Bandwidth and delay
    b) Bandwidth and hop count
    c) Bandwidth, delay, load, and reliability
    d) Bandwidth, delay, and MTU

11. OSPF is classified as which type of routing protocol?
    a) Distance-vector
    b) Link-state
    c) Path-vector
    d) Hybrid

12. OSPF uses which algorithm to determine the shortest path?
    a) Bellman-Ford
    b) Dijkstra
    c) DUAL
    d) A* algorithm

13. What is the multicast address used by OSPF to send hello packets to all OSPF routers?
    a) 224.0.0.9
    b) 224.0.0.5
    c) 224.0.0.10
    d) 224.0.0.6

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

14. In OSPF, what is the router ID?
    a) An IP address assigned to each OSPF router
    b) A unique identifier for each OSPF router, often the highest IP address on an active interface
    c) The IP address of the router's interface connected to the backbone
    d) The MAC address of the router

15. What is the main purpose of OSPF areas?
    a) To simplify administration
    b) To reduce the size of the routing table
    c) To optimize the network and reduce the amount of routing information that must be processed
    d) To provide security for routing updates

Dynamic Routing

16. What is the primary advantage of dynamic routing over static routing?
    a) It is easier to configure
    b) It adapts automatically to changes in the network
    c) It requires less memory
    d) It is more secure

17. Which of the following is NOT a dynamic routing protocol?
    a) RIP
    b) OSPF
    c) BGP
    d) ARP

18. Which dynamic routing protocol is typically used for routing within an autonomous system (AS)?
    a) BGP
    b) EIGRP
    c) OSPF
    d) Both b and c

19. Which of the following routing protocols use the concept of areas to segment a large network into smaller, more manageable sections?
    a) RIP
    b) EIGRP
    c) OSPF
    d) BGP

20. Which of the following is a key characteristic of link-state routing protocols?
    a) They send their entire routing table to all neighboring routers.
    b) They send updates only when there is a change in the network topology.
    c) They use a hop count as their metric.
    d) They do not require a hierarchical network design.

21. In OSPF, what is the function of the Designated Router (DR)?
    a) To reduce the number of adjacencies formed and the amount of routing information exchanged.
    b) To broadcast routing updates to all routers in the network.
    c) To act as the central router in a star topology.
    d) To handle all routing decisions within an area.

22. EIGRP uses which protocol to provide reliable delivery of packets?
    a) TCP
    b) UDP
    c) RTP (Reliable Transport Protocol)
    d) ICMP

23. What is the main purpose of using a wildcard mask in OSPF?
    a) To specify the range of IP addresses for network statements.
    b) To identify the subnet mask used by the network.
    c) To filter routing updates.
    d) To secure routing updates.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

24. Which of the following is NOT a characteristic of RIP?
    a) Uses hop count as the metric.
    b) Supports VLSM (Variable Length Subnet Mask).
    c) Sends the entire routing table in updates.
    d) Maximum hop count of 15.

25. Which OSPF network type elects a DR and BDR?
    a) Point-to-point
    b) Broadcast multi-access
    c) Non-broadcast multi-access
    d) Point-to-multipoint

26. What is the administrative distance of EIGRP for internal routes?
    a) 90
    b) 110
    c) 120
    d) 170

27. Which routing protocol uses Autonomous System Numbers (ASNs) for routing decisions?
    a) RIP
    b) OSPF
    c) EIGRP
    d) BGP

Answer:

Sl. No.	Right Answer
1.	c) Hop count
2.	a) 15
3.	a) Network
4.	c) 520
5.	b) Every 30 seconds
6.	a) Distance-vector and link-state
7.	c) DUAL (Diffusing Update Algorithm)
8.	c) 224.0.0.10
9.	b) Topology table
10.	a) Bandwidth and delay
11.	b) Link-state
12.	b) Dijkstra
13.	b) 224.0.0.5
14.	b) A unique identifier for each OSPF router, often the highest IP address on an active interface
15.	c) To optimize the network and reduce the amount of routing information that must be processed
16.	b) It adapts automatically to changes in the network
17.	d) ARP
18.	d) Both b and c
19.	c) OSPF
20.	b) They send updates only when there is a change in the network topology.
21.	a) To reduce the number of adjacencies formed and the amount of routing information exchanged.
22.	c) RTP (Reliable Transport Protocol)
23.	a) To specify the range of IP addresses for network statements.
24.	b) Supports VLSM (Variable Length Subnet Mask).
25.	b) Broadcast multi-access
26.	a) 90
27.	d) BGP

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Short Answer Type Questions

RIP (Routing Information Protocol)

1. What is the maximum number of hops allowed in RIP?
2. Name the default administrative distance for RIP.
3. What type of routing protocol is RIP considered?
4. How often does RIP send out its routing updates by default?
5. What is the significance of the RIP hold down timer?

EIGRP (Enhanced Interior Gateway Routing Protocol)

6. What does EIGRP use as its metric for determining the best path?
7. Name the algorithm used by EIGRP to calculate its routes.
8. What multicast address does EIGRP use for communication?
9. Describe the purpose of the EIGRP neighbor table.
10. What does the EIGRP successor route represent?

OSPF (Open Shortest Path First)

11. What type of metric does OSPF use to determine the best path?
12. Explain the function of OSPF area 0.
13. How does OSPF elect a Designated Router (DR) and Backup Designated Router (BDR)?
14. What is the OSPF router ID used for?
15. What OSPF packet type is used for discovering neighbors?

Dynamic Routing

16. Differentiate between dynamic routing and static routing.
17. What are the advantages of using dynamic routing protocols?
18. Name two examples of distance-vector routing protocols.
19. How do routers using dynamic routing protocols share routing information?
20. Explain the concept of route convergence in dynamic routing.

Long Answer Type Questions

RIP (Routing Information Protocol)

1. Describe the operation of RIP in terms of how it exchanges routing information and updates its routing tables.
2. Explain the concept of split horizon in RIP. How does it prevent routing loops?
3. Discuss the limitations of RIP in modern network environments and why it may not be suitable for large networks.
4. Compare and contrast RIP version 1 (RIPv1) and RIP version 2 (RIPv2) in terms of features, improvements, and differences.
5. Describe the process of route poisoning and how it is implemented in RIP to handle route failures.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

EIGRP (Enhanced Interior Gateway Routing Protocol)

6. Explain how EIGRP calculates its metric (composite metric) and discuss the factors involved in this calculation.
7. Compare and contrast EIGRP's neighbor discovery mechanism with that of other routing protocols like OSPF.
8. Discuss the benefits of EIGRP's DUAL (Diffusing Update Algorithm) compared to traditional distance-vector algorithms.
9. Describe the convergence process in EIGRP and explain how it ensures loop-free paths in a network.
10. Explain the concept of feasible successors in EIGRP and how they contribute to route redundancy and faster convergence.

OSPF (Open Shortest Path First)

11. Discuss the OSPF areas and their significance in large network deployments. Explain how OSPF reduces routing overhead using areas.
12. Compare OSPF with RIP and EIGRP in terms of scalability, convergence speed, and support for hierarchical networks.
13. Describe the OSPF router types (internal router, backbone router, ABR, and ASBR) and their roles in OSPF operation.
14. Explain OSPF's link-state database and how routers use this information to build their routing tables.
15. Discuss OSPF's metric calculation (cost) and how it differs from other routing protocols like EIGRP.

Dynamic Routing

16. Compare and contrast distance-vector and link-state routing protocols. Discuss their advantages, disadvantages, and use cases.
17. Explain the concept of routing loops in dynamic routing and how protocols like RIP, EIGRP, and OSPF prevent or mitigate them.
18. Describe the process of route redistribution and its implications in dynamic routing protocols. Provide examples where route redistribution is necessary.
19. Discuss the concept of administrative distance in dynamic routing protocols. How does administrative distance influence route selection?
20. Explain the role of routing protocols like BGP (Border Gateway Protocol) in dynamic routing. How does BGP differ from interior routing protocols like RIP, EIGRP, and OSPF

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Module III

Access Control List

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

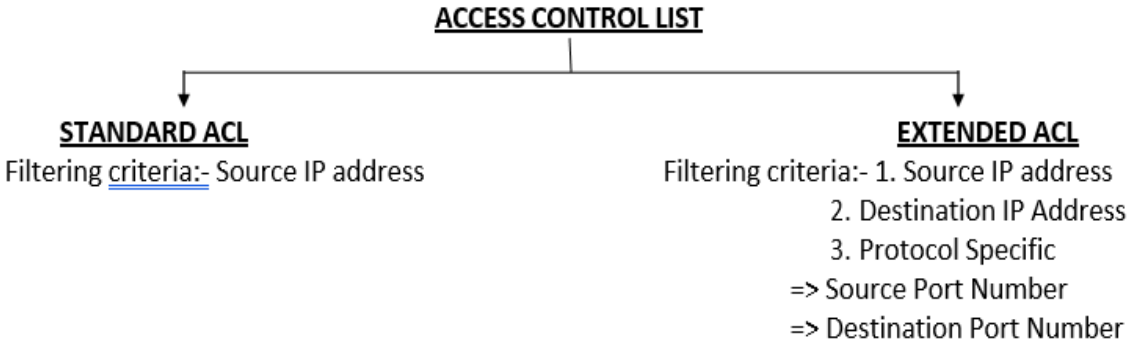
- The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
- The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
- There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

What are Inbound access lists?

When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.

What are Outbound access lists?

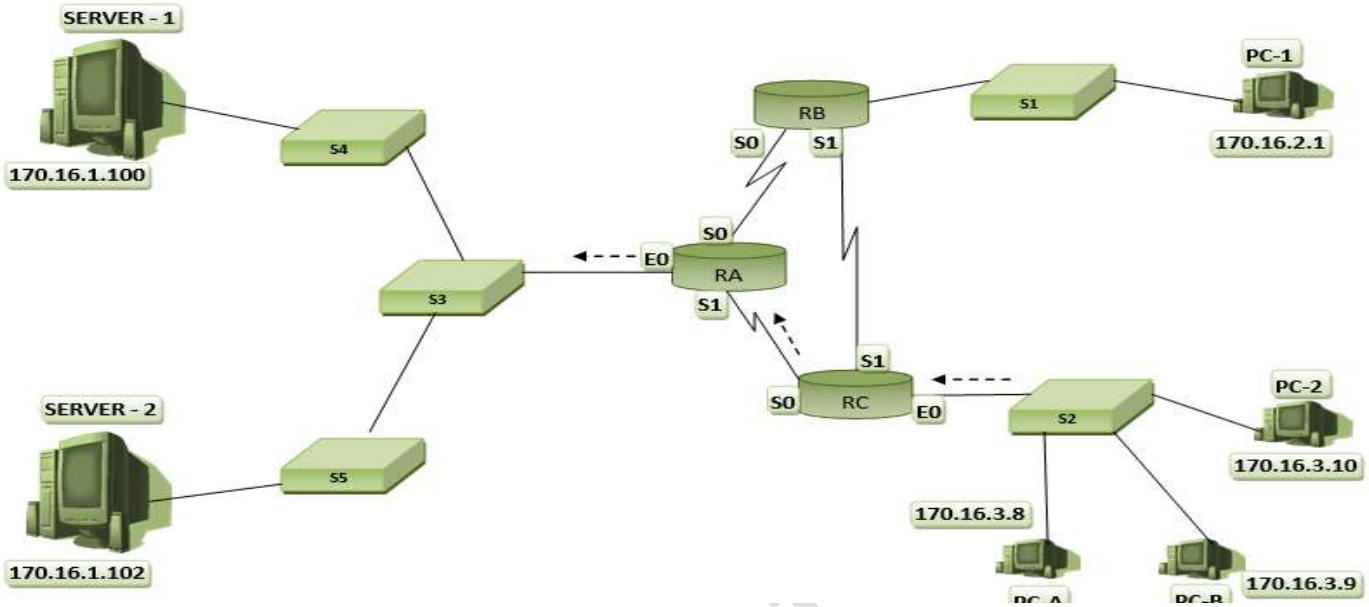
When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.



- ACL is created in Global Config mode.
- ACL is applied in an interface of the router.
- In case of Standard ACL, the ACL is applied as close as possible to the destination.

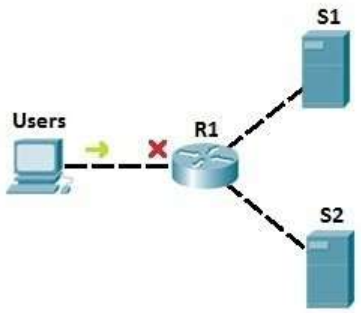
Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Location logic where ACL logic can be applied in the network as Standard ACL



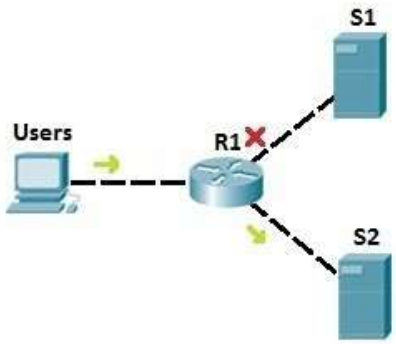
- In the above scenario we have three lans
- 170.16.1.0 (SERVER 1 & 2)
- 170.16.2.0 (PC-1)
- 172.16.3.0 (PC-2, PC-A, PC-B)
- RA, RB & RC have redundant connection.
- Now the scenario is such that PC-2 will not be able to access SERVER-1.
    - Next it is required to know or understand that at which interface of which router ACLshould be configured. You have three routers in your choice.
- The best interface to implement ACL is at RC's – E0.
- The traffic direction will be inbound.
- As in RC's – E0 ACL is implemented for IP 170.16.3.10 (i.e. PC-2) as deny permission, soPC-2 will also not able to communicate with Server-2 and PC-1 but it will able to communicate with PC-A & PC-B.
- So the next best interface to implementation ACL is at RA's, E0.
- But still PC-2 will not be able to communicate SERVER-1 as well as SERVER-2.

Extended Access Control Lists – with extended access lists, you can be more precise in your network traffic filtering. You can evaluate the source and destination IP addresses, type of layer 3 protocol, source and destination port, etc. Extended access lists are more complex to configure and consume more CPU time than standard access lists, but they allow a much more granular level of control.



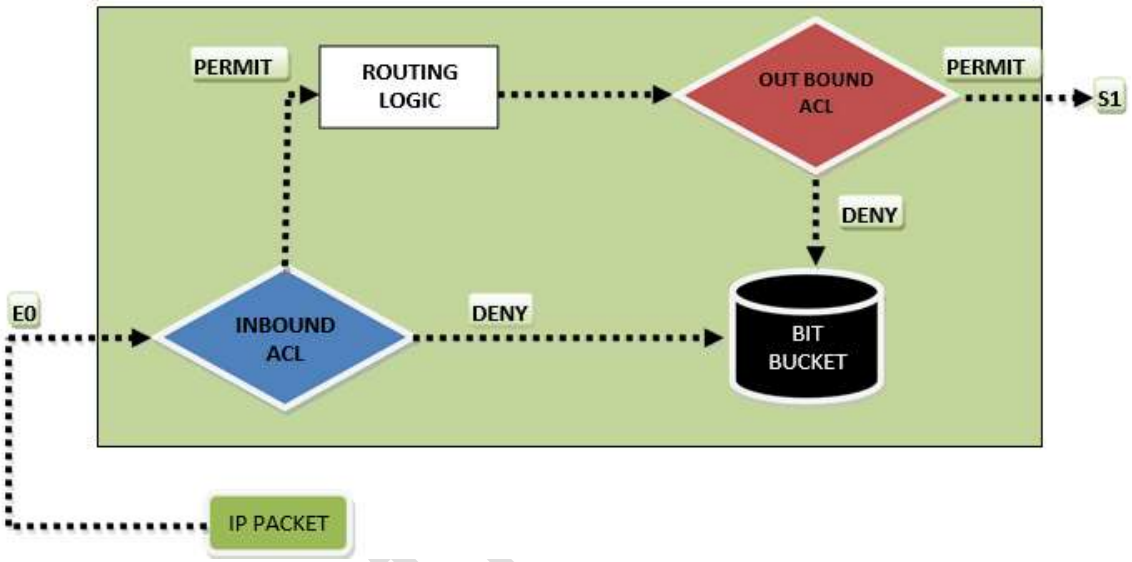
To demonstrate the usefulness of extended ACLs, we will use the following example:

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



In the example network above, we have used the standard access list to prevent all users from accessing server S1. But, with that configuration, we also deny access to S2! To be more specific, we can use extended access lists. Let's say that we need to prevent users from accessing server S1. We could place an extended access list on R1 to prevent users only from accessing S1 (we would use an access list to filter the IP traffic according to the destination IP address). That way, no other traffic is forbidden, and users can still access the other server, S2:

A block diagram, how ACL is performed



Explanation:

- IP Packets are filtered as they enter an interface before the routing table.
- Packet can filter before they exit an interface, after the routing decision.
- Deny is term used in Cisco IOS software to imply that the packet is not allowed toforward.
- Permit is the term used in the Cisco IOS software to imply that the packet is allowed toforward.
- The filtering is configured in the access list.
- At the end of every access list the default setting is "deny all traffic" statement. Therefore, if a packet does not match any of your access list statement, it is blocked.

Range for Standard ACL :– 1 – 99 & 1300 – 1999
Range for Extended ACL :-- 100 – 199 & 2000 - 2699

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Also, there are two categories of access-list:

Numbered access-list – These are the access list that cannot be deleted specifically once created i.e. if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.

Named access list – In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access list, unlike numbered access list. Like numbered access lists, these can be used with both standards and extended access lists.

Advantages of ACL –

- Improve network performance.
- Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of the network.

Difference Between Standard and Extended ACL

Standard	Extended
Filters Based on Source.	Filters Based on Source and destination.
Permit or deny entire TCP/IP protocol suite.	Specifies a specific IP protocol and port number.
Range is 1 – 99 and 1300 - 1999.	Range is 100 – 199 and 2000 - 2699.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Suggestive Questions

Multiple-choice Questions

1. What is the primary purpose of an Access Control List (ACL) in networking?
   a) To encrypt data
   b) To manage IP address assignment
   c) To filter network traffic
   d) To perform network address translation
2. What are the two main types of ACLs in networking?
   a) Standard and Extended
   b) Public and Private
   c) Static and Dynamic
   d) Local and Remote
3. Standard ACLs filter traffic based on which criteria?
   a) Source IP address only
   b) Source and destination IP address
   c) Source IP address and port number
   d) Destination IP address only
4. Extended ACLs can filter traffic based on which criteria?
   a) Source and destination IP address, protocol type, and port numbers
   b) Source IP address only
   c) MAC address only
   d) VLAN ID
5. In Cisco IOS, which number range is used for standard ACLs?
   a) 1-99
   b) 100-199
   c) 200-299
   d) 300-399
6. In Cisco IOS, which number range is used for extended ACLs?
   a) 1-99
   b) 100-199
   c) 200-299
   d) 300-399
7. Which command is used to apply an ACL to an interface in Cisco IOS?
   a) ip access-group
   b) access-list apply
   c) ip access-list
   d) set access-list
8. What does the wildcard mask 0.0.0.255 represent?
   a) Match any IP address
   b) Match the first three octets exactly, any value in the last octet
   c) Match any value in the first three octets, exact match in the last octet
   d) Match all bits exactly
9. Which of the following is a correct statement about an implicit deny in ACLs?
   a) It allows all traffic by default
   b) It denies all traffic that is not explicitly permitted
   c) It is a command that must be configured
   d) It only applies to extended ACLs
10. What is the correct command to create a standard ACL in Cisco IOS?
   a) access-list 10 permit 192.168.1.0 0.0.0.255
   b) access-group 10 permit 192.168.1.0 0.0.0.255
   c) ip access-list 10 permit 192.168.1.0 0.0.0.255
   d) permit ip access-list 10 192.168.1.0 0.0.0.255
11. In an extended ACL, which protocol keyword is used to filter HTTP traffic?
   a) icmp
   b) tcp
   c) udp
   d) http
12. Which of the following ACLs will block all traffic from the IP address 192.168.1.100?
   a) access-list 1 deny 192.168.1.100 0.0.0.0
   b) access-list 1 deny 192.168.1.100 255.255.255.255
   c) access-list 1 deny 192.168.1.100 0.0.0.255
   d) access-list 1 deny 192.168.1.100 0.0.0.255
13. Where should a standard ACL be placed to effectively filter traffic?
   a) As close to the destination as possible
   b) As close to the source as possible
   c) On the core router
   d) On the firewall
14. Where should an extended ACL be placed to effectively filter traffic?
   a) As close to the destination as possible
   b) As close to the source as possible
   c) On the core router

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

d) On the firewall

15. Which command would you use to view all ACLs configured on a Cisco router?
a) show ip access-lists
b) show access-lists
c) show running-config access-lists
d) show config access-lists

16. What does the "permit" keyword in an ACL do?
a) Blocks traffic
b) Allows traffic
c) Redirects traffic
d) Logs traffic

17. What does the "deny" keyword in an ACL do?
a) Allows traffic
b) Blocks traffic
c) Redirects traffic
d) Logs traffic

18. Which command applies an ACL to outbound traffic on an interface?
a) ip access-group 10 out
b) access-list apply 10 out
c) access-list 10 out
d) ip access-list out 10

19. What is a named ACL in Cisco IOS?
a) An ACL that uses a name instead of a number for identification
b) An ACL that can only be applied to specific interfaces
c) An ACL with enhanced security features
d) An ACL that can only filter traffic based on port numbers

20. Which command would you use to delete an ACL in Cisco IOS?
a) no access-list 10
b) delete access-list 10
c) remove access-list 10
d) clear access-list 10

Answer:

Sl. No.	Right Answer
1.	c) To filter network traffic
2.	a) Standard and Extended
3.	a) Source IP address only
4.	a) Source and destination IP address, protocol type, and port numbers
5.	a) 1-99
6.	b) 100-199
7.	a) ip access-group
8.	b) Match the first three octets exactly, any value in the last octet
9.	b) It denies all traffic that is not explicitly permitted
10.	a) access-list 10 permit 192.168.1.0 0.0.0.255
11.	b) tcp
12.	a) access-list 1 deny 192.168.1.100 0.0.0.0
13.	a) As close to the destination as possible
14.	b) As close to the source as possible
15.	b) show access-lists
16.	b) Allows traffic
17.	b) Blocks traffic
18.	a) ip access-group 10 out
19.	a) An ACL that uses a name instead of a number for identification
20.	a) no access-list 10

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Short Type Questions

1. What is the primary purpose of an Access Control List (ACL) in a network?
2. What are the two main types of ACLs in Cisco IOS?
3. How does a standard ACL filter traffic?
4. How does an extended ACL filter traffic?
5. What is the range of numbers used for standard ACLs in Cisco IOS?
6. What is the range of numbers used for extended ACLs in Cisco IOS?
7. Explain the purpose of a wildcard mask in an ACL.
8. What does the implicit deny statement in an ACL do?
9. How would you apply an ACL to an interface to filter inbound traffic in Cisco IOS?
10. Where should you place a standard ACL to effectively filter traffic?
11. Where should you place an extended ACL to effectively filter traffic?
12. What is a named ACL in Cisco IOS?
13. How can you view all ACLs configured on a Cisco router?
14. Describe the difference between the "permit" and "deny" keywords in an ACL.
15. How can you remove an ACL from a Cisco router configuration?

Long Type Questions

1. Define what an Access Control List (ACL) is in the context of computer networking and security.
2. Explain the difference between a standard ACL and an extended ACL.
3. What are the typical components of an ACL entry?
4. How does an ACL determine whether to permit or deny traffic?
5. Describe the order of operations when multiple ACLs are applied to a network interface or router interface.
6. What is the wildcard mask used for in ACLs, and how is it different from a subnet mask?
7. Discuss the advantages and disadvantages of using ACLs for network security.
8. How can ACLs be used to mitigate Denial of Service (DoS) attacks?
9. Explain the concept of implicit deny in the context of ACLs.
10. Provide an example scenario where you would use a standard ACL versus an extended ACL

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Module IV
Layer 2 Switching

What Is switching Technology?

Switching technology refers to the techniques and devices used to manage the flow of data across a network. It involves directing data packets between devices within a network or between different networks. Switches are key networking devices that play a crucial role in this process by connecting multiple devices, such as computers, printers, and servers, within a local area network (LAN) and directing data traffic efficiently.

What is Layer 2 Switching?

Layer 2 switching (or **Data Link layer switching**) is the process of using devices' MAC addresses to decide where to forward frames. Switches and bridges are used for Layer 2 switching. They break up one large collision domain into multiple smaller ones.

In a typical LAN, all hosts are connected to one central device. In the past, the device was usually a hub. But hubs had many disadvantages, such as not being aware of traffic that passes through them, creating one large collision domain, etc. To overcome some of the problems with hubs, bridges were created. They were better than hubs because they created multiple collision domains, but they had limited number of ports. Finally, switches were created and are still widely used today. Switches have more ports than bridges, can inspect incoming traffic and make forwarding decisions accordingly. Also. each port on a switch is a separate collision domain, so no packet collisions should occur.

What is Basic operation of switch?

Learning:

When a switch is powered on and starts receiving Ethernet frames, it begins to populate its MAC address table, also known as the Content Addressable Memory (CAM) table.

- **Source MAC Address**: The switch examines the source MAC address of each incoming frame and records it in the MAC address table, along with the port number through which the frame was received.
- **Learning Process**: If the source MAC address is not already in the MAC address table, the switch adds it. If it is already there, the switch updates the table to reflect the latest port through which the MAC address was seen.

2. **Forwarding/Filtering**:

Once the switch has learned the MAC addresses, it uses this information to decide how to handle incoming frames.

- **Destination MAC Address**: The switch looks up the destination MAC address of the incoming frame in its MAC address table.
- **Forwarding**: If the destination MAC address is found in the table, the switch forwards the frame out of the port associated with that MAC address.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **Filtering**: If the destination MAC address is on the same port as the source, the switch filters (discards) the frame to avoid unnecessary traffic.

3. **Flooding**:

When a switch receives a frame with a destination MAC address that is not in its MAC address table, it floods the frame.

- **Broadcast**: The switch sends the frame out of all ports except the one it was received on. This ensures that the frame reaches its intended destination, even if the switch does not know which port to use.
- **Unknown Unicast**: Similar to a broadcast, the switch floods unknown unicast frames to all ports to find the destination.

4. **Loop Prevention**:

Switches use protocols like the Spanning Tree Protocol (STP) to prevent network loops.

- **STP Operation**: STP detects potential loops in the network topology and blocks certain switch ports to prevent broadcast storms and other issues caused by loops.
- **Port States**: STP ports can be in different states such as Blocking, Listening, Learning, and Forwarding to ensure a loop-free environment.

Benefits of Using Switches

- **Improved Performance**: Switches provide dedicated bandwidth to each connected device, reducing collisions and improving overall network performance.
- **Enhanced Security**: VLANs and other security features on managed switches can segment and secure network traffic.
- **Scalability**: Networks can be easily expanded by adding more switches without significant reconfiguration.

Switching Methodology

Store-and-Forward Switching:
Store-and-forward switching is a method of switching data packets by the switching device that receives the data frame and then checks for errors before forwarding the packets. It supports the efficient transmission of non-corrupted frames. It is generally used in telecommunication networks.

In store-and-forward switching, the switching device waits to receive the entire frame and then stores the frame in the buffer memory. Then the frame is checked for errors by using CRC(Cyclic Redundancy Check) if the error is found then the packet is discarded else it is forwarded to the next device.

Cut-through Switching:
Cut-through switching is a method of switching data packets by the switching device that forwards the packets as soon as the destination address is available without waiting for the rest of the data to arrive. It supports low latency and high-speed transmission and requires less storage space. It is used in fibre channel transmission, SCSI traffic transmission, etc.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

In cut–through switching, data transmission starts as soon as the destination address field arrives at the switching device. Then the device performs a lookup operation to check whether the destination address is valid or not. If the address is found valid and the link to the destination is available then the switching device starts to transmit the packets to the destination without waiting for the rest of the frame to arrive.

Fragment-Free Switching

Fragment-free (runt less switching) switching is an advanced form of cut-through switching. The switches operating in cut-through switching read only up to the destination MAC address field in the Ethernet frame before making a switching decision. The switches operating in fragment-free switching read at least 64 bytes of the Ethernet frame before switching it to avoid forwarding Ethernet runt frames (Ethernet frames smaller than 64 bytes).

Difference between Cut-through Switching and Store-and-Forward Switching:

Store-and-Forward Switching	Cut-through Switching
The switching device waits to receive the entire frame before forwarding the data packet.	The switching device forwards the data packet as soon as the destination address is received and doesn't wait for the entire frame to be received.
It supports error checking and collided/ bad frames are discarded before forwarding the packets.	There is no error-checking technique.
It checks for errors based on FCS bits of the data frame.	It relies on higher-level protocols to detect the error.
Frames are stored in the buffer memory of the switching device.	Frames are not stored in the switching device.
It is not further classified into different types.	Cut through switching is further classified as Rapid frame forwarding and Fragment free.
It has a high latency rate as the device waits for the entire frame to be received before sending the packets to the destination.	It has a low latency rate as the device does not wait for the entire frame to be received before sending the packets to the destination.

Limitation of layer-2 switching

Scalability

- **Limited Broadcast Domains**: Layer-2 switches operate within a single broadcast domain, which can lead to excessive broadcast traffic as the network grows. This limits the size of the network.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **VLAN Limitations**: Although VLANs can segment broadcast domains, the number of VLANs is limited, and managing a large number of VLANs can become complex.

Security

- **Lack of Isolation**: Devices within the same VLAN can communicate directly, which can pose security risks. VLAN hopping attacks can also exploit vulnerabilities in VLAN configurations.
- **Limited Access Control**: Layer-2 switches do not natively support advanced access control mechanisms, making it difficult to enforce security policies strictly.

Loop Prevention

- **Dependence on Spanning Tree Protocol (STP)**: Layer-2 networks rely on STP to prevent loops, which can result in suboptimal path selection and slower convergence times.
- **STP Limitations**: Changes in the network topology can cause STP recalculations, leading to temporary network disruptions.

Multicast Handling

- **Inefficient Multicast Traffic Management**: Layer-2 switches typically flood multicast traffic to all ports, which can lead to inefficiencies and excessive bandwidth consumption.

Inter-VLAN Communication

- **Lack of Native Routing**: Layer-2 switches cannot route traffic between VLANs. Inter-VLAN routing requires a Layer-3 device (router or Layer-3 switch), adding complexity and potential bottlenecks.

Bridging vs LAN switch

Switch	Bridge
It is a device which is responsible for channelling the data that is coming into the various input ports to a particular output port which will further take the data to the desired destination.	It is basically a device which is responsible for dividing a single network into various network segments.
A switch can have a lot of ports.	A bridge can have 2 or 4 ports only.
The switch performs the packet forwarding by using hardwares such as ASICS hence, it is hardware based.	The bridge performs the packet forwarding by using softwares so it is software based.
The switching method in case of a switch can thus be store, forward, fragment free or cut through.	The switching method in case of a bridge is store and forward.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Switch	Bridge
The task of error checking is performed by a switch.	A bridge cannot perform the error checking.
A switch has buffers.	A bridge may not have a buffer.

Address learning methodology of a switch

Frame Reception:

- When a switch receives an Ethernet frame on one of its ports, it extracts the frame's source and destination MAC addresses.

Source MAC Address Learning:

- **Check the Source MAC Address**: The switch examines the source MAC address of the received frame.
- **Update the MAC Address Table**:
  - **If the source MAC address is not in the table**: The switch adds a new entry to the MAC address table. This entry includes the source MAC address and the port number through which the frame was received.
    - **Example**: If a frame with a source MAC address AA:BB:CC:DD:EE:FF is received on port 1, the switch creates an entry: AA:BB:CC:DD:EE:FF -> port 1.
  - **If the source MAC address is already in the table but associated with a different port**: The switch updates the entry to reflect the current port number.
  - **If the source MAC address is already in the table and associated with the same port**: No changes are made to the table.

Destination MAC Address Forwarding:

- **Look Up the Destination MAC Address**: The switch searches its MAC address table for the destination MAC address of the frame.
- **Forwarding Decision**:
  - **Known Destination MAC Address**: If the destination MAC address is found in the table, the switch forwards the frame out of the port associated with that MAC address.
  - **Unknown Destination MAC Address**: If the destination MAC address is not found in the table, the switch floods the frame out of all ports except the one it was received on. This ensures that the frame reaches its intended destination even if the switch doesn't know where that destination is.

Flooding for Unknown Addresses:

- When the switch encounters a destination MAC address that is not in its MAC address table, it floods the frame to all ports (except the port on which the frame was received). This helps to discover the correct port for future frames.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Handling Broadcast and Multicast Frames:

- **Broadcast Frames**: Frames addressed to the broadcast MAC address (FF:FF:FF:FF:FF

) are forwarded to all ports.

- **Multicast Frames**: Frames addressed to a multicast MAC address are also typically flooded to all ports unless specific multicast group management is implemented.

Aging Process:

- **Aging Timer**: The switch maintains an aging timer for each entry in the MAC address table. If an entry is not updated within a certain period (typically 300 seconds), it is removed from the table. This prevents the table from becoming cluttered with outdated addresses and ensures efficient memory use.

Difference between Network Switch and Router

Network Switch	Router
Network Switch works on Layer 2 of the OSI Model.	The router is primarily a device of Layer 3 of the OSI Model.
The resource is shared among multiple devices with the help of a single LAN using a network switch.	Data is moved between two or more computers with the help of a router.
Network switches uses data frames.	Routers use data packets.
Switches only work in a Wired network connection.	Router works with both wired and wifi networks.
Switches use MAC Addresses for transferring data to the proper destination.	Routers use IP Addresses for the same work.

What is CAM table of a switch
The CAM (Content Addressable Memory) table, also known as the MAC address table, is a critical component of a network switch. It stores the mapping of MAC addresses to the switch ports, enabling the switch to efficiently forward Ethernet frames to the correct destination.

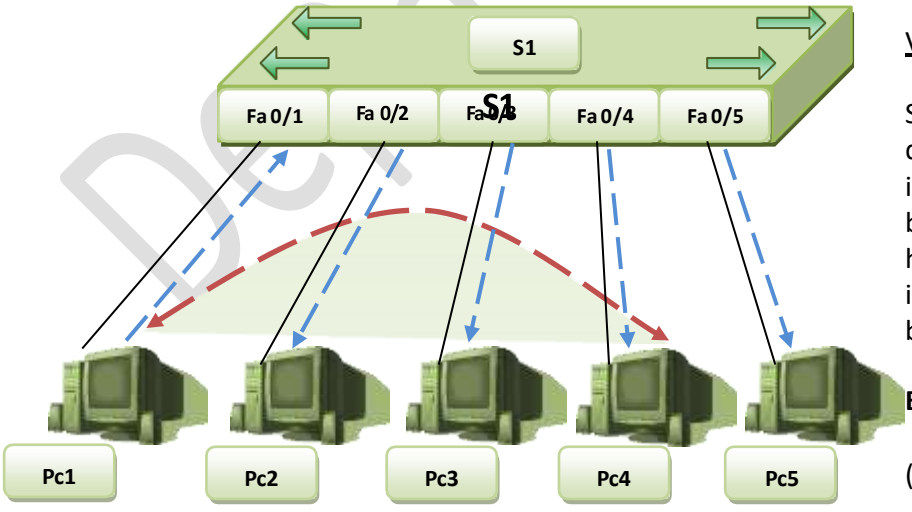
Features of access layer switch; distribution layer switch and core layer Switch

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **Access** – controls user and workgroup access to the resources on the network. This layer usually incorporates Layer 2 switches and access points that provide connectivity between workstations and servers. You can manage access control and policy, create separate collision domains, and implement port security at this layer.
- **Distribution** – serves as the communication point between the access layer and the core. Its primary functions are to provide routing, filtering, and WAN access and to determine how packets can access the core. This layer determines the fastest way that network service requests are accessed –for example, how a file request is forwarded to a server – and, if necessary, forwards the request to the core layer. This layer usually consists of routers and multilayer switches.
- **Core** – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high-speed devices, like high end routers and switches with redundant links.

Difference between manage and unmanage switch

	Managed Switches	Unmanaged Switches
Features	Dynamic ARP Inspection, IPv4 DHCP snooping, QoS, SNMP, VLAN, CLI, IP routing, port mirroring, redundancy, etc	Dynamic ARP Inspection, IPv4 DHCP snooping, QoS, SNMP, VLAN, CLI, IP routing, port mirroring, redundancy, etc
Performance	Switch can be configured Control over Access Control over LAN traffic—Priority SNMP—Allows for remote troubleshooting of the network	Plug and play with limited configuration like default QoS settings
Security	Very good. Provide protection of the data plane, control plane and management plane	Not very good. No security other than accessories such as lockable port cover
Costs	Expensive	Less expensive
Application Places	Data center, large size enterprise networks	Small size business network, home, lab, conference rooms, etc.



VLAN

Switch by default have a single broadcast domain. As the number of devices increases in the domain the size of the broadcast domain also increases. Now to have a better efficiency in the network, it is necessary to limit the size of the broadcast domain.

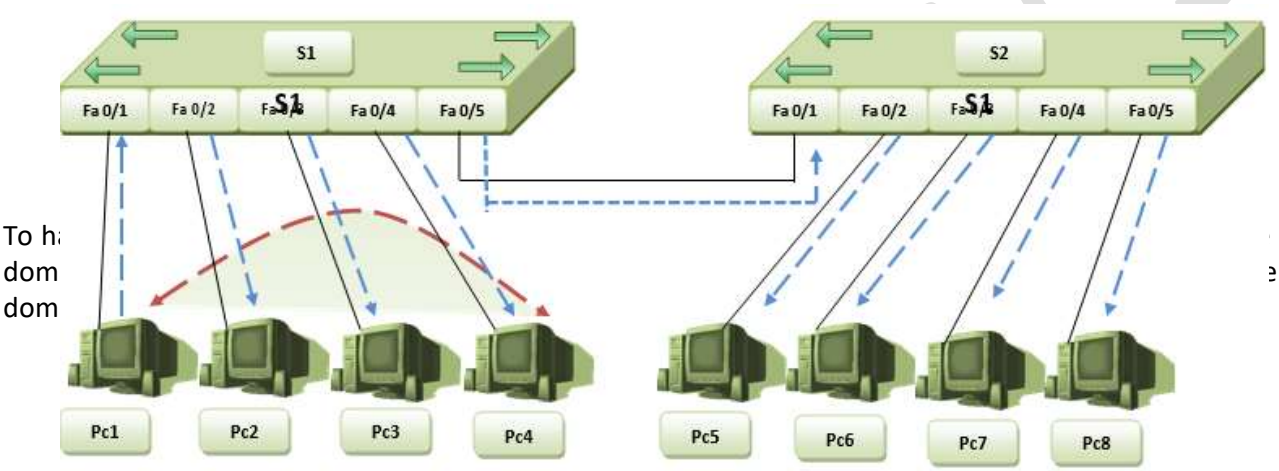
Explanation

- 5PCs are connected with a Switch (S1).

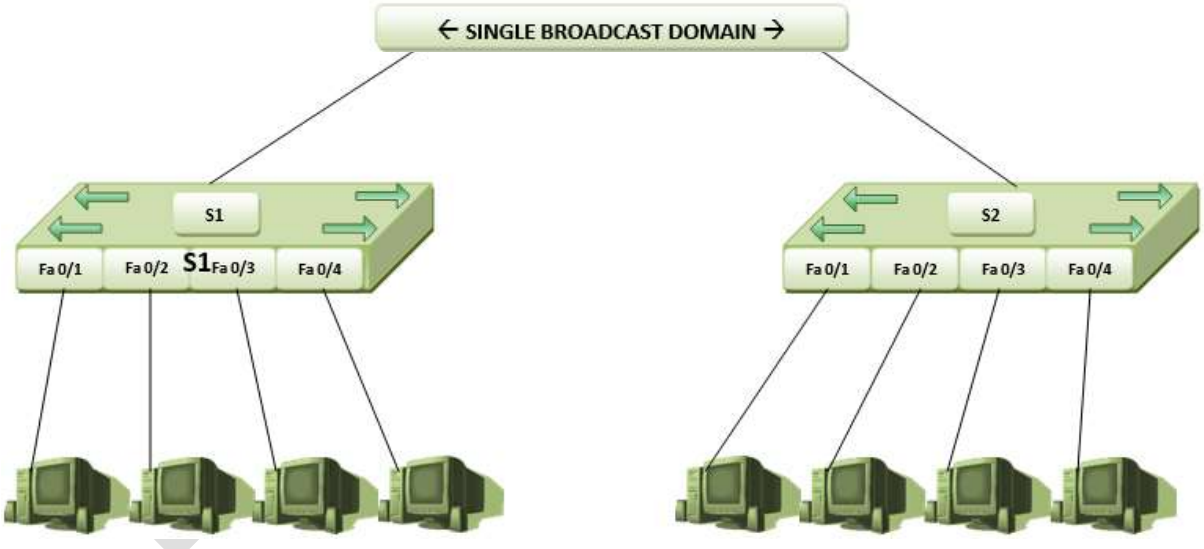
Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- PC1 is connected with the interface Fa0/1 of S1.
- PC 1 wants to communicate with PC 4 (reff: the doted red arrow).
- PC1 started generating PDU frames. The frames received by the Switch S1 in interface Fa0/1. (reff: the doted blue arrow)
- The Switch S1 broadcast the frames through rest of the active interface.
- So, as the Switch belongs to a single broadcast domain, the Switch S1 broadcast the incoming frames generated by PC1 through the entire active interface. All the PC connected with S1 sense the traffic generated by PC1, though the traffic was not for them. This deteriorates the efficiency of the total network.

  As the number of network devices increases in the network, the size of the broadcast domain also increases.

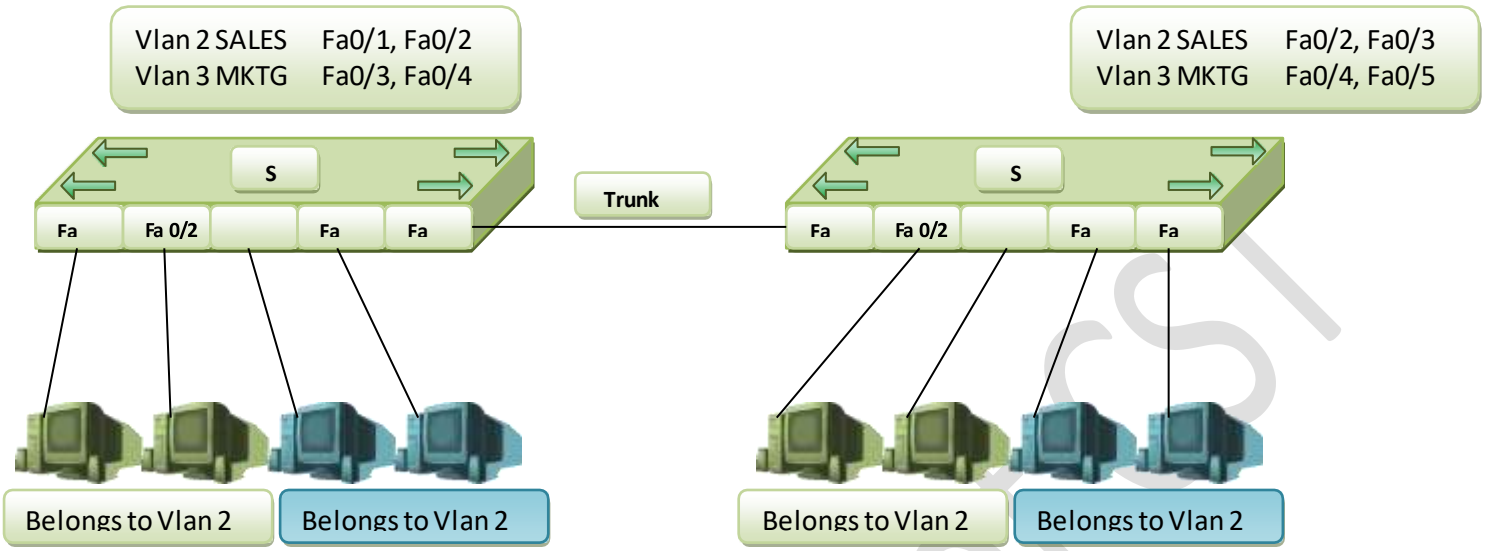


To h broadcast
dom broadcast
dom



Vlan: A Vlan is a group of devices in the same broadcast domain or subnet. Vlans provides logical separation of subnets to have better efficiency with network traffic between different groups of users. Vlancontains isolated broadcast domains, where router is required to move traffic between different Vlans.

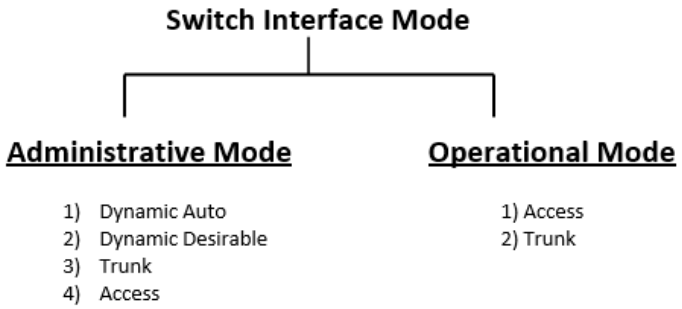
Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.



- Vlan information is not taged with the PDU frames generated by the PC.
- The information of Vlan is present in Switch. By default all the interface of the Switch belongs to Vlan1.
- By default, interface Fa0/5 of S1 and interface Fa0/1 of S2, belongs to Vlan1. As this link is used to carry multiple Vlan information, it will act as a special link(i.e. trunk link). We need to activate trunk protocol on the trunk port of the Switch.
- The ethernet interfaces through which PCs are connected, should be configured to work in access mode. In access mode, when a Switch receives any frame it does not make any changes in the frame.
- In trunk mode when a Switch receives any frame, the Switch adds some information in the frames before forwarding those frames through the trunk link.
- For tagging Vlan information in the trunk port, two protocols are used.
- ISL (Inter Switch Link)
- 802 . 1 Q

Advantages of Vlan

- Vlan enable us to create more flexible design that group user users by department, that work together, instead fo any physical location.
- To segment a single broadcast domain into smaller multiple broadcast domain to reduce the overhead traffic caused by each host in the Vlan.
- Vlan reduces the workload of the STP.
- Vlan enforce better security by keeping a group of hosts in a separate vlan.



Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Access: It prevent the use of trunking, the port will always acts access (non trunk) port. The link normally can be associated with a single Vlan.

Trunk: The port will always use trunking. It modify the original frame to carry Vlan information.

Dynamic Desirable: Exchange, negotiate messages and also responds to the negotiation to dynamically choose whether to start using trunking.

Dynamic Auto: Passively waits to receive trunk messages and will respond to negotiate whether to use trunk.

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) – VTP is CISCO proprietary protocol used to maintain consistency throughout the network or the user can say that synchronizing the VLAN information in the same VTP domain. VTP allows you to add, delete and rename VLANs which is then propagated to other switches in the VTP domain. VTP advertisements can be sent over 802.1Q, and ISL trunks.
Requirements – There are some requirements for VTP to communicate VLAN information between switches. These are:

1. The VTP version must be same on the switches user wants to configure
2. VTP domain name must be same on the switches
3. One of the switches must be a server
4. Authentication should match if applied

VTP modes – There are 3 modes:

- **Server –** The switches are set to this mode by default. This mode allows you to create, add and delete VLANs. The changes you want to make should be done in this mode. Any changes that are done on this mode (on a particular switch) will be advertised to all the switches that are in the same VTP domain. In this mode, the configuration is saved in NVRAM.

- **Client –** In this mode, the switches receive the updates and can also forward the updates to other switches (which are in the same VTP domain). The updates received here are not saved in NVRAM so all the configuration will be deleted if the switch is reset or reloaded i.e. the switches will only learn and pass the VTP summary advertisements to the other switches.

- **Transparent –** This mode only forwards the VTP summary advertisements through trunk link. The transparent mode switches can make their own local database which keep secret from other switches. The whole purpose of transparent mode is to forward the VTP summary advertisements but not to take part in the VLAN assignments.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

FUNCTION	SERVER	TRANSPARENT	CLIENT
Only sends VTP messages through the trunk port	YES	YES	YES
Support CLI configuration of VLAN's	YES	YES	NO
Can use normal range VLAN's (1-1005)	YES	YES	YES
Can use extended range VLAN's (1006-4095)	NO	YES	NO
Synchronize (updates) its own config database when receive VTP message with a higher revision number	YES	NO	YES
Create and sends periodic VTP update in every 5 minuets	YES	NO	YES

Difference between IEEE802.1q and ISL

PARAMETER	ISL	DOT1Q
Abbreviation for	ISL (Inter Switch Link)	-
Standard	Cisco proprietary protocol	IEEE Standard
Vlans Supported	Supports up to 1000 Vlans	Supports 4096 Vlans
Encapsulation	Original frame is encapsulated and a new header is inserted during encapsulation process. A 26 byte header and a 4 byte FCS (frame check sequence) are inserted which makes it total of 30 Bytes of overhead.	802.1q encapsulation inserts a 4 byte tag into original frame and FCS (Frame Check Sequence) is re-calculated.
PVST	Supported	Not Supported
Supported on Cisco NX-OS	Not Supported	Supported

What is VTP pruning

pruning is a feature that is used in Cisco switches to reduce unnecessary traffic in VLAN (Virtual Local Area Network) trunks. When VTP pruning is enabled on a trunk, the switch will stop forwarding broadcast, multicast, and unknown unicast traffic to VLANs that do not have any active ports.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

This feature optimizes network bandwidth utilization by preventing unnecessary traffic from being sent across the network, which can help improve network performance. However, VTP pruning should only be used in situations where there are VLANs with no active ports, as enabling it on all trunks can cause connectivity issues if new ports are added to VLANs in the future.

What is STP?

The Spanning Tree Protocol (STP) is a network protocol designed to prevent loop formation in Ethernet networks. Developed by Dr. Radia Perlman, it is standardized as IEEE 802.1D. STP ensures that a network topology is loop-free by creating a spanning tree within a network of connected Ethernet switches and then disabling the links that are not part of the tree, thus preventing the possibility of broadcast storms and multiple frame copies.

Here are some key points about STP:

Purpose

- **Loop Prevention**: STP's primary purpose is to prevent network loops which can cause broadcast storms and multiple frame copies.
- **Redundancy**: It allows for redundant paths in the network to provide fault tolerance. If a primary path fails, STP can re-enable a backup path to maintain network connectivity.

How It Works

1. **Bridge Protocol Data Units (BPDUs)**: Switches exchange BPDUs to share information about their ports and link states. BPDUs are sent out regularly to detect network topology changes.
2. **Root Bridge Election**: The switches elect a root bridge (the central reference point in the spanning tree) based on the lowest bridge ID, which is a combination of the switch's priority and MAC address.
3. **Path Cost Calculation**: Each switch calculates the cost to reach the root bridge. The path with the lowest cost becomes the preferred path.
4. **Designated Ports**: For each network segment, the switch with the lowest path cost to the root bridge is designated as the designated switch, and its port on that segment is called the designated port.
5. **Non-Designated Ports**: Ports that do not serve as the shortest path to the root bridge are put into a blocking state, preventing loops by disabling the redundant paths.

Port States

1. **Blocking**: The port does not participate in frame forwarding to prevent loops.
2. **Listening**: The port prepares to participate in frame forwarding, listening to BPDUs.
3. **Learning**: The port begins to populate the MAC address table but does not forward frames yet.
4. **Forwarding**: The port forwards frames and participates in the network.
5. **Disabled**: The port is administratively shut down.

Types of Spanning Tree Protocol (STP)

1. 802.1D – This is also known as CST (Common Spanning Tree). It is a spanning tree standard developed by IEEE which elects only one root bridge per whole topology. All the traffic flows over the same path (the best path to

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

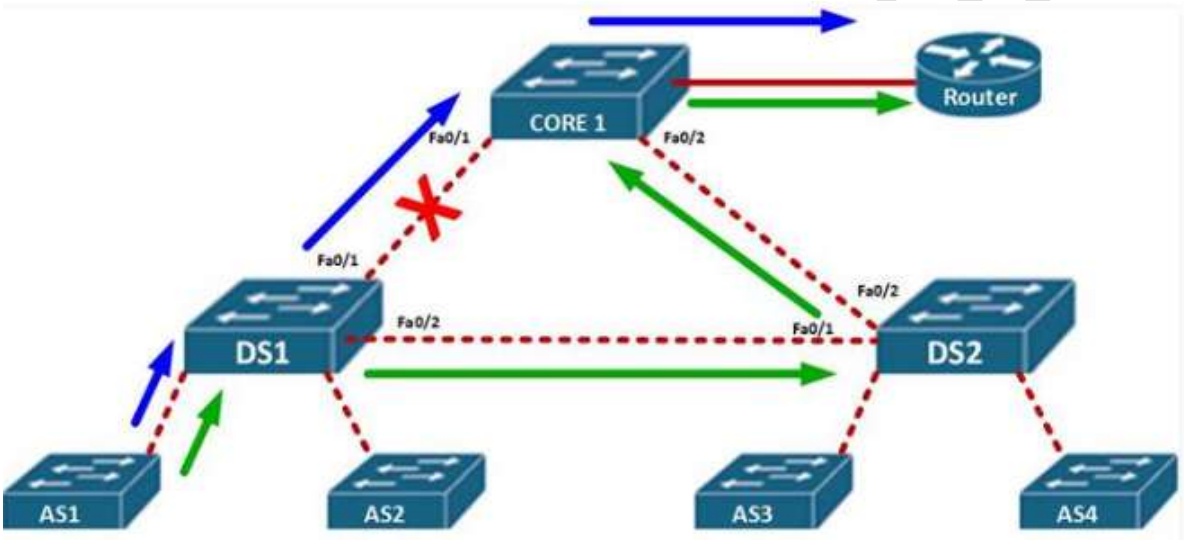
the root bridge) but this doesn't hold good always as there can be scenarios in which the optimised path to reach a VLAN is different than the path obtained on electing the root bridge. It is very slow as it takes 32 seconds to converge.

2. Per VLAN Spanning Tree + (PVST+) – It is a spanning tree standard developed by Cisco for its devices which finds the root bridge per VLAN. It is a Cisco default version of STP. It finds separate 802.1d spanning tree instance for each VLAN. It also provides backward comparability with 802.1d or CST. This is more optimized to the IEEE because it provides optimal path selection as separate instance of STP per VLAN is find. This is as slow as CST.

3. 802.1w – Rapid Spanning Tree Protocol (RSTP) – It is a spanning standard developed by IEEE which provides faster convergence than CST but holds the same idea of finding a single root bridge in the topology. The bridge resources needed in RSTP is higher than CST but less than PVST+ .

4. Rapid Per VLAN Spanning Tree + (RPVST+) –This Spanning Tree standard is developed by Cisco which provides faster convergence than PVST+ and finds separate instance of 802.1w per VLAN. It requires much more CPU and memory than other STP standards.

5. 802.1s (Multiple Spanning Tree) :-This standard is developed by IEEE in which grouping of VLANs is done and for each single group, RSTP is run. This is basically a Spanning Tree Protocol running over another Spanning Tree Protocol.



Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Suggestive Questions

Multiple-choice Questions

1. **Which IEEE standard defines VLANs?**
   A) 802.1D
   B) 802.1Q
   C) 802.1X
   D) 802.3
2. **What is the primary benefit of VLANs?**
   A) Increased broadcast domain
   B) Reduced network performance
   C) Enhanced network security
   D) Simplified network management
3. **Which type of VLAN is used for network management?**
   A) Data VLAN
   B) Default VLAN
   C) Native VLAN
   D) Management VLAN
4. **What is a common default VLAN ID for an untagged port on a switch?**
   A) VLAN 1
   B) VLAN 100
   C) VLAN 1000
   D) VLAN 4095
5. **Which command is used to assign a VLAN to a switch port on a Cisco switch?**
   A) switchport access vlan [vlan-id]
   B) vlan database [vlan-id]
   C) assign vlan [vlan-id]
   D) port access vlan [vlan-id]

VTP (VLAN Trunking Protocol)

6. **What is the primary purpose of VTP?**
   A) To manage VLAN configuration across multiple switches
   B) To provide inter-VLAN routing
   C) To create VLANs
   D) To assign IP addresses to VLANs
7. **Which VTP mode allows a switch to create, modify, and delete VLANs?**
   A) Client
   B) Server
   C) Transparent
   D) Host
8. **Which VTP mode does not synchronize VLAN information but forwards VTP advertisements?**
   A) Server
   B) Client
   C) Transparent
   D) Monitoring
9. **What is the default VTP mode on a Cisco switch?**
   A) Server
   B) Client
   C) Transparent
   D) Host
10. **Which command displays the VTP status of a switch?**
    A) show vtp status
    B) show vlan brief
    C) show running-config
    D) show switchport
11. **What is the main purpose of STP?**
    A) To increase network speed
    B) To prevent switching loops
    C) To manage VLANs
    D) To route IP packets
12. **Which protocol is the faster-converging version of STP?**
    A) RSTP
    B) PVST
    C) MSTP
    D) BPDU
13. **Which device becomes the root bridge in an STP topology?**
    A) The device with the highest MAC address
    B) The device with the lowest MAC address
    C) The device with the lowest bridge ID
    D) The device with the highest bridge ID
14. **What is the purpose of BPDU (Bridge Protocol Data Unit) frames?**
    A) To carry IP traffic
    B) To manage VLANs
    C) To exchange STP information
    D) To configure switch ports
15. **Which STP state does a port enter first after being enabled?**
    A) Blocking

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

B) Listening
C) Learning
D) Forwarding

16. **Which switching method checks the CRC (Cyclic Redundancy Check) before forwarding a frame?**
    A) Cut-through
    B) Store-and-forward
    C) Fragment-free
    D) Fast-forward
17. **What is the function of a MAC address table in a switch?**
    A) To store IP addresses
    B) To route packets between VLANs
    C) To map MAC addresses to switch ports
    D) To perform DNS lookups
18. **Which switch port mode is used to connect an end device to a VLAN?**
    A) Trunk mode
    B) Access mode
    C) Hybrid mode
    D) Dynamic mode
19. **Which command is used to display the MAC address table on a Cisco switch?**
    A) show mac-address-table
    B) show ip interface brief
    C) show interfaces
    D) show vlan brief
20. **What is the purpose of a trunk port on a switch?**
    A) To connect multiple VLANs on different switches
    B) To connect a single device to a VLAN
    C) To provide power to end devices
    D) To perform routing between VLANs
21. **Which IEEE standard defines Link Aggregation (LAG)?**
    A) 802.1D
    B) 802.1Q
    C) 802.3ad
    D) 802.1w
22. **Which feature allows for redundancy by having multiple switches acting as a single virtual switch?**
    A) STP
    B) VTP
    C) VLAN
    D) StackWise
23. **In which switching mode does the switch forward the packet as soon as the destination address is read?**
    A) Store-and-forward
    B) Cut-through
    C) Fragment-free
    D) Fast-forward
24. **What is the result of a broadcast storm in a switching network?**
    A) Increased network performance
    B) Network congestion and packet loss
    C) Efficient data delivery
    D) Improved security
25. **Which command on a Cisco switch enables an interface to automatically negotiate a trunk link?**
    A) switchport mode trunk
    B) switchport trunk encapsulation dot1q
    C) switchport mode dynamic desirable
    D) switchport access vlan

Short Type Questions

1. What is the purpose of a VLAN and how does it enhance network management?
2. Explain the role of a VLAN trunk link in a network.
3. Describe the function of the Native VLAN in a trunk port.
4. How does VLAN tagging work, and which IEEE standard defines it?
5. What is the difference between an access port and a trunk port on a switch?
6. What are the main differences between VTP Server, VTP Client, and VTP Transparent modes?
7. How does VTP pruning help reduce unnecessary traffic on trunk links?

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

8. What is a VTP domain and why is it important in VTP operations?
9. Describe the impact of VTP version mismatches in a network.
10. Explain the process of VTP advertisement and synchronization between switches.
11. What is the primary purpose of the Spanning Tree Protocol (STP) in a network?
12. How is the root bridge selected in an STP-enabled network?
13. What is the function of BPDU (Bridge Protocol Data Unit) in STP?
14. Explain the differences between traditional STP and Rapid Spanning Tree Protocol (RSTP).
15. What is the purpose of the Port-Fast feature in STP and when should it be used?

Long Type Questions

1. Explain the concept and purpose of VLAN tagging.
2. Describe the differences between static VLANs and dynamic VLANs.
3. What is the function of the Native VLAN in a trunk link?
4. How does Inter-VLAN routing work, and why is it necessary?
5. Discuss the security benefits of using VLANs in a network.

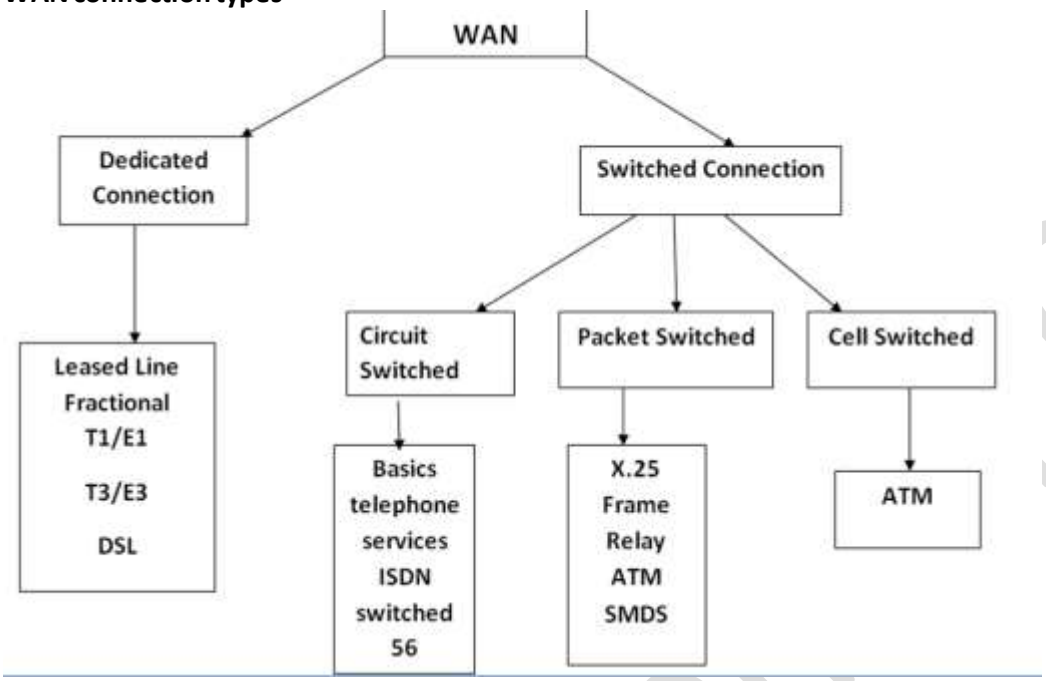
6. Explain the differences between VTP Server, VTP Client, and VTP Transparent modes.
7. How does VTP pruning improve network efficiency?
8. Describe the process of VTP synchronization between switches.
9. What is the significance of the VTP domain name in VTP operations?
10. Explain how VTP versions differ and why it's important to use a consistent version across a network.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Module V

Wide Area Networking and Authentication Protocols

WAN connection types



What is leased lines, circuit switching, packet switching

Leased Lines

Leased Lines are dedicated, private telecommunications circuits that provide continuous and fixed-bandwidth connectivity between two locations. These lines are leased from a telecommunications provider and are typically used for internet access, private networks, and point-to-point data transmission.

- **Features:**
  - **Dedicated Connection:** Exclusive use of the line, not shared with other users.
  - **High Reliability:** Consistent performance with minimal latency.
  - **Fixed Bandwidth:** Guaranteed bandwidth as specified in the service agreement.
  - **Security:** Higher security as it is a private connection.
- **Use Cases:**
  - Connecting two business locations.
  - Providing dedicated internet access.
  - Establishing private networks (WANs).

Circuit Switching

Circuit Switching is a method of communication where a dedicated communication path or circuit is established between two nodes for the duration of the session. This method is typically used in traditional telephone networks.

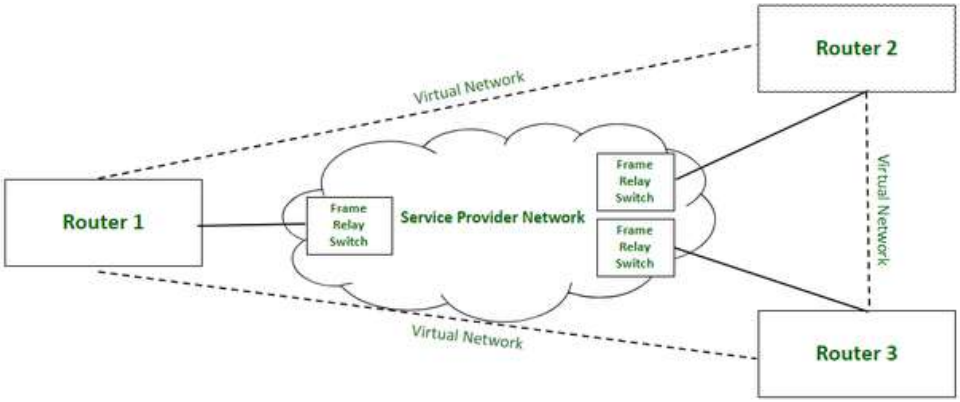
Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

- **Features:**
  - **Dedicated Path:** A specific path is reserved for the entire duration of the call.
  - **Fixed Bandwidth:** The bandwidth is reserved and constant throughout the session.
  - **Connection-Oriented:** Requires establishing and maintaining a connection before data transfer.
  - **High Reliability:** Consistent quality of service due to dedicated path.
- **Use Cases:**
  - Traditional voice telephone calls.
  - Some private network configurations.
- **Advantages:**
  - Predictable and consistent performance.
  - Suitable for real-time voice communications.
- **Disadvantages:**
  - Inefficient use of resources as the dedicated path remains idle if no data is being transmitted.

Packet Switching

Packet Switching is a communication method where data is broken down into smaller packets that are transmitted over a shared network and reassembled at the destination. This is the method used by the internet and most modern data networks.

- **Features:**
  - **Shared Network:** Multiple communications share the same network infrastructure.
  - **Dynamic Routing:** Packets can take different paths to reach the destination.
  - **Connectionless:** Each packet is routed independently without a dedicated path.
  - **Efficient Use of Resources:** Network resources are used only when data is being transmitted.
- **Use Cases:**
  - Internet data transmission (web browsing, email, file transfer).
  - Modern telecommunications (VoIP, video conferencing).
- **Advantages:**
  - Efficient utilization of network resources.
  - Scalable and flexible.
- **Disadvantages:**
  - Potential for variable latency and packet loss.
  - May require error handling and retransmission mechanisms.



What is Frame Relay

Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation. Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.

How frame Relay Works

Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network. It supports communication with multiple LANs over the shared physical links or private lines.

Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks. Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch. The access link is the private physical link used for communication with other LAN networks over WAN. The frame relay switch is responsible for terminating the access link and providing frame relay services.

For data transmission, LAN's router (or other border device linked with access link) sends the data packets over the access link. The packet sent by LAN is examined by a frame relay switch to get the Data Link Connection Identifier (DLCI) which indicates the destination of the packet. Frame relay switch already has the information about addresses of the LANs connected to the network hence it identifies the destination LAN by looking at DLCI of the data packet. DLCI basically identifies the virtual circuit (i.e. logical path between nodes that doesn't really exist) between source and destination network. It configures and transmits the packet to frame relay switch of destination LAN which in turn transfers the data packet to destination LAN by sending it over its respective access link. Hence, in this way, a LAN is connected with multiple other LANs by sharing a single physical link for data transmission.

Types of Frame Relay

- **Permanent Virtual Circuit (PVC) –**
  These are the permanent connections between frame relay nodes that exist for long durations. They are always available for communication even if they are not in use. These connections are static and do not change with time.
- **Switched Virtual Circuit (SVC) –**
  These are the temporary connections between frame relay nodes that exist for the duration for which nodes are communicating with each other and are closed/ discarded after the communication. These connections are dynamically established as per the requirements.

SDN (Software-Defined Networking)

SDN is a network architecture that separates the network's control plane from the data plane, allowing for centralized and programmable network management to improve flexibility and efficiency.

HDLC (High-Level Data Link Control)

HDLC is a bit-oriented synchronous data link layer protocol used for reliable data transmission between network points, incorporating mechanisms for error detection and flow control.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

PPP (Point-to-Point Protocol)

PPP is a data link layer protocol that facilitates direct communication between two network nodes. It supports authentication, encryption, and compression, making it versatile for various network connections, such as dial-up and VPNs.

ATM (Asynchronous Transfer Mode)

ATM is a high-speed networking technology that transfers data in fixed-size cells. It is designed to handle a variety of traffic types, including voice, video, and data, providing efficient and low-latency communication.

PAP (Password Authentication Protocol)

PAP is a simple authentication protocol that sends the user's password in plain text from the client to the server, where it is validated. It is used in situations where security is not a primary concern.

CHAP (Challenge Handshake Authentication Protocol)

CHAP is an authentication protocol that provides a more secure method than PAP by using a three-way handshake. It periodically re-authenticates the client to protect against replay attacks and ensure ongoing security during a session.

Single Homed EBGP

The single homed design means you have a single connection to a single ISP. With this design, you don't need BGP since there is only one exit path in your network. You might as well just use a static default route that points to the ISP.
The advantage of a single-homed link is that it's cost effective, the disadvantage is that you don't have any redundancy. Your link is a single point of failure but so is using a single ISP.

What is a VPN?
A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. A Virtual Private Network is a way to extend a private network using a public network such as the Internet. The name only suggests that it is a "Virtual Private Network", i.e. user can be part of a local network sitting at a remote location. It makes use of tunnelling protocols to establish a secure connection.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Types of VPN

There are several types of VPN and these are vary from specific requirement in computer network. Some of the VPN are as follows:

1. Remote Access VPN
2. Site to Site VPN
3. Cloud VPN
4. Mobile VPN
5. SSL VPN

VPN Protocols

- **OpenVPN:** A cryptographic protocol that priorities security is called OpenVPN. OpenVPN is compatible protocol that provides a variety of setup choices.
- **Point-To-Point Tunneling Protocol (PPTP):** PPTP is not utilized because there are many other secure choices with higher and more advanced encryption that protect data.
- **Wire Guard:** Wire guard is a good choice that indicates capability in terms of performance.
- **Secure Socket Tunneling Protocol (SSTP):** SSTP is developed for Windows users by Microsoft. It is not widely used due to the lack of connectivity.
- **Layer 2 Tunneling Protocol (L2TP)** It connects a user to the VPN server but lacks encryption hence it is frequently used with IPSec to offer connection, encryption, and security simultaneously.

What are the advantages of VPN

Enhanced Security

VPNs encrypt internet traffic, protecting data from being intercepted by hackers and other malicious entities, particularly on unsecured networks like public Wi-Fi.

Privacy Protection

By masking the user's IP address, VPNs help maintain online anonymity, preventing websites, advertisers, and ISPs from tracking browsing activities.

Bypassing Geo-Restrictions

VPNs allow users to access content that may be restricted based on geographic location by routing the connection through servers in different countries.

Remote Access

VPNs enable secure access to a private network from a remote location, making them essential for businesses with remote or traveling employees.

Data Integrity

VPNs help ensure that data sent over the internet remains unchanged and arrives intact at its destination by protecting it against tampering.

Cost Savings

Using VPNs can reduce costs associated with leased lines and long-distance telephone charges, as they allow secure, low-cost connections over the public internet.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

Suggestive Questions
Multiple-choice Questions

1. What is a leased line?
A. A shared network connection
B. A dedicated, private telecommunications circuit
C. A type of packet-switched network
D. An internet-based virtual network

2. Which of the following is a characteristic of circuit switching?
A. Data is broken into packets
B. A dedicated path is established for the duration of the communication
C. Data is transmitted in fixed-size cells
D. Multiple virtual circuits share the same physical link

3. In packet switching, how is data transmitted?
A. In fixed-size cells
B. Over a dedicated circuit
C. As a continuous stream
D. In small packets that are routed independently

4. Frame Relay operates at which layer of the OSI model?
A. Network layer
B. Data link layer
C. Transport layer
D. Physical layer

5. What does ISDN stand for?
A. Internet Service Digital Network
B. Integrated Services Digital Network
C. Internal Services Data Network
D. Interconnected Services Data Network

6. HDLC is a protocol used at which layer of the OSI model?
A. Network layer
B. Transport layer
C. Data link layer
D. Application layer

7. Which protocol provides a simple method for point-to-point communication and supports authentication, encryption, and compression?
A. HDLC
B. Frame Relay
C. PPP
D. ATM

8. ATM transfers data in:
A. Packets
B. Frames
C. Segments
D. Fixed-size cells

9. Which of the following protocols sends passwords in plain text?
A. PAP
B. CHAP
C. EAP
D. RADIUS

10. CHAP improves security over PAP by using:
A. Plain text transmission
B. Two-way handshake
C. Three-way handshake and periodic re-authentication
D. Single-way authentication

11. Single-homed EBGP refers to:
A. A BGP setup with multiple ISPs
B. A BGP setup with a single ISP
C. A BGP setup within an Autonomous System
D. A multi-homed internal BGP setup

12. Which type of VPN uses the public internet to create a secure and encrypted connection between two points?
A. MPLS VPN
B. Remote Access VPN
C. Frame Relay VPN
D. ISDN VPN

13. Which VPN protocol is known for its robust security and ability to encapsulate PPP traffic?
A. L2TP

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

B. PPTP
C. SSL
D. IPSec

14. What is the primary advantage of using a leased line for WAN connectivity?
A. Low cost
B. High flexibility
C. Dedicated and consistent bandwidth
D. Easy to set up

15. Frame Relay is most similar to which other WAN technology in terms of function?
A. ISDN
B. ATM
C. HDLC
D. Ethernet

Answer:

Sl. No.	Right Answer
1.	B. A dedicated, private telecommunications circuit
2.	B. A dedicated path is established for the duration of the communication
3.	D. In small packets that are routed independently
4.	B. Data link layer
5.	B. Integrated Services Digital Network
6.	C. Data link layer
7.	C. PPP
8.	D. Fixed-size cells
9.	A. PAP
10.	C. Three-way handshake and periodic re-authentication
11.	B. A BGP setup with a single ISP
12.	B. Remote Access VPN
13.	D. IPSec
14.	C. Dedicated and consistent bandwidth
15.	B. ATM

Shote Types questions

1. What is the primary function of a VPN?
2. How does a leased line differ from a typical broadband connection?
3. In packet switching, how are data packets transmitted across the network?
4. What is the key characteristic of circuit switching that distinguishes it from packet switching?
5. What layer of the OSI model does HDLC operate on?
6. What does PPPoE stand for and what is its primary use?
7. How does CHAP improve security over PAP in the authentication process?
8. What is one advantage of using a leased line for business communications?
9. Describe a key advantage of packet switching in modern networks.
10. What are the main benefits of using HDLC for data link layer communication?

Long Types questions

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.

1.Describe the key differences between leased lines and packet-switched networks in terms of performance and use cases.

2. How does packet switching enhance network efficiency and scalability compared to circuit switching? Provide examples.

3. What are the main benefits of using Frame Relay for WAN connectivity, and how does it compare to other WAN technologies like ATM and MPLS?

4. Discuss the advantages of ISDN in providing high-speed and reliable communication services. What are the main types of ISDN services available?

5. Explain the error detection and correction mechanisms used by HDLC. How do these mechanisms contribute to data integrity?

6. Describe how PPP encapsulates network layer protocols for transmission over point-to-point links. What are the key features that make PPP versatile?

7. Compare the use of fixed-size cells in ATM with variable-size packets in traditional packet-switched networks. What are the benefits and drawbacks of each approach?

8. How does CHAP provide a more secure authentication method compared to PAP? Describe the process of CHAP authentication.

9. Explain the concept of autonomous systems in BGP. How does single-homed EBGP differ from multi-homed EBGP, and what are the implications for network redundancy?

10. What are the primary security features of VPNs, and how do they protect data transmitted over the internet?

11. Describe the role of committed information rate (CIR) in Frame Relay networks. How does it impact network performance and cost?

12. Explain how ISDN channels (B channels and D channels) are utilized for different types of data transmission. Provide examples of their applications.

13. Discuss the significance of the three-way handshake in CHAP authentication. How does it enhance security compared to PAP?

14. Describe the differences between remote access VPNs and site-to-site VPNs in terms of their architecture and typical use cases.

15. How do VPN protocols like IPSec and SSL differ in terms of their operation and security features? Provide examples of when each protocol might be used.

Anirban Lahiri
Assistant Professor
Department of Cyber Science & Technology
BRAINWARE UNIVERSITY.