Exploring the OSI Model and TCP/IP

The need for networking models

- A **network** is defined as having two or more computing devices interconnected, using a set of communication protocols (rules) that allow them to share a resource between themselves.
- A **resource** can be anything, such as a file on a centralized server, a multiplayer game on an online server, and even a network-connected printer.
- **Networks** are all around us and we use them every day to communicate with each other, share information, and even deliver an online service.
- The largest network in the world is the **internet.**
- it is not owned by a single person, organization, or government, but various organizations globally have the responsibility of ensuring its sustainability, availability, security, and scalability.
- The following are important organizations that play key roles on the internet:

Internet Society (ISOC), Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Assigned Numbers Authority (IANA), Internet Corporation for Assigned Names and Numbers (ICANN).

- In the 1970s, the International Organization for Standardization (ISO) developed the OSI networking model for computer networks.
- The OSI model was designed to be a common standard for using networking protocols (rules) to allow intercommunication between devices that are connected over a network.
- However, the OSI model didn't have the traction needed to be implemented as a networking protocol suite within systems.
- A **network protocol** is simply the rules and guidelines that are used by a device to allow communication or the exchange of messages from one device to another.
- There are many network protocols, each of which has a different purpose and characteristic.

Exploring the OSI model

- The OSI model was originally developed to be an open networking model for computer networks to allow different devices to use a set of mutual protocols (rules) to allow communication between each other over a network.
- It is described as a reference model because it's not technically implemented on any networked devices.
- The OSI model contains a total of seven layers that describe how communication occurs between one device and another over a network.
- Each layer of the OSI model has a unique role and responsibility to ensure a message from a sender contains all the necessary details to be successfully delivered to the intended destination.

The following diagram shows the seven layers of the OSI model:

Layer	Name	Protocol Data Unit (PDU)
7	Application	Data
6	Presentation	
5	Session	
4	Transport	Segment
3	Network	Packet
2	Data Link	Frame
1	Physical	Bits

Fig. - OSI model

- At each layer of the OSI model, when a message exits at a specific layer, the message is commonly referred to as a **Protocol Data Unit** (**PDU**).
- A PDU is described as a single unit of data/information that can be transmitted from one host to another over a network.
- As the PDU is created at the Application layer of the OSI model of the host, it is referred to as **data**, which is the raw message.
- As the PDU travels down the OSI model, each of the lower layers is responsible for attaching additional information within a header onto the PDU to ensure proper addressing details are inserted to deliver the message. This process is commonly referred to as **encapsulation**.
- When a host on the network receives the message, the PDU travels upward on the OSI model, where each layer **de-encapsulates** the message, removing the header information until the raw message is delivered to the Application layer on the recipient device.

The following diagram shows an overview of the process of sending and receiving a message between two devices using the OSI model:

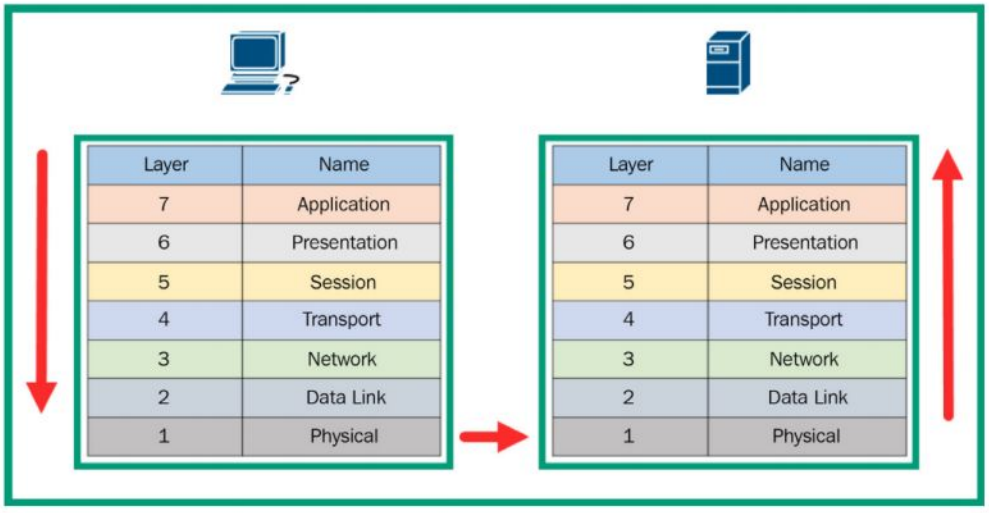


Fig. – Sending and receiving messages

- The upper layers of the OSI model, such as the Application, Presentation, and Session layers, are designed to provide support for the application's functionality.

- The lower layers of the OSI model, such as the Transport, Network, Data Link, and Physical layers, focus on inserting the addressing information needed to deliver the datagram to the destination.
- So, lower layers as having the responsibility of ensuring end-to-end connectivity between hosts over a network.

Application layer

- It is the closest to the end user, such as yourself.
- It provides an interface so that you can run the applications of a host such as a computer or even a smartphone to communicate with the underlying network protocols of the OSI model.
- The following screenshot shows a standard web browser using HTTPS as the Application layer protocol to communicate with the CompTIA web server:

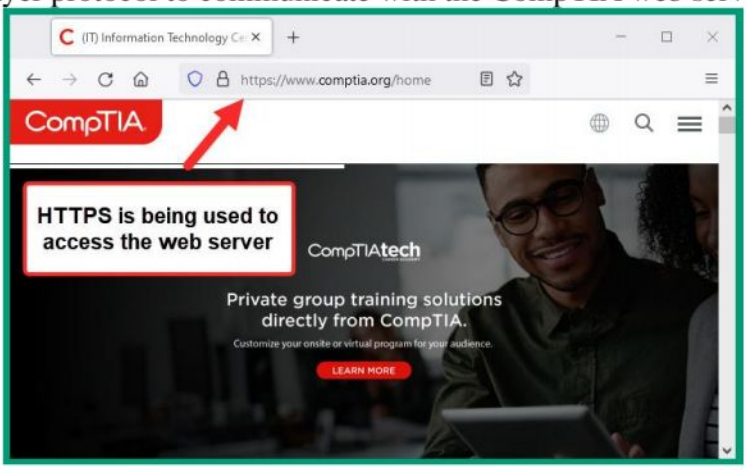


Fig. – Observing an Application layer protocol

- Installing a web browser on your computer allows your operating system to interact with the **Hypertext Transfer Protocol** (**HTTP**) and **Hypertext Transfer Protocol Secure** (**HTTPS**) protocols.
- Another example is using an email application such as Microsoft Outlook to interact/interface with the **Simple Mail Transfer Protocol** (**SMTP**), an application layer protocol that is responsible for sending email messages over a network.
- Each protocol uses its own set of rules and structure for creating a PDU.
- At the Application layer, the PDU contains only the raw data created by the application layer protocol and does not have any addressing information needed to be delivered to the intended recipient.
- At the Application layer, the PDU is known as **Data**.

Presentation layer

- It transforms system-dependent data (for example, ASCII or JPEG) into an independent format.
- This allows the Presentation layer on the receiving system to transform the data back into the system-dependent format (ASCII or JPEG) that the Application layer requires.

The following are the main responsibilities of the Presentation layer:

- Data formatting (encoding)
- Data compression
- Data encryption
- Data decryption

Session layer

The following are the core functions of the Session layer:

- Create/establish a session
- Maintain the session
- Terminate a session

Transport layer

- The Transport layer assigns a service port number to the PDU so that the receiving system will know how the Presentation layer should interpret and format the data.
- Then, the receiving system can read the data in the Application layer.

The following diagram shows a high-level visual representation of the client using HTTP to communicate with the same application layer protocol on the web server:

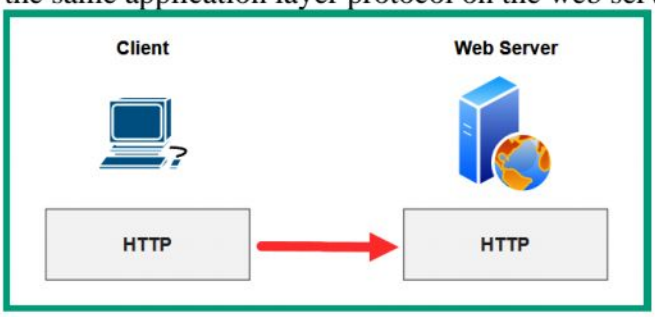


Fig. - Application layer protocol communication

- Within an operating system that supports TCP/IP, there are 65,535 service port numbers.
- The following diagram shows how these ports are categorized:

Port Range	Category
0 - 1,023	Well-known ports
1,024 - 49,151	Registered ports
49,152 - 65,535	Private/Dynamic ports

Well known ports- These are very common on a network. Some of these common application layer protocols are HTTP, HTTPS, and SMTP.

Registered ports-Their range belongs to users and organizations who have officially registered a service port number to operate on a custom build application or software.

Private/dynamic ports- Their range belongs to service ports that are temporarily used during communication, such as using a randomly generated service port on the sender's device as the source port.

- These service ports are logical ports within an operating system.
- Each service port number is logically mapped to an application layer protocol.

The following is a brief list of common application layer protocols and their corresponding service ports numbers:

Application Layer Protocol	Service Port Number
File Transfer Protocol (FTP)	20 & 21
Secure Shell (SSH)	22
Secure Copy (SCP)	22
SSH File Transfer Protocol (SFTP)	22
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name System (DNS)	53
Hypertext Transfer Protocol (HTTP)	80
Hypertext Transfer Protocol Secure (HTTPS)	443

Fig. – Common application layer protocols

- Transport layer encapsulates (inserts) a layer 4 header onto the datagram that contains both the source and destination service port numbers.
- Once the layer 4 header is added to the datagram from the Application layer, the PDU is referred to as a **segment**.

The following diagram shows a segment at the Transport layer containing a source and destination service port number with the data received from the application layer protocol:

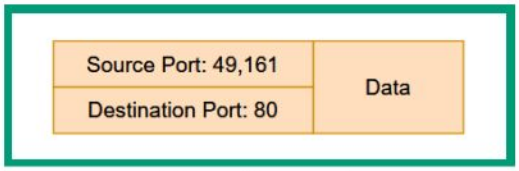


Fig. – Segment

- The source port number informs the recipient about the sender's return address.
- The destination service port number informs the destination device about which application layer protocol to deliver the message to.

The following diagram shows a visual representation of the client sending a message to the web server that is running HTTP as the application layer protocol on service port 80:

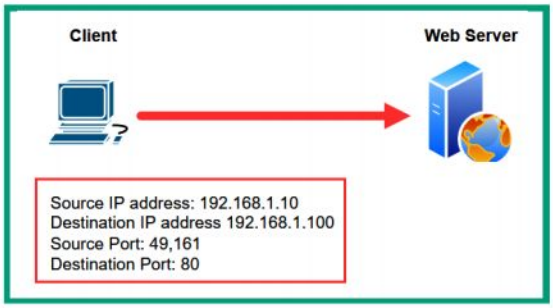


Fig. – HTTP Request message

The following diagram shows the addressing information used by the web server to respond to the client on the network:

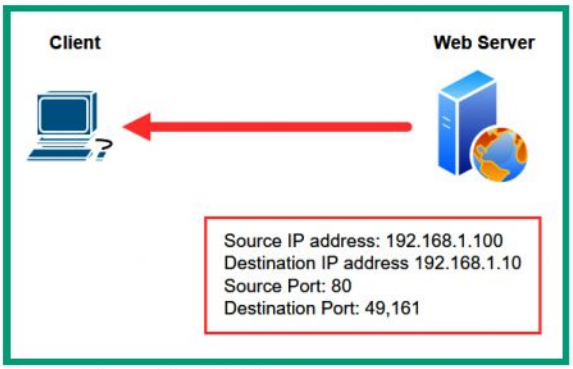


Fig. – HTTP Response message

- The Transport layer contains two protocols that assist with transporting and delivering datagrams over the network.
- These Transport layer protocols are as follows:
  - **Transmission Control Protocol (TCP)**
  - **User Datagram Protocol (UDP)**

Transmission Control Protocol

- It is a connection-oriented protocol that establishes a logical connection between the source and destination devices before exchanging messages over a network.
- This connection referred to as the **TCP three-way handshake**.

The following diagram shows a high-level overview of the TCP three-way handshake between two devices:

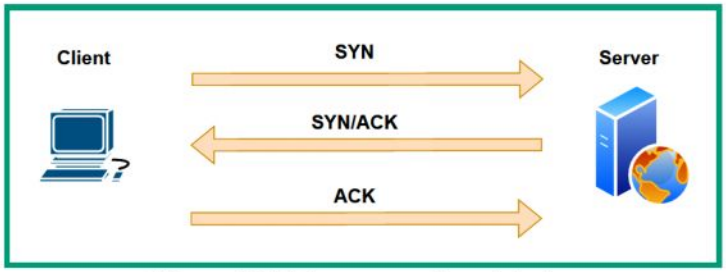


Fig. – TCP three-way handshake

The following is a breakdown of this process:

1. The client device wants to communicate with the server, so the client device sends a **synchronization (SYN)** message to the server. The SYN message is used to initiate a connection with the server. Within the SYN message, a randomly generated sequence number is created.

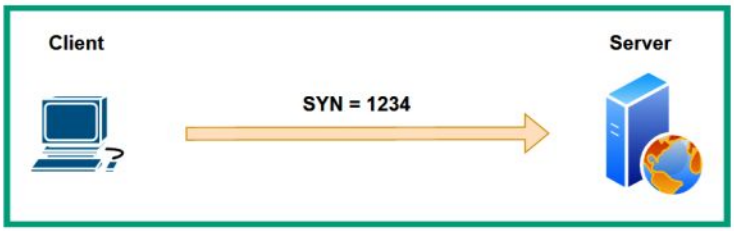


Fig. – SYN sequence number

2. The server receives the SYN message from the client and responds with an **acknowledgment (ACK)** message. Within the ACK message is an ACK sequence number; which is the client's sequence number + 1. The server also includes a SYN

message within its response, containing a randomly generated sequence number to inform the client it also wants to initiate a connection; this message is known as a **SYN/ACK**, as shown in the following diagram:

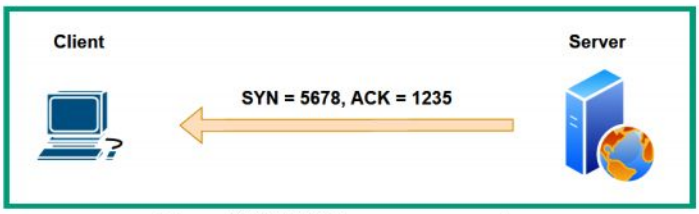


Fig. – SYN/ACK sequence number

3. The client receives the SYN/ACK message from the server and responds with an ACK message. The ACK message from the client contains an increment value of the SYN message received from the server, as shown in the following diagram:

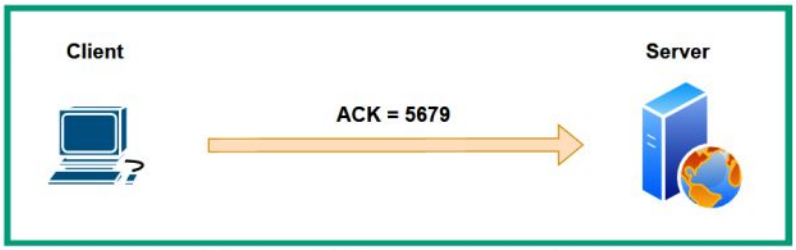


Fig. – ACK sequence number

TCP three-way handshake with sequence numbers

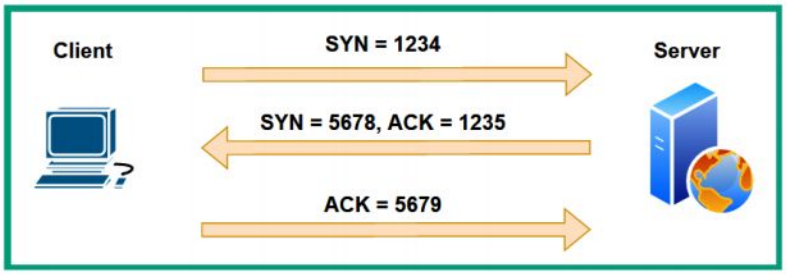


Fig. – TCP three-way handshake with sequence numbers

Note

The sequence numbers used by TCP allow a destination device to easily reassemble incoming messages if they are received out-of-order compared to the order they were sent onto the network.

- If the sender does not receive an ACK packet from the intended destination host, after a while, the sender will attempt to retransmit the same message, repeating the process to ensure the message is delivered successfully.
- This is another benefit of using TCP when communicating over a network as it provides guaranteed delivery of messages and retransmits messages when needed.
- When both hosts are no longer transmitting data between themselves over the network, TCP will attempt to terminate the connection using a four-step process, as shown here:

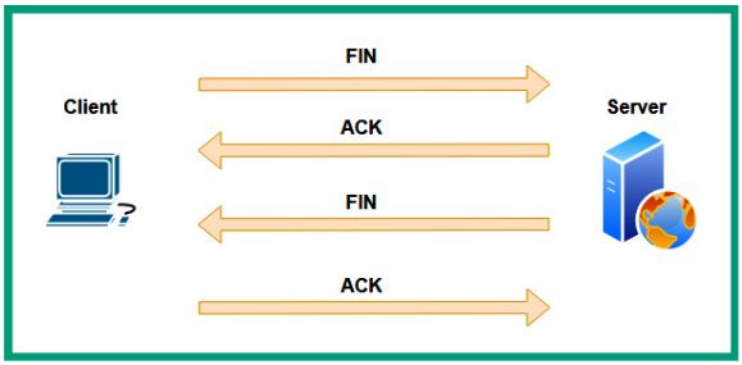


Fig. – TCP terminating a connection

Advantages of TCP

- Establishes a session such as the TCP three-way handshake before exchanging data.
- Provides reliability in delivering data over a network.
- Delivers data using the same order of delivery from the sender to the receiver.
- Uses flow control by creating a window size that has been mutually agreed upon between the source and destination hosts.

Disadvantages of TCP

- There is more overhead on a network as for each message delivered to a destination device; the receiver responds with an ACK message.
- TCP wait for acknowledgment messages from the receiver before sending more data. This creates a delay in the delivery of the messages.

User Datagram Protocol

- It is a connectionless protocol that does not establish a logical connection between the source and destination devices.
- It does not provide any guarantee of delivery of messages over a network.
- It does not provide any acknowledgments when messages are delivered, so the sender does not know whether the messages were delivered or not.
- This makes UDP an unreliable Transport layer protocol within the networking model.
- As the sender device does not use sequence numbers, there is no way to determine how to properly reassemble the messages in their correct order.

Advantages

- Since it does not wait for any acknowledgment from the destination host, it is faster. It is beneficial for application layer protocols that are time-sensitive such as Voice over IP (VoIP) and Video over IP solutions that are used in real time.
- Low overhead on the network since no acknowledgment messages are returning to the sender.

Disadvantages

- It does not provide reliability in delivering data over a network.
- It may not deliver the message to the receiver in the same order as send by the sender.
- It does not use flow control.

Network layer

- The Network layer of the OSI model is responsible for ensuring the logical addressing information is inserted into the datagram.

- Each device requires a unique Internet Protocol version4 (IPv4) or Internet Protocol version 6 (IPv6) address that allows them to communicate with devices on their local and remote networks.
- The Network layer encapsulates a layer 3 header onto the datagram by inserting the source and destination IP addresses.
- Once the PDU from the Transport layer is encapsulated with the layer 3 header, it is referred to as a **Packet**.

The following diagram shows a high-level overview of a client sending a message to a server:

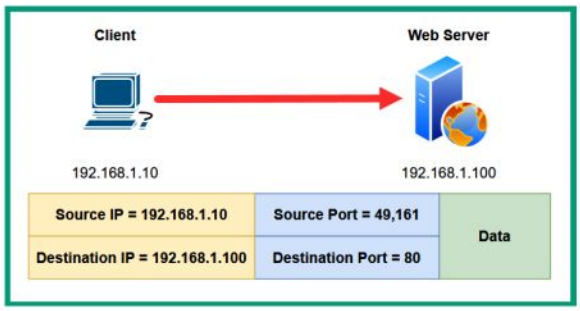


Fig. – Packet header

- Additionally, the Network layer is responsible for the routing services that occur on the network.
- Devices such as routers are considered to be layer 3 devices that can interconnect different networks and forward packets between networking using the information within the layer 3 headers of the packet, such as the destination IP address.
- Each time a router on the network receives a packet, it checks the destination IP address within the layer 3 headers of the packet and the routing table on the router to determine whether a valid route to the destination exists.
- Therefore, a sender must insert the accurate layer 3 addressing (IP addresses) onto the layer 3 header of the packet to ensure networking devices such as routers can forward the packet to the destination.

Note

The source IPv4 address on a packet may change due to the **Network Address Translation** (**NAT**) operating on a router.

Internet Protocol (IP)

- It is a connectionless layer 3 protocols that does not establish any logical connection or session between the sender and receiver of the message.
- If packets are lost or corrupted during the transmission process, the messages are not retransmitted.
- It is unreliable and does not provide any guarantee that the data will be delivered to the destination host.
- However, it provides low overhead on the network as a connectionless protocol.
- The IP indicates to the Transport layer whether or not to use the TCP, UDP, or other protocols in its header information.

Data Link layer

- It is responsible for moving the datagrams from the upper layers onto the actual network.
- It handles flow control.
- It encapsulates a layer 2 header and trailer onto the packet, creating a **frame**.
- It handles error detection to identify whether any incoming frames from the physical network are corrupted and discard them.

Within the Data Link layer, two sublayers assist with ensuring frames are encapsulated, de-encapsulated.

- **Logical Link Control** (**LLC**)
- **Media Access Control** (**MAC**)

Logical Link Control

- It is responsible for ensuring there is communication between the networking applications, software, and protocols of the upper layers of the OSI model and the local host's device hardware such as the Network Interface Card (NIC).
- It inserts information within theframe, which indicates the network layer protocol that is being used within the frame.
- Additionally, it allows many layer 3 protocols such as IPv4 and IPv6 to use the same network media and device.

Media Access Control

- It is responsible for performing the data encapsulation process and controlling access to the network device such as the NIC and networkmedia (wired, wireless, or fiber optic).
- It is also responsible for inserting the layer 2 physical addressing information onto the layer 2 header of the frame.
- This layer 2 physical address is commonly referred to as a **MAC address** or a **Burned-In Address** (**BIA**).
- It handles error detection by inserting a trailer **Frame Check Sequence** (**FCS**) into the frame.

  The following diagram shows a high-level overview of the layer 2 header and trailer of a frame:

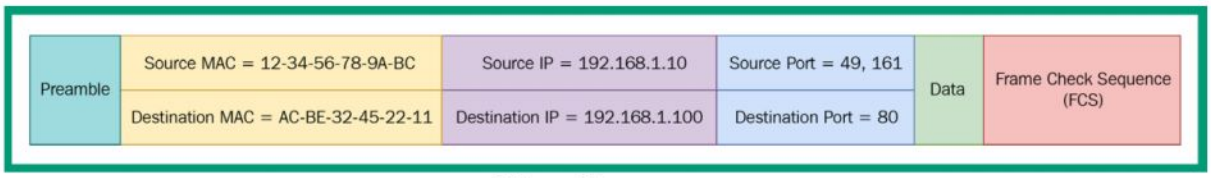


Fig. – Frame

As shown in the preceding diagram, the frame is encapsulated with a layer 2 header that contains the source and destination MAC addresses, as well as the preamble, which is used to identify the start of the frame with sequencing and synchronization.

- The **preamble** helps the receiver of the message determine where the frame begins and how to reassemble the message in the correct order.

- The minimum support frame size on a network is 64 bytes, while the maximum support size is 1,518bytes of all the contents, including the addressing headers, trailer, and data, excluding the preamble.

A MAC address is a **48-bit** address that is embedded onto a NIC by the vendor of the device. The 48-bit (6-byte) binary MAC address is usually written in hexadecimal (ranges 0 – 9, A – F) to easily identify an address apart from another.

The first 24 bits (3 bytes) of a MAC address is known asthe **Organizationally Unique Identifier** (**OUI**) as it is assigned by the vendor of the device/NIC.

- The OUI portion of a MAC address can determine the type/vendor of a device that is connected to a network.
- The last 24 bits (3 bytes) of the MAC address are uniquely addressed.

The following diagram shows an example of the OUI portion of a MAC address:

Organizationally Unique Identifier (OUI)	Assigned by the Vendor
3 Bytes	3 Bytes
24 Bits	24 Bits
00-60-5C	3d-d9-01
Cisco Systems	Device-Specific

Fig. – The OUI portion of a MAC address

MAC addresses are usually presented a bit differently based on the vendor of the device or operatingsystem. The following are examples of the same MAC address in different formats:

- 0060.5c3d.d901: This format is usually used by Cisco systems
- 00-60-5c-3d-d9-01: This format is commonly used on Microsoft Windows operating systems
- 00:60:5c:3d:d9:01: This format is found on Linux-based systems.

Physical layer

- When the Data Link layer places the small blocks of data (bits) onto the physical network media, they are converted into electrical signals that are sent through media such as fiber optic, cable, or the air.
- It defines various standards and frameworks that describe how data can travel over the network media types.
- It is simply the electrical wires, mediatype, and even the connections such as ports and interfaces on a network.
- Each physical componenton a network needs a set of rules on how to send and receive data over the physical network.

It addresses the following elements to ensure data can be sent over a network:

- Physical components
- Encoding
- Signaling

The **physical components** are the hardware elements that you see on a network, such as the networking devices, the physical interfaces/ports on a device, the networking cables that are used to interconnect devices, and so on. These uses a set of standards to ensure devices can transmit messages over the network.

The **encoding process** describes the processes or methods used by a device to convert a stream of messages, such as bits, into code. This code is used to represent patterns that are recognizable by both the sender and receiver devices over the network.

The **signaling** element of the Physical layer describes how the signals are created and placed on the physical network media by a sender device. The signals that are generated by the sender are electrical,wireless, or even optical (light), depending on the network media that is connected to a device.

Understanding TCP/IP

- It was developed by US DoD
- The TCP/IP protocol suite is a group of networking protocols that all work together to ensure messages can be exchanged over any type of network between sender and receiver devices.
- Its original version consists of 4 layers.
- Modern versions of the TCP/IP protocol suite have five layers, splitting the bottom layer into Physical and Data Link layers.

The following diagram shows a comparison of the original TCP/IP protocol suite and the OSI model:

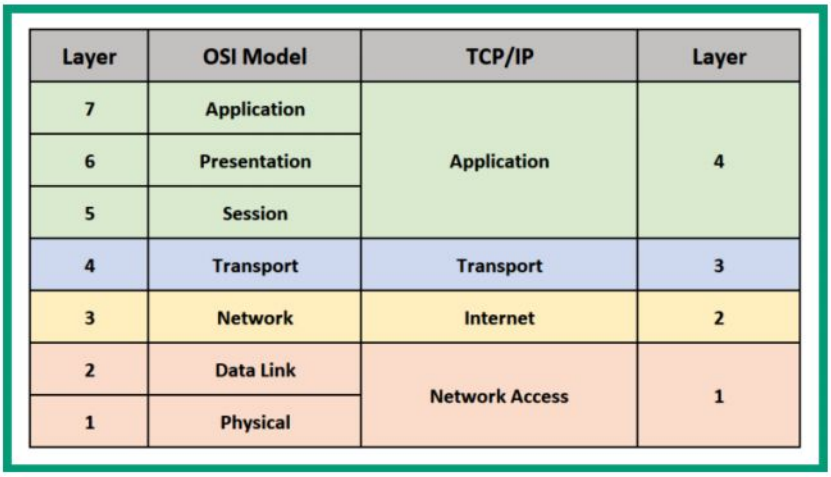


Figure – TCP/IP protocol suite

As shown in the preceding diagram, the following are the four layers of the TCP/IP protocol suite:

- **Application**
- **Transport**
- **Internet**
- **Network Access**

- The Application layer of TCP/IP absorbs all the functionality and responsibilities of the Application, Presentation and Sessions layers of the OSI model.
- The Transport layer of both the OSI model andTCP/IP has the same functionalities and responsibilities.
- The Internet layer of TCP/IP is equivalent to the Network layer of the OSI model.
- The Network Access layer of TCP/IP is equivalent to both the Data Link and Physical layers of the OSI model.

Note

The **Network Access** layer of TCP/IP is sometimes referred to as the **Link** layer or the **Network Interface** layer.

The following diagram provides a high-level overview of a computer sending a message that contains data to a server using the TCP/IP protocol suite:

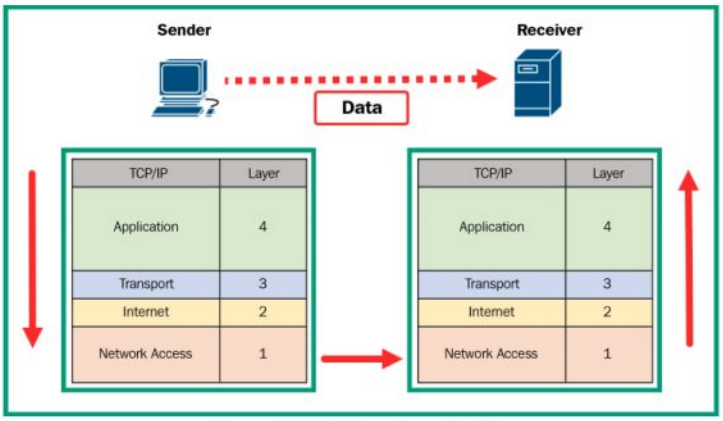


Fig. – TCP/IP protocol suite

Important note

As data moves down a networking model, such as the OSI model or TCP protocol suite, each layer encapsulates a header containing addressing information. When a device receives a message over a network, the process is reversed as each layer de-encapsulates the headers and the message moves up to the Application layer.

Data encapsulation concepts

It's important to understand the various fields found within Ethernet, IPv4, IPv6, TCP, and UDP headers.

Ethernet header

At the Data Link layer, when a packet is received from the Network layer, it is encapsulated with a layer 2 header and trailer. The following diagram shows each field within an Ethernet header:

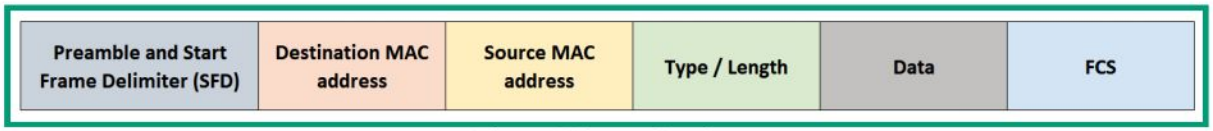


Fig. – Ethernet header

The following are the roles and functions of each field found within an Ethernet header:

- **Preamble** and **SFD**: The preamble is made up of 7 bytes and the **Start Frame Delimiter** (**SFD**)is 1 byte in size, so the entire field is a total of 8 bytes in size. This field is used to synchronize messages being transmitted between a sender and receiver overa network. This field is also used to indicate the start of the frame to the receiver.
- **Destination MAC address**: This field is 48 bits (6 bytes) in length and contains the layer 2 physical address (MAC address) of the next device to receive the message.
- **Source MAC address**: This field is 48 bits (6 bytes) in length and contains the layer 2 physical address of the sender of a frame.
- **Type / Length**: This field is 2 bytes in length and contains details that are used to identify the upper layer protocol (IPv4, IPv6) that is encapsulated within a frame.
- **Data**: The data field ranges between 46 to 1,500 bytes and contains the raw data from the Application layer of the networking model. All Ethernet frames are required to be at least 64 bytes in length. If the frame is less than 64 bytes, additional bits, known as a *pad*, are inserted to increase the size of the frame to the minimum length.
- **FCS**: The **Frame Check Sequence** (**FCS**) field is made up of 4 bytes in length and it's used to verify the integrity of a frame and detect errors.

IP headers

The following diagram shows the field within an IPv4 header:

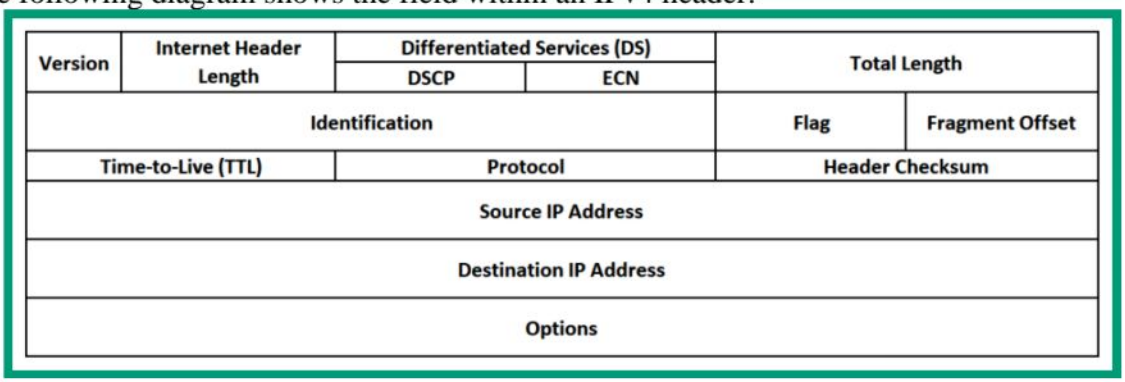


Fig. – IPv4 header

The following is a description of each field within an IPv4 header:

- **Version**: This field is made up of 4 bits and is used to identify the message as an IPv4 packet.
- **Internet Header Length**: This field is made up of 4 bits and is used to indicate where the header section ends and the data section starts.
- **Differentiated Services** or **DiffServ** (**DS**): This field is made up of 1 byte (8 bits) and is used to determine the priority of the packet on the network. Within the DS field, the 6 most significant bits (from the left to right in a binary number) are used to present the **Differentiated ServiceCode Point** (**DSCP**), while the 2 least significant bits (from right to left in a binary number) are used to represent the **Explicit Congestion Notification** (**ECN**) details.
- **Total length**: This field is made up of 16 bits (2 bytes) and is used to indicate the total size of the IPv4 packet.
- **Identification**: This field is made up of 16 bits (2 bytes) and is used to provide identification numbering to each fragmented packet that belongs to an original message.
- **Flags**: This field is made up of 3 bits and is used to indicate whether the packet is to be fragmented or not.
- **Fragment offset**: This field is made up of 13 bits and is used to indicate the sequencing position of a fragmented packet.
- **Time To Live** (**TTL**): The TTL field is made up of 1 byte (8 bits) and is used to determine the life of the packet as it is transmitted between a sender and receiver over the network.
- **Protocol**: This field is made up of 1 byte (8 bits) and is used to indicate the payload type that is enclosed within the packet.
- **Header checksum**: This field is made up of 2 bytes (16 bits) and is used to determine whether there's any corruption within the IPv4 header.
- **Source IP address**: This field contains the source IPv4 address of the sender, which is 32 bits (4 bytes) in length.
- **Destination IP address**: This field contains the destination IPv4 address of the intended recipient, which is 32 bits (4 bytes) in length.
- **Options**: This field is optional as it's not always used.

The Network and Internet layers can also be encapsulated within an IPv6 header on the segment to create a packet. The following are the fields within an IPv6 header:

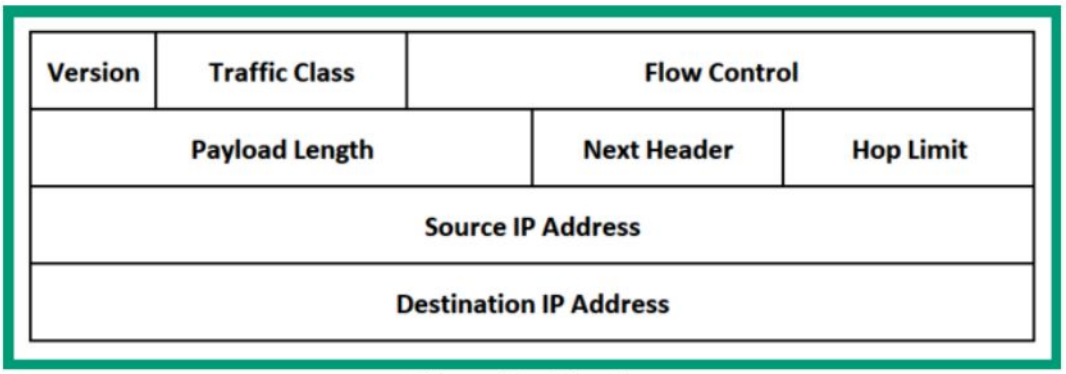


Fig. – IPv6 header

The following is a description of each field found within an IPv6 header:

- **Version**: This field is 4 bits in length and is used to identify this packet as an IPv6 packet on the network.
- **Traffic class**: This field is 8 bits (1 byte) in length. It has the same functionality as the DS field found within an IPv4 packet.
- **Flow control**: This field is 20 bits in length and is sometimes referred to as the **Flow Label**. This field is used to inform the routers on the network to use the same type of handling for IPv6 packets that has the same flow control/flow label information.
- **Payload length**: This field is 16 bits (2 bytes) in length. It is used to represent the length of the enclosed data or payload in the IPv6 packet.
- **Next header**: This field is 8 bits (1 byte) in length. It is used to indicate the payload type that is enclosed within the IPv6 packet.
- **Hop limit**: This field is 8 bits (1 byte) in length and it has the same role and functions as the TTL field found within an IPv4 packet.
- **Source IP address**: This field contains the 128-bit IPv6 address of the sender.
- **Destination IP address**: This field contains the 128-bit IPv6 address of the receiver.

TCP header

The following diagram shows the fields within a TCP header:

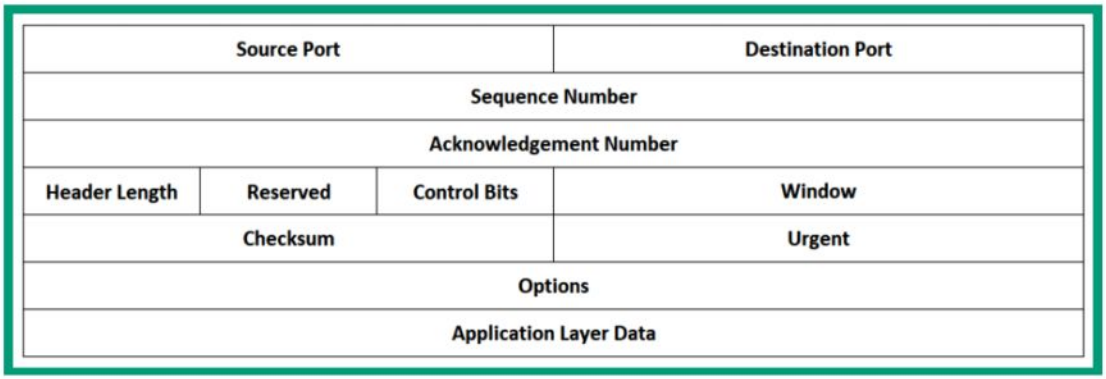


Fig. – TCP header

The following is a description of each field within a TCP header:

- **Source port**: This is a 16-bit (2-byte) field that contains the source service port number of the source application layer protocol.

- **Destination port**: This is a 16-bit (2-byte) field that contains the destination service port number for the destination application layer protocol.
- **Sequence number**: This is a 32-bit (4-byte) field that is used during the reassembly process on the receiver device.
- **Acknowledgment number**: This is a 32-bit (4-byte) field that is used to indicate that the message (data) has been received. This value will be the sequence number + 1.
- **Header length**: This is a 4-bit field that is sometimes referred to as the **data offset** field. It indicates the length of the TCP header.
- **Reserved**: This is a 6-bit field reserved for future usage.
- **Control bits**: This is a 6-bit field that is used to specify various TCP flags such as URG, ACK, PSH, RST, SYN, and FIN. These are sometimes referred to as the **Flag** field.
- **Window**: This is a 16-bit (2-byte) field that indicates the number of bits or bytes that can be accepted during data transmission between a sender and receiver.
- **Checksum**: This is a 16-bit (2-byte) field that is used to detect any errors within the TCP header.
- **Urgent**: This is a 16-bit (2-byte) field that is used to indicate urgency on the TCP header.
- **Options**: This is an optional field within the TCP header that can range between 0 and 320 bits in length.
- **Application layer data**: This field contains the data that's been received from the application layer protocol.

The following six TCP flags are found within the control bit field within a TCP header:

- **URG**: Indicates urgency on the TCP segment
- **ACK**: Indicates acknowledgment of a message
- **PSH**: Performs the push function
- **RST**: Used to reset a connection
- **SYN**: Indicates a synchronization message with a synchronization sequence number
- **FIN**: Indicates to gracefully terminate (finish) a session

UDP headers

Many use the User D tagram Protocol (UDP) to ensure low overhead and faster transmission. The following diagram shows the fields within a UDP header:

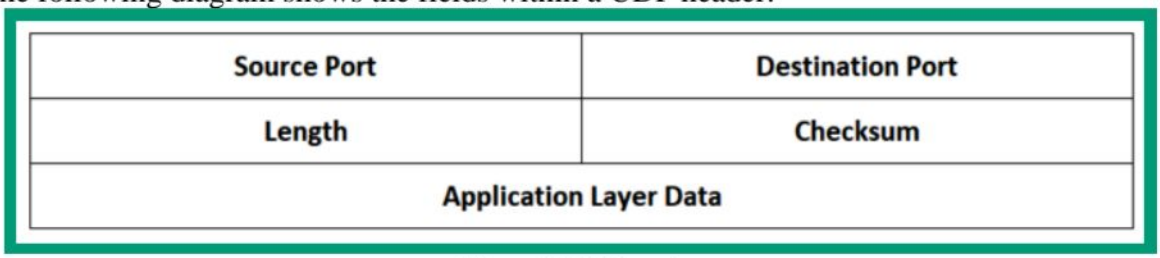


Fig. – UDP header

The following is a description of each field within a UDP header:

- **Source port**: This is a 16-bit (2-byte) field that contains the source service port number of the source application layer protocol
- **Destination port**: This is a 16-bit (2-byte) field that contains the destination service port number for the destination application layer protocol
- **Length**: This is a 16-bit (2-byte) field that indicates the length of the UDP header.
- **Checksum**: This is a 16-bit (2-byte) field that is used for detecting any errors within the UDP header.
- **Application layer data**: This field contains the data that's been received from the application layer protocol.

2. Network Topologies andConnections

Understanding network topologies

- This idea of creating a layout of a network is commonly referred to as a topology or **network topology.**
- It is used to help IT professionals understand how systems and devices are interconnected and to identify areas of improvement or where an issue may exist.
- It can be
  - Physical
  - Logical

Physical Topology

- It contains a high-level overview showing the actual arrangement and placement of devices within an organization.
- It also shows the types of network connections and connectors.

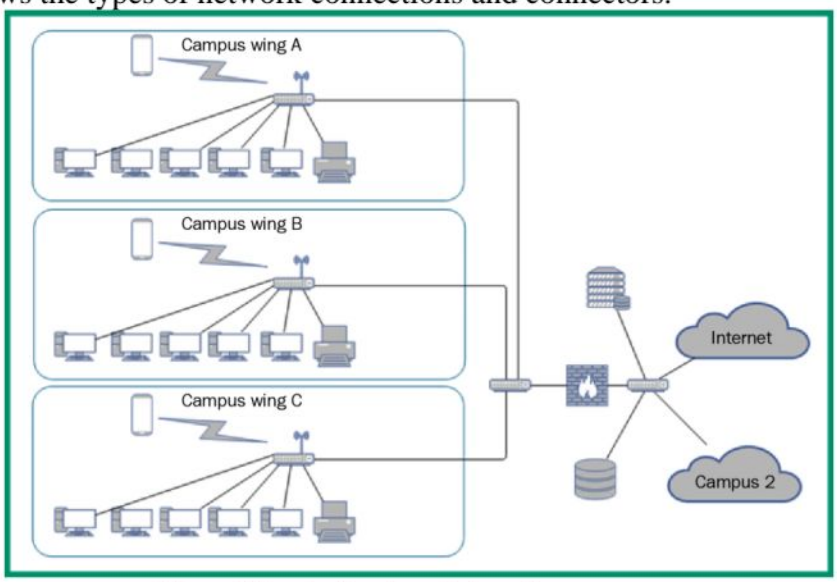


Fig. – Physical network topology

Logical Topology

- It focuses on the technical details of the network, such as the IP addresses and schemes, which demonstrate how data flows across the organization.
- It provides details about the different devices, such as switches, routers and firewalls.

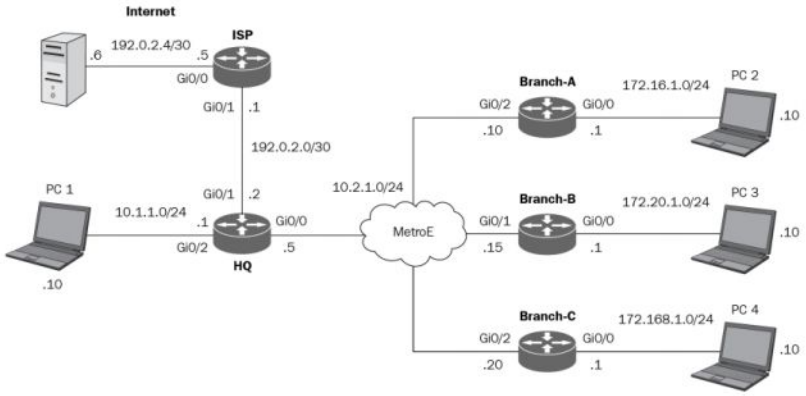


Fig. – Logical network topology

Network diagrams should always be updated whenever a change occurs on the network. A change can be anything such as an upgrade, implementing new technologies and devices, and replacing a device.

Types of network topologies

There are various types of networktopologies, and each has its advantages and disadvantages.

Bus

- This type of network topology was designed to use a single networking cable as the main backbone of the entire network.
- This single backbone allowed nodes such as computers to connect to and access any resource on the network.

The following diagram shows an example of a traditional bus topology:

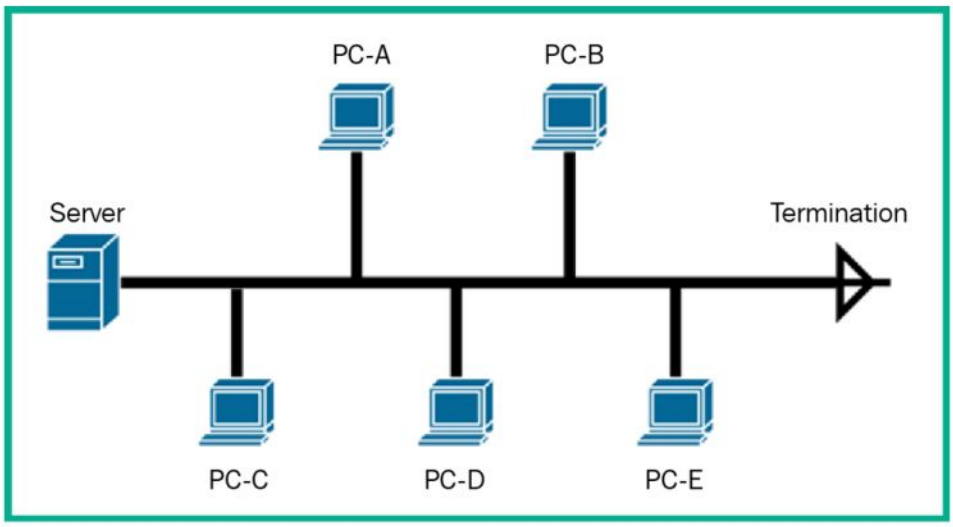


Fig. – Bus topology

- On each end of the backbone networking cable, some terminators are installed to terminate or ground the cable if there are any unwanted electrical signals on the wire.
- In **Shared Ethernet**, the message is sent to a specific destination **Media Access Control** (**MAC**) address.
- Each node receives the message but only the **Network Interface Card** (**NIC**) whose MAC address matches the destination MAC address in the destination section of the Ethernet frame will accept the message (packet).
- All other NICs will discard this message (packet).

The following diagram shows an example of a host sending a Shared Ethernet message:

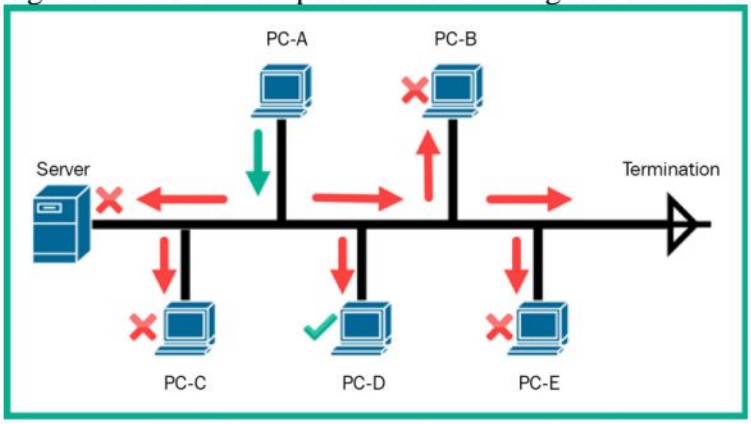


Fig. – Shared Ethernet on a bus topology

Drawbacks

- Only one device can send a messageat a time.
- If multiple devices broadcast their message, networkcollisions can occur.
- There is no redundancy if a network failure was to occur.
- If there's a break at any point along the backbone network cable, this will result in an entire network outage.
- The bus topology does not support scalability.

Ring

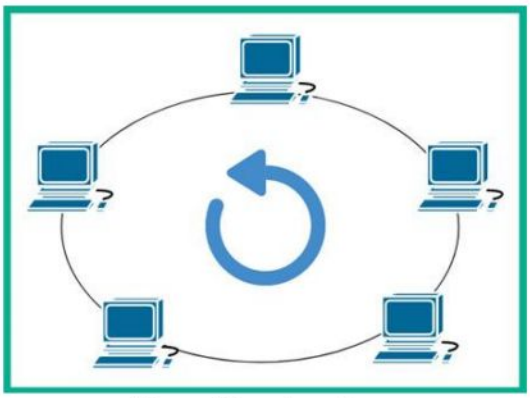


Fig. – Ring topology

- Each host (device) is interconnected to another host to create the ring topology.
- Here communication only occurs in a single direction.

Dual ring

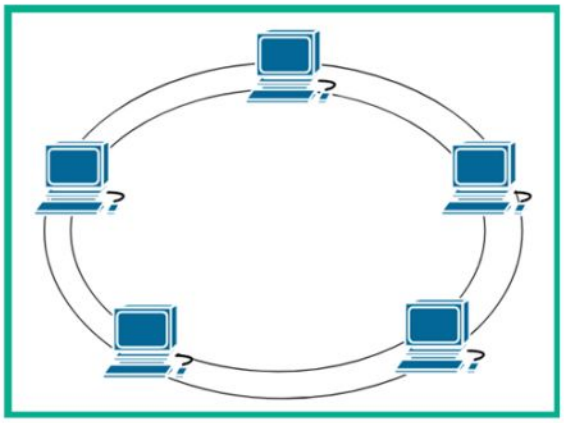


Fig. – Dual ring topology

- It has two logical ring connections on each node on the network.
- The dual ring allows communication to occur in opposite directions on each ring.
- Here, one ring willallow traffic to flow clockwise only and counterclockwise in the other ring.

Drawbacks of ring topology

- The message from the sender is passed to each host on the network until it arrives at the destination host.
- Only one host can send a message at a time on the network.
- If one node is not available, the entire network goes down.

Star

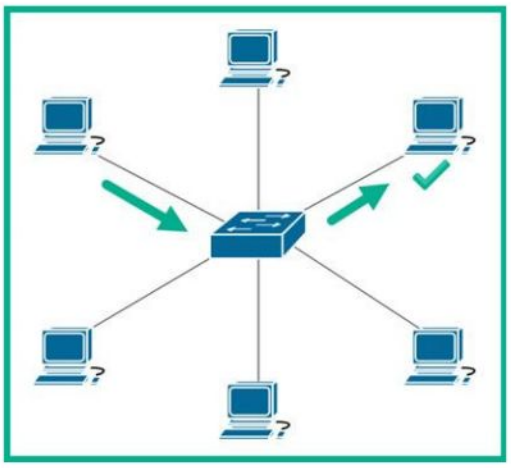


Fig. – Star topology

- It allows the hosts to connect to a single networking device such as a switch/hub.
- If any host wants to send a message to another host, the sender will forward the message to the network switch, which forwards the message to the destination host.
- The switch functions as the network intermediary device to forward messages between a sender and receiver on the network.

Advantages

- If one host on the network is offline or unavailable, the entire network is not affected. The hosts can continue to send and receive messages simultaneously.
- It supports scalability.

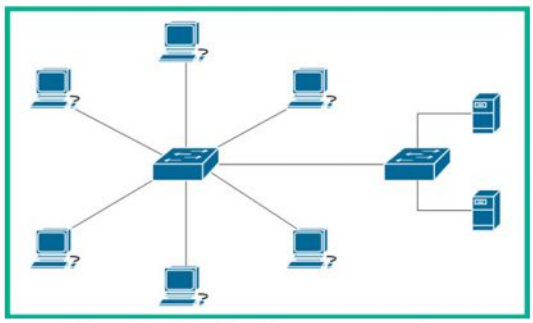


Fig. – Scalability in a star topology

- If the organization wants to connect more hosts to the network, the network professional can connect another switch that will be able to support more hosts.
- Furthermore, scalability does not only apply to the increase of connected devices – it needs to support the increase of network traffic and traffic types too.

Disadvantages

- If the central networking device such as the switch goes down or becomes unavailable, the entire network or all the connected hosts to the switch will be affected and won't be able to communicate.

The following diagram shows a visual representation of a network outage in a star topology:

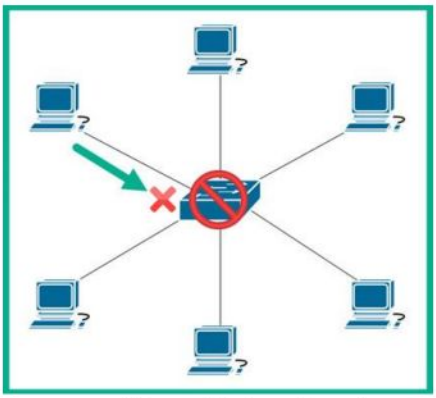


Fig. – Network outage

Mesh

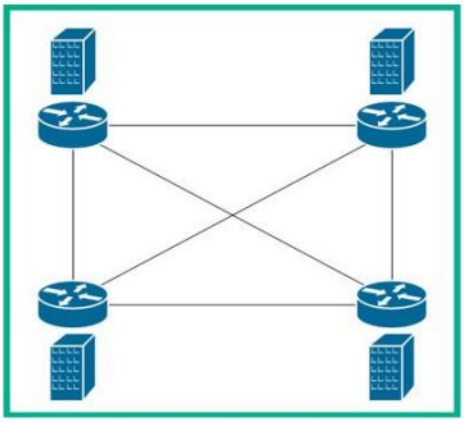


Fig. – Mesh topology

- Each device within the network is connected to all other devices, creating a physical and logical mesh design.

Advantages

- It creates multiple and redundant paths within the network. So, if one path goes down or becomes unavailable, there are multiple other paths available to forward network traffic between a source and a destination.
- It provides full redundancy for traffic flow between any source and any destination as all devices are interconnected.

Disadvantages

- It can be complex to troubleshoot if an issue occurs due to the number of available paths.
- It becomes quite costly and complex as the network increases in size.

No. of links = N(N-1)/2, where N is the no. of devices
e.g., if there are 5 devices, the total number of links = 5(5-1)/2 = 10.
Adding just 1 additional device no. of links =6(6-1)/2 = 15.

Hybrid

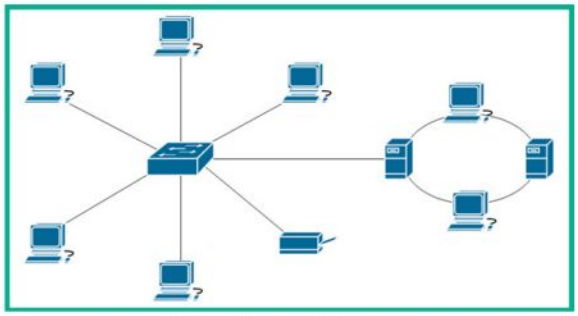


Fig. – Hybrid topology

- It is a combination of two or more different topologies that are interconnected to create a unified network.
- The above network consists of both star and ring topologies.
- Often, network professionals use this topology within their organizations to interconnect end devices such as computers and servers, as well as interconnect their branch offices together to share resources.

Hub and Spoke

- It is designed to provide a centralized node that acts as the main hub for all other nodes to interconnect.
- Each node is connected to the hub and these connections are referred to as spokes.
- It does not allow nodes to directly connect; all network traffic is sent through the hub which is responsible for forwarding traffic to another node on the network.

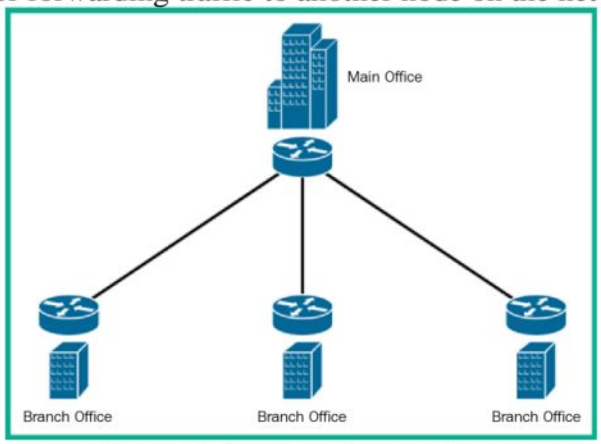


Fig. – Hub and spoke topology

- As shown in the preceding diagram, the organization has one main office that will function as the headquarters that contains all the servers, while three remote branch offices will be used to provide services to customers are various geographic locations.
- Whenever a user or device needs to access a resource at another branch location, the traffic is sent to the main officer router (hub), which then forwards the traffic to the destination network.

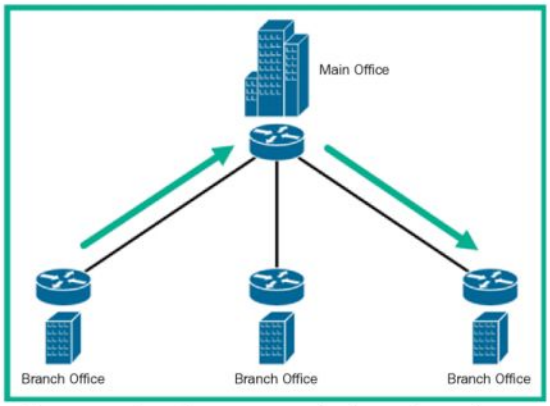


Fig. – Communication over a hub and spoke network

- This topology is commonly used by medium-sized and large organizations to interconnect their remote branch offices to their main office location.
- It is a cost-efficient design that allows organizations to save on internet subscription fees and improve their security monitoring.

Discovering network types

Network types are used to define the geographic boundary orlimitation of a network and help network professionals understand the relationship between the connected devices within the network.

Peer-to-peer

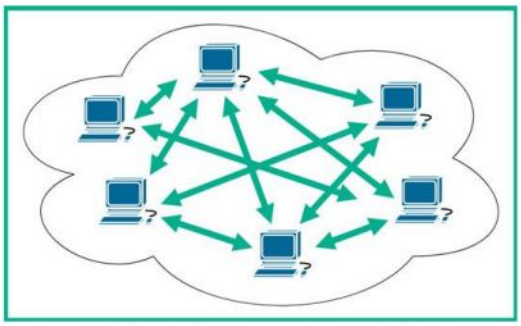


Fig. – Peer-to-peer model

- Here each client is logically connected and shares their resources with other clients on the network without the need for a centralized, dedicated server to provide the resources.
- If a client has a printer, that client can be configured to share the printer as a resource with other clients on the network. The client that is sharing the printer or resource becomes a server, while the others hosts (computers) are clients that are accessing or requesting the resource.
- It does not support scalability well.
- These are typically implemented as workgroups in many small organizations.
- A real-world example of a peer-to-peer network is sharing files using a *torrent*. In the world of torrenting, *seeds* or *seeders* are the computers that have the complete file on their device and share it with others to download.
- On the other hand, *leeches* or *leechers* are devices that download the file from each peer, preferably the seeds, until it reaches 100% download completion.

Disadvantages

- There's no centralized management of resources,
- Security is a huge concern as each node is responsible for managing its security posture.

Client-server

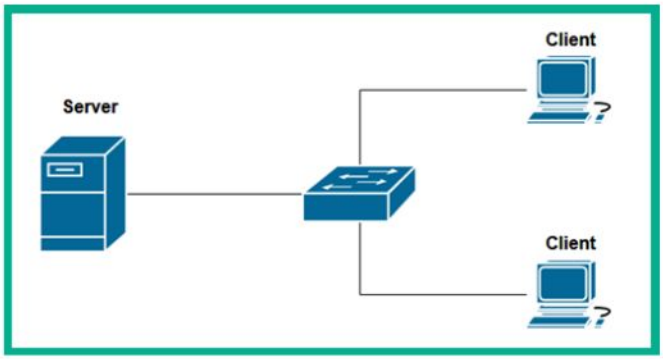


Fig. – Client-server model

- It contains dedicated devices that provide a resource or service to hosts on a network. These devices are referred to as servers.

- A server can be any device running an application that allows other hosts on the network to access the resources stored or being provided by the server.
- The server can be configured as a file server to centrally store files and data for other devices and users on the network. The clients on the network are the devices that are requesting a service or resource.

Advantages

- Scalability allows the network to grow while ensuring the resources are centrally accessible by all clients on the network.

Personal area network

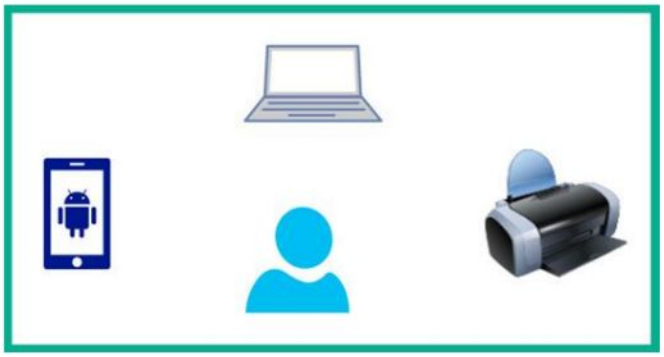


Fig. – Personal area network

- It is a small network that is usually created by a user to interconnect their devices, such as a laptop, smartphone, wireless headphones, or a wireless printer.
- A user can set up a wired or wireless network to ensure their devices are connected to the same network.
- It is not designed to connect to a larger network with other devices.
- A real-world example of a PAN is connecting a laptop and smartphone to a wireless printer at home to print pictures.
- Each device is responsible for managing its security.

Local area network

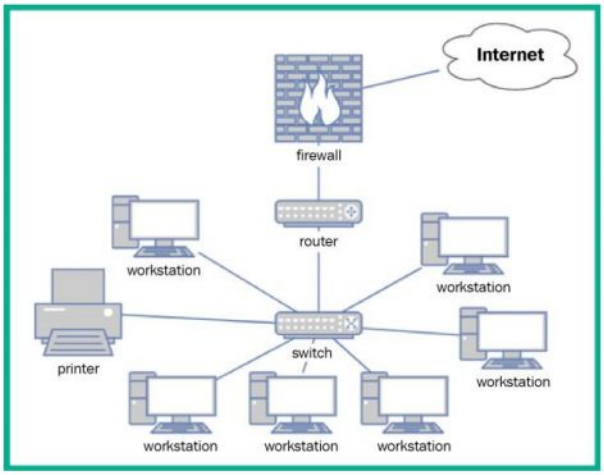


Fig. – LAN network model

- It exists within a single geographic location, such as within a building.
- A LAN allows all devices within an office location or building to be interconnected and share resources.
- Interconnecting all the devices, such as the computers, servers, and network printers, into a single physical network creates a LAN that allows everyone and all devices on the same network to easily share resources.
- As shown in the preceding diagram, the network contains a few workstations that are used by the employees within a small office, and each end device, such as a computer and printer, is connected to the network switch.
- The switch connects to the router, which functions as the **default gateway** to forward traffic from the internal network to a remote/foreign network such as the internet.
- The router connects to the firewall to filter inbound and outbound traffic between the internal network and the internet.

Important note
Without a default gateway device such as a router at the edge of a logical IP network, clients will not be able to communicate with remote networks or devices.

Wide area network

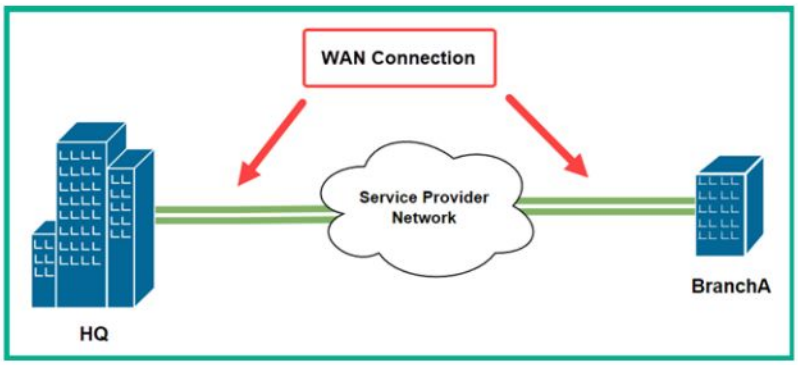


Fig. – WAN

- It allows organizations to extend their LAN and its resources over a large geographic distance.
- As time goes by, the organization will grow and create new remote office locations within other cities or countries to support its customers.
- The organization may have all its servers located at its main office and want to share access with employees who are working at a remote office.
- Using a WAN allows the organizations to extend their LAN from their main office over a large geographic distanceto each of the remote offices as needed.
- The WAN connection is established by a **Managed Service Provider** (**MSP**) or an **Internet Service Provider** (**ISP**).
- All traffic sent into a WAN connection by anorganization remains private as the traffic passes through the service provider's network infrastructure.

What if an organization has multiple branch offices? How can internet services be established for all locations of the company?
One solution is to implement a WAN solution and an internet service ateach office location. The WAN solution will be used to share the network resources between branches, while the

internet services provide access to the online services and resources that are outside the company's network.

The following diagram shows a WAN connection being used to create a hub and spoke topology to connect each remote office to the main office location; each office location has a dedicated internet connection:

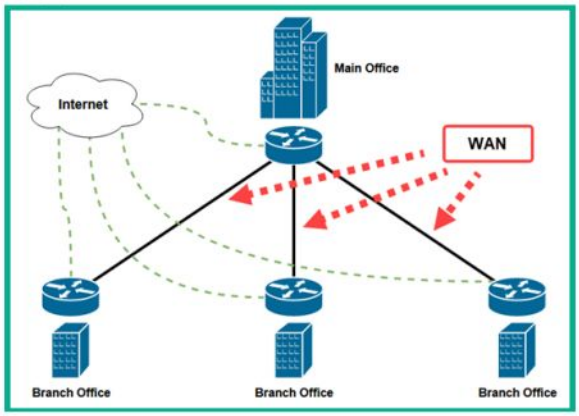


Fig.– Hub and spoke WAN connection

If each branch office is located within the same country, it's not cost-efficient as the organization is charged for the internet service at each branch location, including the main office.

A better solution for an organization that has multiple branch offices within the same country is to create a hub and spoke topology for the WAN solution and implement a single internet connection at the main office. The internet service can be redistributed within the WAN connected to each branch router.

The following diagram shows an example of using a hub and spoke topology for a WAN solution while redistributing the internet to each branch office within the same country:

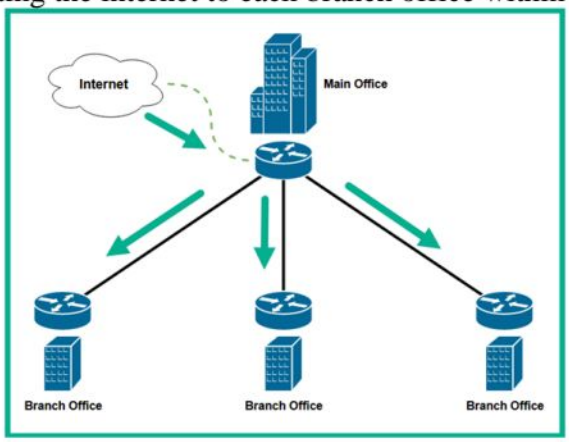


Fig. – Hub and spoke WAN topology with internet connectivity

This design allows an organization to save a lot of moneyon their internet services when the branch offices are usually in the same country.

Important note

It is possible to redistribute internet services through a WAN connection to a branch office in another country, but the latency (response time) and network performance will not be optimal.

Metropolitan area network

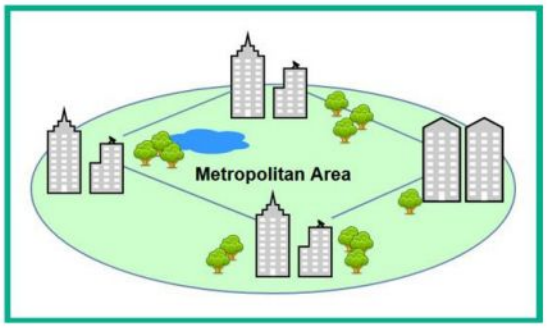


Fig. – Metropolitan area network type

- In large cities, some organizations have multiple branch offices within the same city and need interconnectivity between their offices to share resources with employees.
- Using a **metropolitan area network** (**MAN**), a service provider can interconnect all the branch offices of a single company within the same city.
- Some cities offer a MAN to residences as a low-cost, high-speed connection to the internet. These MANs can be used to incentivize residents to move to that city.

Wireless local area network

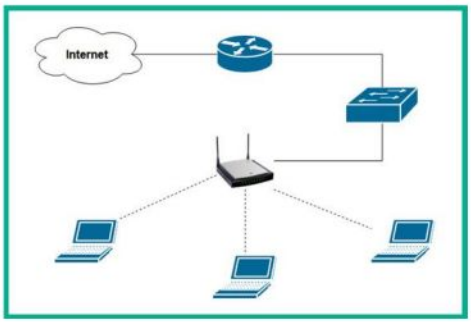


Fig. – WLAN network type

- It is a wireless local area network that has one or more Access Points or wireless routers to allow wireless capable clients to connect and share resources.
- APs are connected to a network switch that provides wireless connectivity to wireless clients, as shown in the above diagram.
- The wireless router generates a wireless signal using radio frequencies on the 2.4 GHz, 5 GHz, and 6GHz bands based on the **Institute of Electrical and Electronics Engineers** (**IEEE**) 802.11 standard.
- The wireless network generated by the wireless router is on a unique **Internet Protocol** (**IP**) network, while the wireless router is connected to a wired network on a different IP network.
- Hence, a wireless router performs routing between the two different IP networks, from wireless to wired, and between the different IP networks.

Important note

Wireless routers are commonly used on small networks such as within homes and small businesses. An **Access Point** (**AP**) is a layer 2 device that provides a wireless network to allow wireless clients to establish a connection and access the resources on the wired network.

Ethernet Technology and Virtualization

Types of connections

- Wired
  - Copper
  - Fibre Optic
- Wireless

Copper cables

These are inexpensive network cables that are very easy to implement within buildings, office spaces, and homes.

There are two types of copper cables that are used within networks:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

Unshielded Twisted Pair (UTP)

- UTP cables are very common and you will find them in almost any network within an organization and even **Small Office/Home Office** (**SOHO**) networks.
- It does not contain a protective coating to prevent the actual conductors from absorbing **electromagnetic interference** (**EMI**) from machinery and other components.
- The **Network Access** layer of the **Transmission Control Protocol/Internet Protocol** (**TCP/IP**) networking model converts the message into an appropriate signal for the network media before placing the message onto the actual network.
- Copper cables transmit electrical signals over the wire in short distances and networking devices can decode the signals into packets and data.
- It can absorb EMI from nearby devices and other electrical wires. So, the bits that are being transmitted between devices will become corrupted and the sender will need to retransmit any messages that are damaged or corrupted.
- It referred to as *twisted pair* cabling. There are a total of 8 individual wires that have a unique color coating. These wires are twisted in a total of 4 pairs.

The following figure shows a UTP cable:

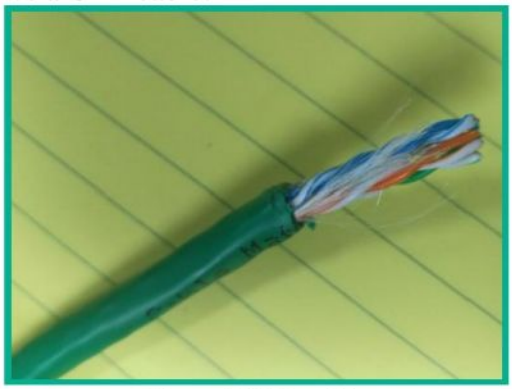


Fig. – UTP cable

- It's not recommended to implement UTP cables in areas or zones that contain a lot of machinery that emits EMI.

Shielded Twisted Pair (STP)

- It is a type of twisted cable with the addition of protective shielding around the twisted conductors within the outer jacket.

The following figure shows an STP cable:

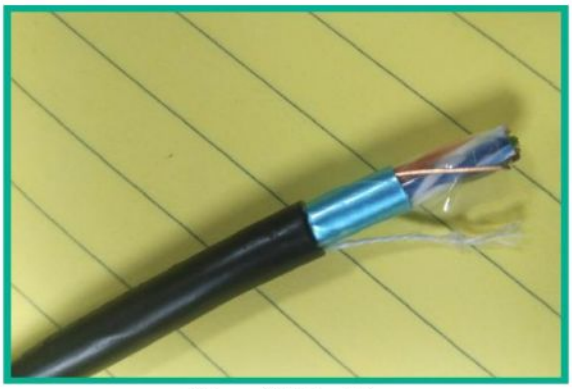


Fig. – STP cable

- It is used to prevent EMI from entering the copper conductors within the cable.
- It is a bit more expensive because of the additional layer of protection within the cable's design.
- It is implemented within environments that have a lot of EMI.

- Both the UTP and STP cables are made using Polyvinyl Chloride (PVC), a material that releases toxic/harmful fumes to humans when burnt. These are known as non-plenum-rated cables.
- It's highly recommended to implement plenum-rated cables within the plenum spaces within buildings when needed.

The following diagram shows an example of a plenum-rated cable:

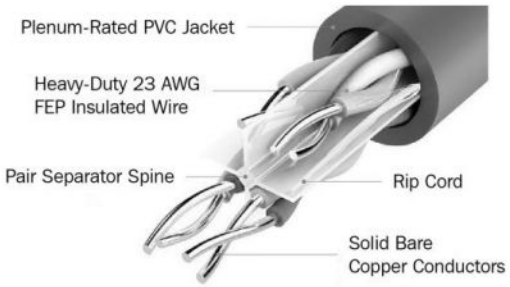


Fig. – Plenum-rated cable

- These cables contain a plenum-grade outer jacket to prevent fire from burning the conductors; there's also a pair of separator spines to keep each pair of twisted cables separate from other pairs.
- These are more expensive compared to non-plenum-rated cables.
- These are less toxic.

- Various types of copper cables are used to interconnect end devices to the network.
- The **Telecommunication Industry Association** (**TIA**) created a cabling standard that's used by networking professionals within the industry.
- These cables are described as a **category** (**Cat**) cable followed by a number.
- Each category defines how the cable can be applied to a network, its support speed, such as bandwidth, and the maximum length for data transmission.

The following is a list of various types of category cables that are commonly found within organizations:

- **Cat 3**: Supports speeds up to 10 Mbps with a maximum distance of 100 meters

- **Cat 5**: Supports speeds up to 100 Mbps with a maximum distance of 100 meters
- **Cat 5e**: Supports speeds up to 1 Gbps with a maximum distance of 100 meters
- **Cat 6**: Supports speeds up to 1 Gbps with a maximum distance of 100 meters
- **Cat 6a**: Supports speeds up to 1 Gbps and 10 Gbps with a maximum distance of 100 meters
- **Cat 7**: Supports speeds up to 1 Gbps and 10 Gbps with a maximum distance of 100 meters
- **Cat 8**: Supports speeds up to 40 Gbps with a maximum distance of 30 meters

- The ends of the twisted pair cables are terminated by various types of **Registered Jack** (**RJ**) connectors.
- For CAT 3 cable, an RJ-11 connector is used on both ends of the cable. It contains 4 pins; these are commonly used on traditional landline telephone systems.

The following figure shows a CAT 3 cable with an RJ 11 connector on its end:

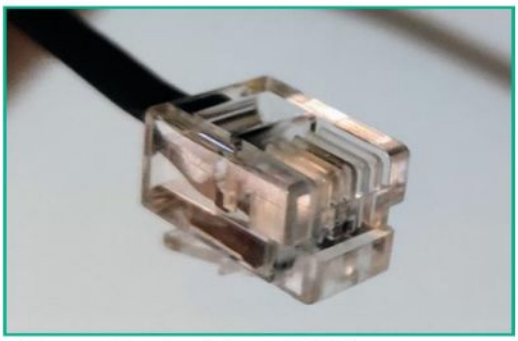


Fig. – Cat 3 with an RJ 11 connector

Additionally, the RJ 45 connector is an 8-pin connector that is used on most modern Ethernet cables, such as CAT 5 and above.

The following figure shows an Ethernet cable with an RJ 45 connector:

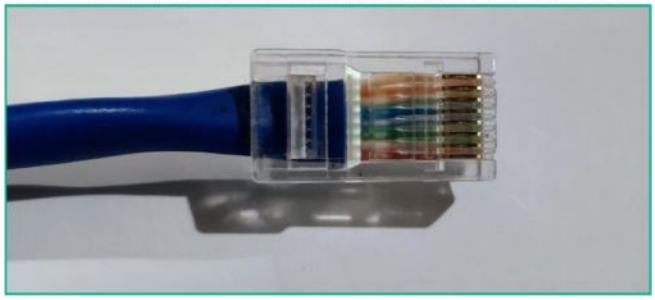


Fig. – Ethernet cable with an RJ 45 connector

- The **TIA-568** standard helps networking professionals and organizations maintain consistency within their networks.
- The TIA has created two cabling termination standards that indicate how each conductor within a cable is terminated to a corresponding pin within an RJ 45 connector.

Fig. – Coaxial cable

- Another type of copper cable is coaxial. It has a foil coating around the copper core to protect it from EMI.
- It contains multiple layers of protection to prevent harm to the copper conductor at the core.
- It transmits its electrical signals through an inner core of either solid or stranded copper, or copper-clad steel. This inner conductor is surrounded by a layer of insulating material (usually plastic), which is itself surrounded by braided copper cable.
- This outer braided copper cable serves to protect the inner core from EMI and signal leakage.
- The inner insulating material (sometimes called a dielectric material) serves to separate the two conductors in the cable, while the outermost insulating sheath serves to cover and protect the outer braided jacket, and the entire cable by extension.
- It uses the **Radio Guide/Grade** (**RG**) standard for their specification. In particular, the **RG-59** legacy standard is used on older TVs and cable modems with a termination point of 75 Ohms.
- The newer **RG-6** standard that is used on cable TV and broadband internet services has a termination point of 75 Ohms.

The following are the various layers of a coaxial cable, from the outer to inner layers:

• **Protective coating**: Made using PVC and protects the internal media from external elements and environmental factors

• **Braided shielding**: Prevents EMI from reaching the copper conductor

• **Foil shielding**: Prevents **Radio Frequency Interference** (**RFI**) from reaching the copper conductor

• **Dielectric Insulator**: An insulator to separate the copper conductor and the braided shielding, and to keep the copper conductor at the center of the coaxial cable

• **Copper conductor**: Used to transmit the electrical signals along the cable.

The following three types of connectors are used on coaxial cables:

• **F-pin connector**

• **Bayonet Neill-Concelman** (**BNC**) connector

• **T type connector**, which is used to interconnect three coaxial cables together

F-pin connector

Fiber optic cables

- These cables transmit data using pulses of light that are sent down a thin core of plastic or glass, which is surrounded by a material called cladding.
- The combination of core and cladding allows for the light to be transmitted through the process of either total internal reflection or continuous refraction of the light.

The following figure shows a fiber optic cable:

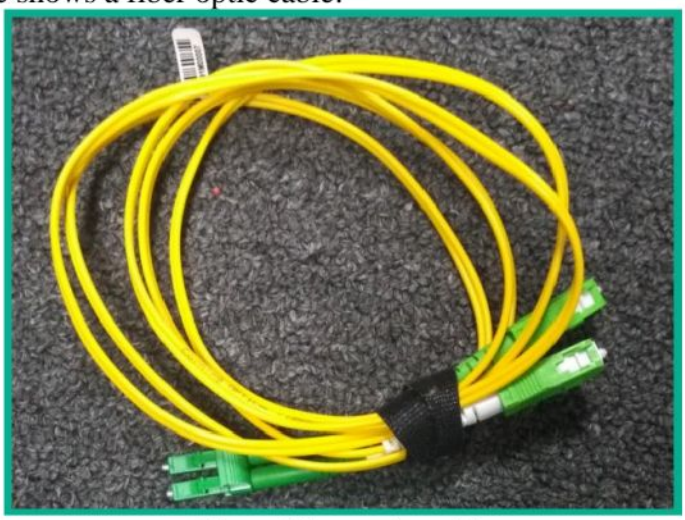


Fig. – Fiber optic cable

Advantages

- It allows faster throughput of data over the cable since it uses **Light Emitting Diodes** (**LED**) or lasers to transmit data in the form of light.
- Photons travel at a higher speed than electrons, meaning that bits of data are delivered faster than in copper cables.
- Fiber optic cables can run for many kilometers before needing a repeater.
- Fiber optic cables are immune to EMI.

Disadvantages

- These are more expensive compared to copper cables.
- These are very fragile and easy to break as the core is either glass or plastic.

The following diagram shows the structure of a fiber optic cable:

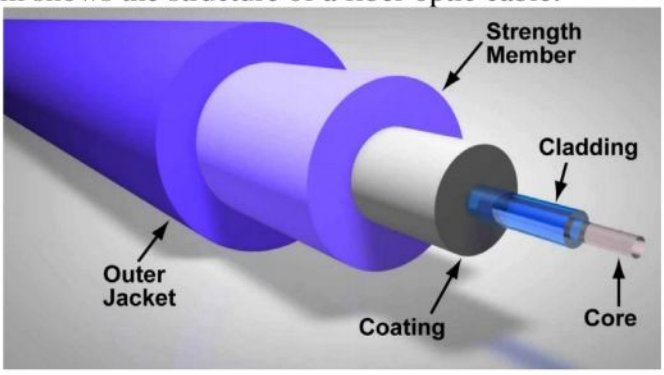


Fig. – Fiber optic cable structure

- It contains multiple layers of protection to prevent damage to the core.
- Each layer, such as the outer jacket, strength member, coating, and cladding, shields the core (glass or plastic) from external and environmental factors.

There are two major categories of fiber cables:

- single-mode
- multimode.

Single-mode fiber

- It is constructed to transmit only one mode of light through the fiber (in a direction parallel to the fiber). Its diameter is quite small concerning the diameter of the cladding.
- For example, 9/125 fiber, which means the core is 9 **micrometers** or **microns** (**µm**) in diameter, while the cladding is 125 µm.
- Light through SMF can consist of multiple frequencies, but all of these frequencies follow a single path through the fiber.
- It is used for fibers that need to span several kilometers in distance.
- The light sources for SMF are usually lasers. Transceivers are often more expensive.
- SMF often operates using wavelengths of 1,310 nm or 1,550 nm, and the cable coating is often colored yellow.

Multimode fiber

- MMF cables are constructed with much larger diameters. For example, one common type of MMF is 62.5/125, meaning that the cable has a diameter of 62.5 µm, compared to the 9 µm of some SMF cables.
- This wider core allows multiple modes of light to propagate through the fiber.
- It limits the maximum link length to much lower distances than SMF.
- Less precise transceivers can be used, allowing the cost of MMF systems to be generally lower than equivalent SMF systems.

Fiber connectors

Fig. – Fiber connectors

Lucent Connector (LC) consists of a small plastic latch, which helps secure the fiber connector to the port, and a 1.25 mm ferrule, which is used to align the fiber optic cable with the connector. It is a small form factor connector, making it suitable for high-density fiber deployments such as in data centers.

The Straight Tip (ST) types of connectors consist of a larger ferrule (2.5 mm) and a twist-type, spring-loaded, cylindrical, nickel-plated, or stainless-steel bayonet connector for locking.

Subscriber Connectors (SCs), also known as Square Connectors or Standard Connectors, are connectors that are push-pull square-shaped connectors with 2.5 mm, spring-loaded, ceramic ferrule, and snap-in connector latches. They are easy to disconnect/reconnect and can be found in many network installations.

Mechanical Transfer Registered Jack (MT-RJ), also known as Media Termination Recommended Jack, are small, duplex fiber connectors, with both fibers terminating on a single 2.45 x 4.4 mm ferrule. They are roughly half the size of SCs and are easy to connect/disconnect from their ports using plastic latches. Two pins, located on transceivers, allow easy alignment of the connector.

Understanding IPv4 and IPv6 Addressing

The need for IP addressing

- An **Internet Protocol** (**IP**) address is a Layer 3 logical address that is assigned to all devices on a network to allow communication between nodes on different IP networks.
- The **Internet Assigned Numbers Authority** (**IANA**) is the governing body that is responsible for managing global **IP version 4** (**IPv4**) and **IP version 6** (**IPv6**) address assignments, **Autonomous System Number** (**ASN**) allocation to organizations that manage a large number of public networks, protocol assignment, and root **Domain Name System** (**DNS**) directories and services of the world.
- To assist with distributing public IP addresses to **Internet Service Providers** (**ISPs**) around the world, IANA delegated the responsibility of IP distribution to five **Regional Internet Registries** (**RIRs**) around the world.
- Each RIR is responsible for distributing IPv4 and IPv6 address blocks to specific regions and geolocation.

The following are the five RIRs and their responsible geolocations:

- **African Network Information Center** (**AFRINIC**): Supports the continent of Africa
- **Asia-Pacific Network Information Centre** (**APNIC**): Supports regions of Asia and the Pacific
- **American Registry for Internet Numbers** (**ARIN**): Supports regions of Canada, the USA and parts of the Caribbean
- **Latin America and Caribbean Network Information Centre** (**LACNIC**): Supports Latin America and parts of the Caribbean regions
- **Reseaux IP Europeens Network Coordination Centre** (**RIPE NCC**): Supports Europe, the Middle East and Central Asia

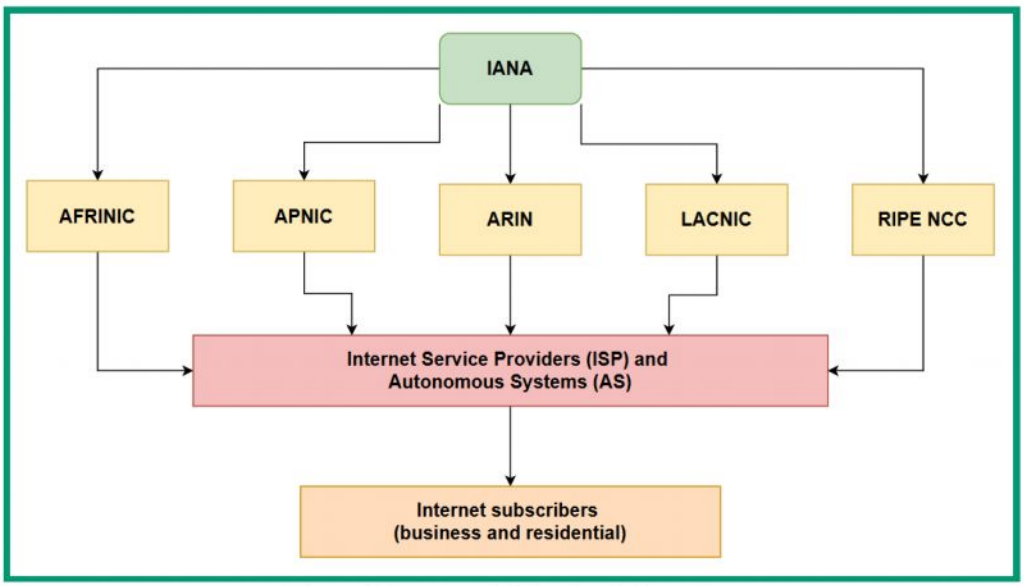


Fig. – IP network blocks delegation

The ISPs use their AS numbers to share their network routing prefixes with other ISPs using the **Border Gateway Protocol** (**BGP**).

Important note

BGP is an **Exterior Gateway Protocol** (**EGP**) that allows network operators such as ISPs to exchange their routing information with each other, allowing users on the internet to reach networks beyond their local ISP.

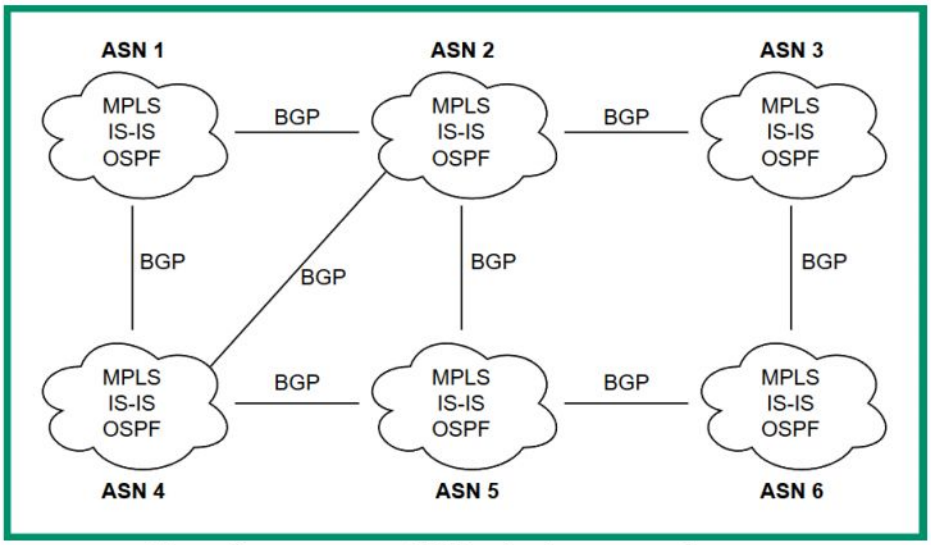


Fig. – Interconnected ISPs sharing network routes

- As shown in the preceding diagram, each network operator or ISP is assigned a unique AS number that allows them to interconnect and share their network routes with other ISPs while using BGP to share their routes.
- Internally, network operators use various **Interior Gateway Protocols** (**IGPs**) such as **Open Shortest Path First** (**OSPF**), **Intermediate System to Intermediate System** (**IS-IS**) and **Multiprotocol Label Switching** (**MPLS**) to route traffic within their networks.

- As the internet began to grow quickly, IPv4 addresses for the internet were determined to one day be exhausted over time.
- As early as 1999, the world began to see a new generation of logical addresses being deployed, known as IPv6 addresses.
- These are 128-bit logical addresses that are written in hexadecimal notation.
- IANA implemented the concept of creating two logical address spaces for IPv4 to help reduce the depletion of IPv4 addresses around the world.
    - Private Address Space
    - Public Address Space

Public versus private address spaces

- The **public address space** specified the IPv4 addresses that are routable on the internet and can be assigned to devices that are directly connected to the internet.
- The **private address space** specifies the classes and ranges of IPv4 addresses that are non-routable on the internet and can be assigned to devices on private networks only.

The following table shows the public classes of IPv4 addresses:

Class	Range	Default Subnet Mask
A	0.0.0.1 - 127.255.255.255	255.0.0.0
B	128.0.0.1 - 191.255.255.255	255.255.0.0
C	192.0.0.1 - 223.255.255.255	255.255.255.0
D	224.0.0.1 - 239.255.255.255	N/A
E	240.0.0.1 - 255.255.255.255	

Fig. – IPv4 public address space

- As shown in the preceding table, classes A, B and C can be assigned to devices that are directly connected to the internet.
- The Class D address range is used for multicast communication between applications and services that operate on devices within a network
- The Class E address range is reserved for experimental uses.

Important note

The subnet mask is used to determine the network and host portion of an IP address, and the total number of IP addresses and usable IP addresses within a network.

Classful IP address

- Originally, the IPv4 address spaces used **classful** addresses, which describe how each IPv4 address class contains a specific number of networks.
- Here, each network contains a specific number of usable/assignable IPv4 addresses to host devices.

The following table shows the IPv4 classful addressing information:

Class	Range	Default Subnet Mask	Number of Networks	Number of Usable IPv4 Addresses
A	0.0.0.1 - 127.255.255.255	255.0.0.0	126	16,777,214
B	128.0.0.1 - 191.255.255.255	255.255.0.0	16,384	65,534
C	192.0.0.1 - 223.255.255.255	255.255.255.0	2,097,152	254

Fig. – Classful IPv4 addresses

- One of the **major issues with classful addressing** is the **wastage of unused IP addresses** within an organization.

Scenario-1

An organization with 2,000 devices requires a network block of addresses to assign to their company's network.

- A Class B address block would be most suitable in this situation. However, since any Class B network provides 65,534 usable IPv4 addresses, there will be a huge wastage of 65,534 – 2000 = 63,534 unused addresses that cannot be allocated to another organization.
- Organizations that were assigned very large IPv4 network blocks with too many addresses led to wastage.

Scenario-2

Let's say an organization has 400 devices and needs IPv4 addresses to assign to its network.

- The organization will need to lease a Class B address block that contains too many IPv4 addresses or multiple Class C address blocks to support the number of hosts.
- So, classful addressing was not flexible enough to support organizations of various sizes.
- The routers within service providers' networks contained very large routing tables, which affected the performance of a router.
- If routers on the internet have a very huge routing table, containing all the classful networks of the internet, each router will take some time to go through its routing table to find a destination path to forward a packet.
- Companies were not able to logically segment their networks into multiple IP subnetworks from a single network block, which was not flexible for businesses of different sizes.
- A simple example is a business with 90 host devices that would be assigned a Class C network block that contains 254 usable IPv4 addresses.

- Any unused IPv4 addresses were not reallocated to another organization.
- One solution was to implement **classless** addresses, **which removed the need to use a default subnet mask** for a specific range of IPv4 addresses.
- In this case, a Class A IPv4 address does not need to use the default subnet mask of 255.0.0.0 in classless addressing.
- It allows networking professionals to use custom subnet masks with any IPv4 address.
- To **help reduce the wastage of public IPv4 addresses, IANA created the private IPv4 address space**, which allows organizations to use a specific set of IPv4 addresses on private networks.
- These private IPv4 addresses are non-routable on the internet, i.e., if a computer is assigned a private IPv4 address, it will not be able to communicate with devices on the internet and vice versa.
- If all devices within the private networks of organizations were configured with a unique public IPv4 address – the public address space would be exhausted a lot quicker than expected.
- So, the private address space allows organizations to assign a unique private IPv4 address on devices within their private networks.

The following table shows the private IPv4 address space:

Class	Range	Default Subnet Mask
A	10.0.0.1 - 10.255.255.255	255.0.0.0
B	172.16.0.1 - 172.31.255.255	255.255.0.0
C	192.168.0.1 - 192.168.255.255	255.255.255.0

Fig. – Private IPv4 address space

- As shown in the preceding table, the private IPv4 address spaces contain three classes of address ranges.
- Each class of address can be used within any organization's private network. This means two or more organizations can be using the same private IPv4 address classes within their private networks without causing any conflict.
- Before devices on a private IPv4 network can communicate with devices with public IPv4 addresses on the internet, the source private IPv4 address has to be translated into a public address.

Network Address Translation (NAT)

- NAT allows a private IPv4 source address to be translated into a public IPv4 address.
- It allows devices on a private network to communicate with devices on a public network.
- To help ensure devices on a private IPv4 network can communicate with the internet, a NAT-enabled router is implemented between the networks.

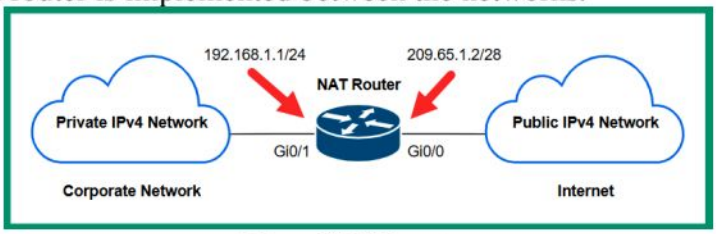


Fig. – NAT router

- There's a private IPv4 network on the left that indicates an organization's private network while on the right there's the internet, where all devices are assigned a public IPv4 address.
- To interconnect these two different networks, a router is implemented to route traffic between the different networks.
- To ensure devices on the private network can communicate with devices on the internet, NAT is configured on the router to translate any source IPv4 address that originates from the private network to the public IPv4 address that's configured on the router.
- All outbound traffic from the corporate network to the internet will be assigned a new source IPv4 public address of 209.65.1.2.
- This allows devices on the internet to see the source traffic as originating from a device with a public IPv4 address of 209.65.1.2 and not from the private IPv4 network.

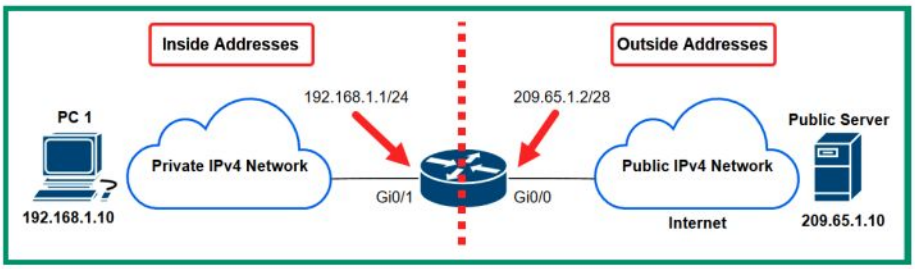


Fig. – NAT operations

- All devices on the left are connected to the private IPv4 network, while all devices on the right are connected to the internet with a public IPv4 address.
- Additionally, the NAT-enabled router/modem identifies the addresses as **inside** and **outside**.
- The inside addresses are the private IPv4 addresses that are to be translated by the NAT-enabled router/modem. The outside addresses are those that are seen by all devices on the public address space – the internet.
- *PC1* is connected to a private network within an organization having a private IPv4 address of 192.168.1.10. This address is referred to as the Inside Local address. If *PC 1* attempts to send a message to the *Public Server* on the internet, the packets from *PC 1* will be restricted from entering the server provider's network and the internet.

The following steps explain how NAT works:

1. *PC 1* creates a packet with the source IPv4 address of 192.168.1.10 (*Inside Local*) and a destination address of 209.65.10 (*Outside Global*), and forwards the message to the default gateway (router) at 192.168.1.1.
2. The router inspects the source and destination IP addresses within the IP header of the packet to determine the destination and checks its routing table for a route (path).
3. Before the router forwards the packet to the internet, it translates the source private IPv4 address from 192.168.1.10 to the public IPv4 address on the router as 209.65.1.2 (*Inside Global*), then sends the packet to the destination server.
4. The *Public Server* will see the source IPv4 address of the packet as 209.65.1.2 (router) but not *PC 1* because NAT allows the private network to be hidden behind the public IPv4 address of the router.

Advantages of using NAT on a network:

- It helps conserve the public IPv4 address space by allowing organizations to use private IPv4 addresses on their internal networks. NAT allows private IPv4 addresses to be translated to a public IPv4 address.
- It allows an entire organization's private network to be hidden behind a single public IPv4 address.
- Since private IPv4 addresses are non-routable on the internet, organizations can use any private IPv4 address blocks on their private, internal networks.

Disadvantages of NAT:

- Network performance is affected. As traffic is sent to the router or modem to be translated before it is placed on the network, there is some delay as the router or modem has to perform the actual translation process.
- Since NAT modifies the IPv4 addresses on the packet, **Virtual Private Network** (**VPN**) solutions that use **IP security** (**IPsec**) to establish a secure logical tunnel over an unsecure network does not work well.
- End-to-end connectivity is lost between a sender and receiver. This makes it difficult for a receiver to determine the true source of a message.

The following are the three common types of NAT:

- Static NAT
- Dynamic NAT
- Port address translation (PAT)

Static NAT

- It allows network professionals to create a one-to-one mapping a private IPv4 address on an internal server to the public IPv4 address on the router/modem internet-facing interface.

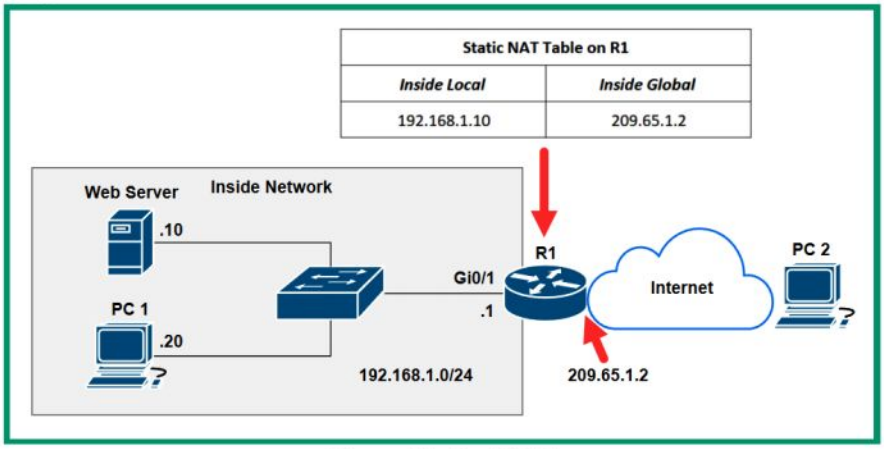


Fig. – Static NAT

- It creates a one-to-one mapping between the private IPv4 address of the server (192.168.1.10) and the public IPv4 address on the router (209.65.1.2).
- Therefore, whenever a device on the internet such as *PC 2* connects to the public IPv4 address of 209.65.1.2, the router will forward all packets to 192.168.1.10, the internal web server.
- The user on the internet, *PC 2*, will not see the private IPv4 address on the internal network because it's being hidden behind the public IPv4 address on the router.

Dynamic NAT

- It allows network professionals to create a many-to-many mapping between multiple private IPv4 addresses and public IPv4 addresses address.

- In dynamic NAT, a pool of public IPv4 addresses is assigned to the private IPv4 addresses on a first come, first served basis.
- If there are six public IPv4 addresses within the pool, and there are 50 devices on the internal network, only a maximum of six devices can use the available public IPv4 addresses at a time.
- If a seventh device wants to communicate over the internet while the pool is exhausted, the seventh device will need to wait until one of the public IP addresses is made available by the router.

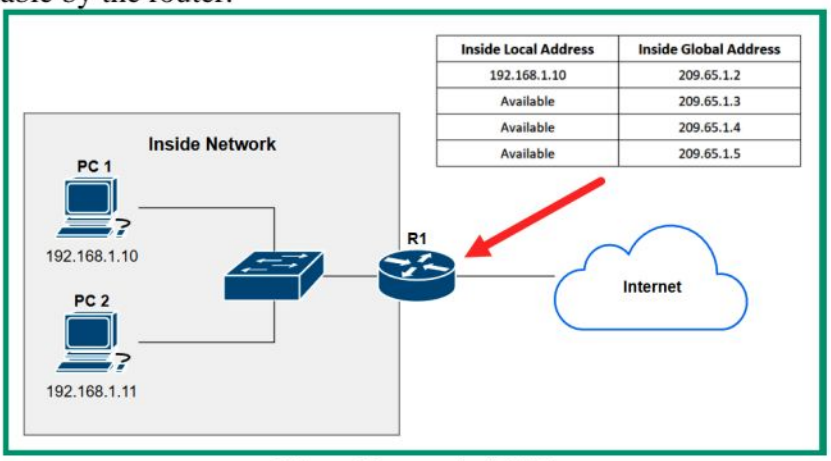


Fig. – Dynamic NAT

- When *PC 1* wants to communicate with a device on the internet, the router will check the NAT pool for an available public IPv4 address to translate the source private IPv4 address into a public address before forwarding the packet to the destination on the internet.
- While *PC 1* is using the 209.65.0.1 address, if another internal device such as *PC 2* wants to communicate with a server on the internet, the same process occurs on the NAT-enabled router and uses the next available public IPv4 address within the pool.
- However, if all addresses within the NAT pool are being used, additional devices on the internal network will need to wait until an address becomes available.

Port address translation (PAT)

- Port address translation (PAT) or NAT overload, is one of the most common types of NAT that is found within many organizations and residential internet subscriber networks.
- It allows organizations and home users to perform a many-to-one translation.
- PAT allows multiple devices with private IPv4 addresses on the internal network to translate their source address to a single public IPv4 address using a NAT-enabled router or modem.
- Using the source and destination service port numbers allows the NAT-enabled router to uniquely identify and track each communication between the private (inside) and public (outside) networks.

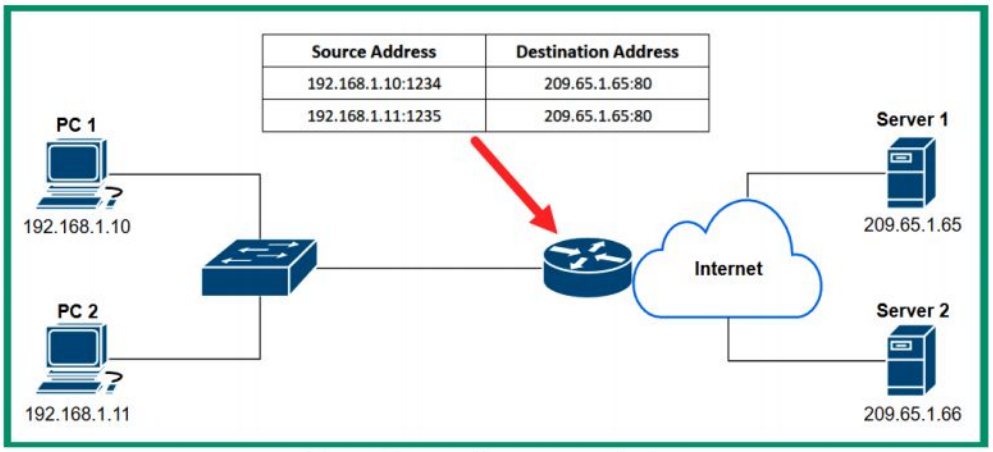


Fig. – Port address translation

- When *PC 1* wants to communicate with *Server 1* on the internet, *PC 1* creates a message to include the source and destination IPv4 addresses and service port numbers.
- When the message arrives at the NAT-enabled router or modem, the router records the source IPv4 address and service port number. Then, it translates the source private IPv4 address to the public IPv4 address while the source service port number remains unchanged.
- The NAT-enabled router keeps track of all translations, so any returning traffic from *Server 1* will be forwarded to *PC 1* only.

Exploring the structure of IPv4 and IPv6

Here you will learn how to convert IPv4 addresses from binary into decimal and vice versa, and explore various address types and their use cases on a network.

Fundamentals of IPv4

- Within an IPv4 address, four octets are separated by a dot (.), and each octet is made up of 8 bits.
- Therefore, 4 octets x 8 bits per octet = 32 bits in length per IPv4 address. The following is an example of an IPv4 address in dotted-decimal and binary notation:

	1st Octet	2nd Octet	3rd Octet	4th Octet
Dotted Decimal	192	168	10	20
Binary	1100 0000	1010 1000	0000 1010	0001 0100

Fig. – IPv4 address format

Converting binary into decimal

Let's take a further look into the format of an IPv4 address with its binary format. Since an IPv4 address is 32 bits in length with four octets, the following is an example of an IPv4 address in binary notation:

11000000.10101000.00000001.10000001

Now let's apply the theory to converting the IPv4 address of 11000000.10101000.00000001 .10000001 into a dotted-decimal notation. To perform this exercise, follow these steps:

1. Let's start with the first octet and place its values within the table, as shown here:

Radix	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	1	1	0	0	0	0	0	0

Fig. – Converting the first octet

2. Using the same principle from the previous step, let's assign the values of the second octet within the positioning system to determine its decimal value:

Radix	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	1	0	1	0	1	0	0	0

Fig. – Converting the second octet

3. Next, let's convert the third octet by placing its bit values within the positioning systems, as shown in the following table:

Radix	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	0	0	0	0	0	0	0	1

Fig. – Converting the third octet

4. Next, let's convert the fourth octet by placing its bit values within the positioning system once more:

Radix	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	1	0	0	0	0	0	0	1

Fig. – Converting the fourth octet

5. The final step is simply putting everything all together: 11000000.10101000.0000000 1.10000001 = 192.168.1.129.

Converting decimal into binary

- Here, you will learn how to use an eight-step method to convert an IPv4 address, 172.19.43.67, from decimal into binary, one octet at a time.
- Let's start by converting the first octet, 172, from decimal into binary.

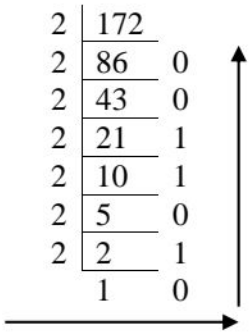


Fig. – Converting 172 into binary

- We get the result as 10101100.
- Similarly, converting the 2nd octet 19 into binary we will get the value 00010011, 3rd octet 43 into binary we will get 00101011 and 4th octet 67 into binary we will get 01000011.

Lastly, let's put everything all together and view the binary notation of 172.19.43.67:

	1st Octet	2nd Octet	3rd Octet	4th Octet
Decimal	172	19	43	67
Binary	10101100	00010011	00101011	01000011

As shown in the preceding table, the IPv4 address is 172.19.43.67 = 10101100.0001001 1.00101011.01000011.

Fundamentals of IPv6

An IPv6 address consists of 128 bits in length and is written in hexadecimal notation. Hexadecimal contains both numbers and letters in the following range:

0 1 2 3 4 5 6 7 8 9 A B C D E F

This 128-bit address allows IPv6 to scale to 2128 IPv6 addresses, which allows 3.4 x 1038 IPv6 addresses that can be uniquely assigned to devices.
Each IPv6 address is made up of 128 bits that are grouped into eight (8) hextets. Each hextet contains 16 bits, so 8 hextets x 16 bits per hextet = 128 bits in length per IPv6 address.

The following is an example of an IPv6 address:

2001:0DB8:0000:1111:0000:0000:0000:0200

Let's break down the following IPv6 address into a more simplified version:

First, all leading 0s in a hextet can be removed.
When there are two or more hextets that are all zeros, a double colon (::) is used to replace the consecutive zeros within the IPv6 address.
The following is a simplified version of the original IPv6 address:

2001:DB8:0:1111:0:0:0:200

Then, replace consecutive zero-only hextets with a double colon (::). The following is a further simplified version:
2001:DB8:0:1111::200

The default subnet mask or prefix length of an IPv6 address is /64. This means the first 64 bits of the IPv6 address represent the network portion of the address and the second portion represents the interface ID.

The following diagram shows the parts of an IPv6 address:

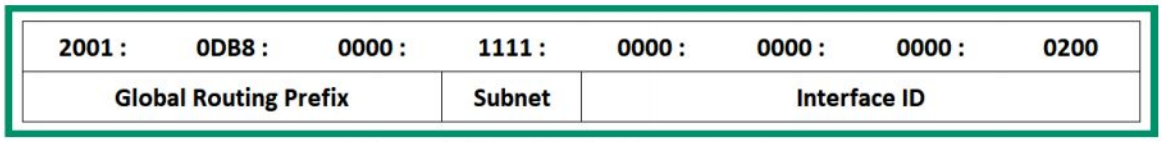


Figure 4.22 – IPv6 address structure

- The first three hextets represent the **Global Routing Prefix** portion, which contains the first 48 bits of the address. This portion of the IPv6 address is assigned by the service provider such as the ISP.
- The fourth hextet (16 bits) represents the **Subnet** ID, which is used by the ISP to create subnetworks of the network block.
- The last 64 bits represent the **Interface ID** portion. Combining the Global Routing Prefix, Subnet ID, and Interface ID, a client is assigned a unique 128-bit IPv6 address on its network interface card.

Types of IPv4 and IPv6 addresses

There are various types of IPv4 and IPv6 addresses and it's important to understand them as an aspiring network professional.

Automatic Private IP Addressing (APIPA)

What if a computer connects to a network and does not receive an IP address? What happens?

There are many reasons a client device may not receive an IP address from the network, as follows:

• The client is unable to communicate with the DHCP server on the network
• The client is configured to use a static IP address that does not change
• The DHCP server is not present or offline on the network

- By default, many client devices are configured to automatically communicate with a DHCP server and receive an IP address from it.
- However, if a client is unable to reach the DHCP server on the network, the client will automatically assign itself a special unique IPv4 address ranging from 169.254.0.1 to 169.254.255.254 with a default subnet mask of 255.255.0.0. This is a feature known as Automatic Private IP Addressing (APIPA), which is built into many operating systems such as Microsoft Windows.

Important note

On an IPv4 network, the APIPA address is sometimes referred to as an IPv4 **Link-Local** address. However, APIPA is a Microsoft-specific term for "Link-Local," which is preferred for Linux-based operating systems.

Extended unique identifier (EUI-64)

- On some IPv6 networks, a stateless IPv6 technology known as **Stateless Address Autoconfiguration** (**SLAAC**) is implemented that helps clients obtain global unicast IPv6 addresses on the network.
- One of the main differences between SLAAC and DHCPv6 is that SLAAC does not keep a record of each client's IPv6 address assignment or details.
- It provides the network portion of the IPv6 address to the client – that is, the first 64 bits of the IPv6 address.
- The client uses a process known as **Extended Unique Identifier 64** (**EUI-64**) to convert its 48-bit **Media Access Control** (**MAC**) address into a 64-bit address, which will become the Interface ID portion of the IPv6 address.

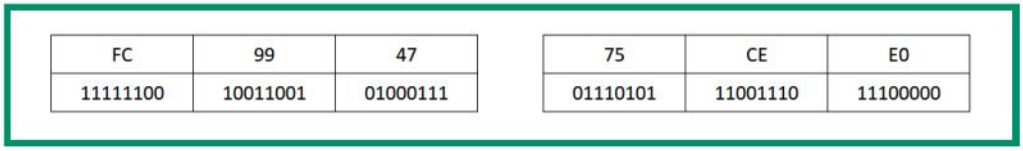
- This allows the client to combine the 64-bit network prefix and the newly created EUI-64 address to create the 128-bit IPv6 address for the network adapter.
- Let's imagine a computer is connected to an IPv6 network and is seeking a DHCPv6 server.

1. However, SLAAC is enabled on the network and provides the client with 2001:DB8:0:1111::/64, the network portion of the IPv6 address for its network adapter.

- The 48-bit MAC address is used on the computer's network adapter and the EUI-64 process is used to create the 64-bit interface ID portion of a 128-bit IPv6 address.

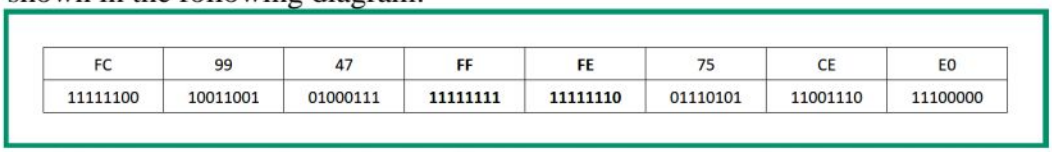
The following steps describe the EUI-64 process of converting a 48-bit MAC address of a network adapter to create a 64-bit address that will be used as the interface ID portion to create a unique IPv6 address:

1. First, split the 48-bit MAC address into half, separating the **Organizational Unique Identifier** (**OUI**) and the device portions, as shown in the following diagram:



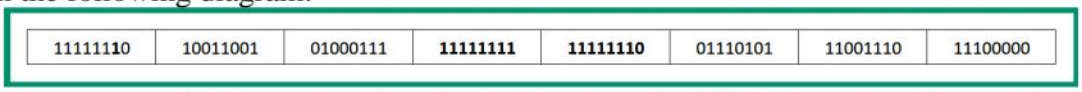
FC	99	47	75	CE	E0
11111100	10011001	01000111	01110101	11001110	11100000

2. Next, insert the hexadecimal value, FFFE, in the middle of the 48-bit MAC address, as shown in the following diagram:



FC	99	47	**FF**	**FE**	75	CE	E0
11111100	10011001	01000111	**11111111**	**11111110**	01110101	11001110	11100000

3. Next, flip the seventh bit within the first byte so that a 0 will become a 1 or a 1 will become a
   0. This bit indicates if the NIC is administered locally (0) or is globally unique (1), as shown
   in the following diagram:



11111**1**10	10011001	01000111	**11111111**	**11111110**	01110101	11001110	11100000

4. Next, convert the binary into hexadecimal to view the EUI-64 portion of the address, as shown in the following diagram:

FE	99	47	**FF**	**FE**	75	CE	E0

5. Lastly, putting it all together, the EUI-64 bit IPv6 address that will be assigned to the device's
   network adapter is 2001:DB8:0:1111:FE99:47FF:FE75:CEE0.

Unicast

- It can be IPv4 and IPv6 address which is uniquely assigned to the network adapter of a device.
- It allows **one-to-one** communication between a sender and receiver device over a network.
- The following diagram shows an example of a unicast network transmission between two devices:

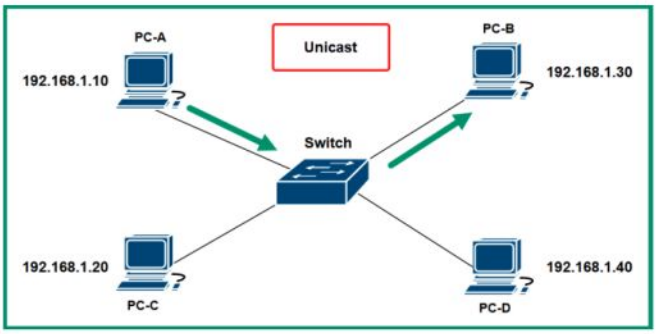


Fig. – Unicast communication

Multicast

- It exists within both the IPv4 and IPv6 address spaces.
- It allows **one-to-many** communication between devices on a network.
- Enterprise-grade routers within a large organization are usually configured with a dynamic routing protocol, which allows each router to automatically learn new networks and maintain an up-to-date routing table by exchanging routing information between themselves.
- These routers send and receive messages to a multicast address group, which is only used by devices running the same dynamic routing protocol.

The following diagram shows an example of multicast transmission over a network:

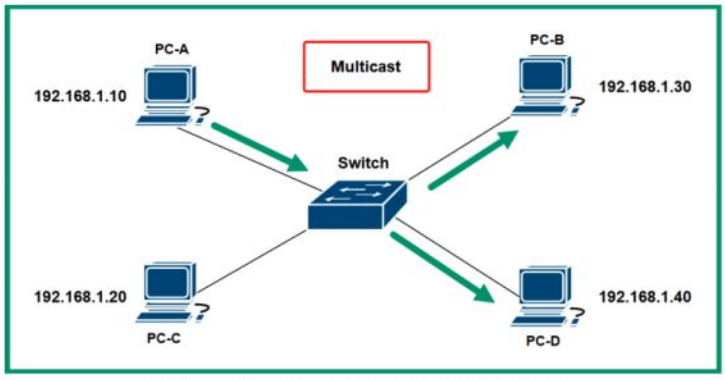


Fig. – Multicast communication

Broadcast

- It allows **one-to-all** communication over an IPv4 network.
- It is only applicable to IPV4 addresses.
- A computer that's connected to a network can send a single message to the network's broadcast address, which allows all devices within the same IP network to receive the message from the sender.
- Within a network that uses a Network ID of 192.168.1.0 and has a subnet mask of 255.255.255.0, the broadcast IP address will be 192.168.1.255.

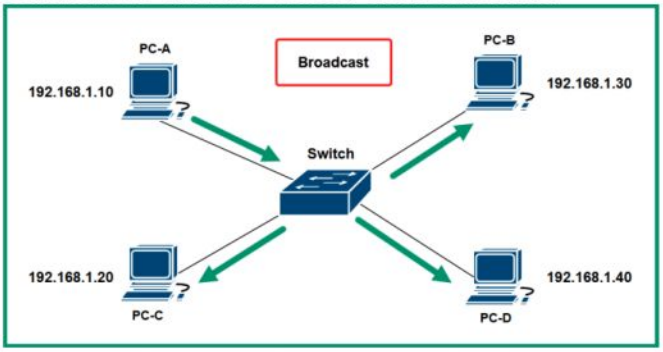


Fig. – Broadcast communication

Anycast

- These are used for **one-to-nearest** communication between devices over a network.
- It is only applicable only to IPV6 addresses.
- It allows the same unicast IPv6 address to be shared between multiple devices, such as servers on the internet.
- When a client such as a computer sends a message to an anycast IPv6 address, the message is delivered to the geographically nearest server that's configured with the anycast address.

Delving into IPv6 concepts

- To help ensure devices that exist on both IPv4 and IPv6 networks can communicate with each other, various IPv6 technologies allow both versions of IP to coexist.

Tunneling

- It allows IPv6 packets to be transported over an IPv4 network.
- The forwarding router is responsible for encapsulating the IPv6 packet inside an IPv4 packet before sending it over the IPv4 network.
- This type of tunneling is referred to as 6to4 tunneling.
- 4to6 tunneling allows an IPv4 packet to be encapsulated within an IPv6 packet so that it can be transported over an IPv6 network.

Dual stack

- Dual stacking both IPv4 and IPv6 addresses on the same NIC of an end device or interface of a networking device such as a router will allow the device to communicate efficiently on both IPv4 and IPv6 networks.
- If the device has sent a message to a host on an IPv4 network, it will use the IPv4 address that's configured on its local NIC or interface.
- If the device has to send a message to a host on an IPv6 network, it will use the IPv6 address that's configured on the local NIC or interface.

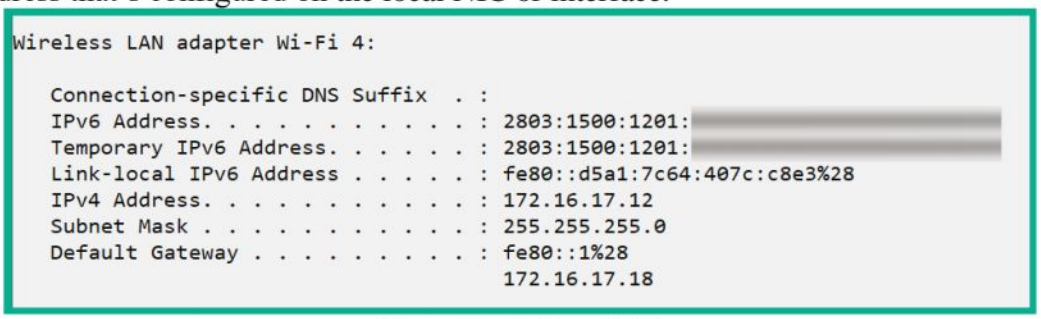


Fig. – Dual stack NIC

Translation

- **Network Address Translation 64 (NAT64)** allows devices within an IPv6 network to communicate with hosts on an IPv4 network using an address translation.
- NAT64 is configured on routers to translate IPv6 addresses into IPv4 addresses, which allows IPv6-enabled devices to communicate with IPv4 hosts and vice versa.

Router advertisement

- Devices on an IPv6 network automatically obtain a GUA IPv6 address using ICMPv6 messages.

- Whenever an IPv6-enabled device such as a computer is connected to an IPv6 network, it sends a Router Solicitation (RS) message to the network to discover any IPv6 routers.
- An IPv6-enabled router responds with a Router Advertisement (RA) message, which is used to inform the host on the network how to obtain a GUA IPv6 address.

Furthermore, the RA message provides the following network information to the client:

- The network prefix and the prefix length of the address
- The default gateway IPv6 address for the network
- The DNS server IP addresses and domain name

Additionally, the RA messages provide the following methods for configuring a GUA IPv6 address for a client on the network:

- Stateless Address Autoconfiguration (SLAAC)
- SLAAC with stateless DHCPv6
- Stateful DHCPv6

Stateless Address Autoconfiguration (SLAAC)

- It allows devices on a network to be configured with a GUA IPv6 address without the need for a Dynamic Host Configuration Protocol v6 (DHCPv6) server.
- The following is the process of a client obtaining a GUA IPv6 address using SLAAC on an IPv6 network:

  1. A client on the network sends an RS message to seek any IPv6-enabled routers.
  2. The IPv6-enabled router responds with an ICMPv6 RA message and provides the network prefix and the prefix length.

2. The client uses the EUI-64 process to convert its 48-bit MAC address on the local NIC to create a 64-bit Interface ID. The 64-bit Interface ID is appended to the end of the 64-bit network prefix to create a 128-bit GUA IPv6 address for the client.

SLAAC with stateless DHCPv6

- Additionally, the RA message from the router can indicate to the client to use both SLAAC and stateless DHCPv6 to obtain a GUA IPv6 address. In this situation, the RA messages inform the client device of the following instructions:

  1. First, use SLAAC to create its own GUA IPv6 address.
  2. Second, use the router's IPv6 Link-Local address as the default gateway for the network. The router's IPv6 Link-Local addresses are set as the source addresses within the RA message from the router to the client.
  3. Lastly, use the stateless DHCPv6 server to obtain the DNS server addresses and domain names only. The stateless DHCPv6 server does not provide the IPv6 address, prefix length, or the default gateway.

Stateful DHCPv6

A stateful DHCPv6 server has similar functionalities to a traditional DHCP server on an IPv4 network as it provides the following configurations to clients:

- GUA IPv6 address
- Prefix length
- DNS server addresses
- Domain name

While using a stateful DHCPv6 server on a network, the RA messages from the router provide the default gateway address to clients. The router's IPv6 Link-Local address is included within the RA message as the source address.

Applied IPv4 Subnetting

Understanding the purpose of the subnet mask

- Both IPv4 and IPv6 addresses have an accompanying subnet mask.
- It helps a sender device determine whether to forward a message to the default gateway or not.

The following are the important key characteristics of the subnet mask and its responsibilities:

- It has the same length as an IPv4 address, i.e., 32 bits in IPV4 and 128 bits in IPV6.
- It is used with an IPv4 or IPv6 address to help devices identify the network and host portions of the IP address.
- It is used to help network professionals to determine the total number of IP addresses and usable (assignable) addresses within an IP network.
- It determines whether the destination host is on the same IP network as the sender or on another network. If the destination host is on another IP subnet, the sender forwards the message to the sender's default gateway.

Default subnet mask for each class of IPv4 addresses on both a private and public network:

Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Fig. – Default subnet masks

Delving into network prefixes and subnet masks

- The /x value that's appended to the end of the IP address is referred to as the network prefix and represents the subnet mask in a simplified format.
- The x value is calculated based on the total number of bits, which are 1s within the subnet mask of the IPv4 or IPv6 address.

The following table shows the binary notation of each default class of subnet mask:

Class A - 255.0.0.0	11111111	00000000	00000000	00000000
Class B - 255.255.0.0	11111111	11111111	00000000	00000000
Class C - 255.255.255.0	11111111	11111111	11111111	00000000

Fig. – Subnet masks

The following are the network prefixes for each default subnet mask:

- **Class A**: 255.0.0.0 - /8
- **Class B**: 255.255.0.0 - /16
- **Class C**: 255.255.255.0 - /24

- The **network portion** of the IP address is the same for all devices within the same IP network, while the **host portion** of the IP address is unique to the interface of the end device only.
- To determine the network and host portion of an IP address, you can simply convert both the IP address and subnet mask into binary notation, as shown in the following table:

10.0.0.0	00001010	00000000	00000000	00000000
255.0.0.0	11111111	00000000	00000000	00000000

Fig. – network ID of Class A

Placing a dotted line after the last 1 within the subnet mask will identify the network and host portions of both IPv4 and IPv6 addresses.

- Similarly, we can find out for class B and class C.

We will commonly discover networks are using custom subnet masks such as 255.255.224.0. To calculate the network prefix, convert each octet from decimal into binary, as shown in the following steps:

1. Converting the first octet, 255, into binary will be 11111111.
2. Converting the second octet, 255, into binary will be 11111111.
3. Converting the third octet, 224, into binary will be 1110000.
4. Converting the fourth octet, 0, into binary will be 0000000.
5. Lastly, calculating the sum of all bits that are 1s from each octet will provide a network prefix of /19.

The following table shows a classless IPv4 address with a custom subnet mask:

192.168.1.54	11000000	10101000	00000001	0011 0110
255.255.255.240	11111111	11111111	11111111	1111 0000

Fig. – Custom subnet mask

Determining the network ID

It's important to understand how to identify whether devices are on the same IP network or not. Let's take a look at the following network topology, which contains a computer, a switch, and a router:

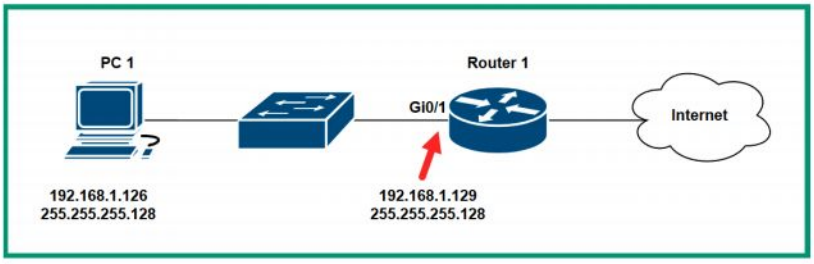


Fig. – Network topology

- As shown in the preceding diagram, there's a small network that contains a computer with a label of **PC 1** that has an IPv4 address of 192.168.1.126 that uses a custom subnet mask of 255.255.255.128.
- There's a router as the default gateway that provides access to the internet, which is configured using an IPv4 address of 192.168.1.129 with a custom subnet mask of 255.255.255.128.
- The computer is connected to the same physical network as the router. If the computer has to send a message to a host on the internet, the computer forwards the traffic to its default gateway on the network.

- It seems Router1 and PC1 are on the same IPv4 network. Actually, these two devices are not on the same IP network and won't be able to communicate with each other.

- We need to calculate the network IDs of each device. The **network ID** allows network professionals to identify which IP network a host belongs to.

- While devices within an organization are all interconnected to the same physical network, network professionals create unique IP subnetworks (subnets) where each subnet has a network ID, a range of usable IP addresses, and a broadcast address.

- To determine the network ID of a host use a logical operation known as **ANDing**. The process of ANDing allows a system to accept two input values and provide a single output. The following are the laws of ANDing:

  0 AND 0 = 0
  0 AND 1 = 0
  1 AND 0 = 0
  1 AND 1 = 1

- Network professionals AND the IP address of a device against the subnet mask, the result of which is the network ID. Let's determine whether the computer and router are on the same IP subnet by following these steps:

- First, let's convert the IPv4 address and the subnet mask of the computer into binary notation, then use the laws of ANDing to determine the network ID of the computer:

IP address	**11000000.10101000.00000001.01111110**
Subnet mask	**11111111.11111111.11111111.10000000**
Network ID	**11000000.10101000.00000001.00000000**

Fig. – PC 1's Network ID

- Next, let's covert the IPv4 and subnet mask of the router into binary notation and use the laws of ANDing to determine the network ID, as follows:

IP address	**11000000.10101000.00000001.10000001**
Subnet mask	**11111111.11111111.11111111.10000000**
Network ID	**11000000.10101000.00000001.10000000**

Fig. – The router's network ID

- Lastly, let's compare the network IDs of both PC 1 and the router. PC 1 has a network ID of 192.168.1.0/25 and the router has a network ID of 192.168.1.128/25. Since these network IDs are not the same, this means PC 1 and the router are not on the same IP subnet.

- Therefore, they will not be able to communicate with each other, even though they are connected to the same physical network.

Understanding the importance of subnetting

- Using classful addressing with default subnet masks isn't the most suitable solution in some cases.
- Using a classless addressing scheme allows network professionals to create smaller networks with custom subnet masks with fewer usable IP addresses to avoid wastage by using a technique known as **subnetting**.
- Subnetting provides the following benefits to organizations and network professionals:
    - To efficiently distribute IP addresses with the least wastage
    - To create more networks with smaller broadcast domains
- A large broadcast domain within an organization can affect the performance of the network.
- Each time a device sends a broadcast message, it's propagated throughout the entire network and all devices receive a copy of the message and process it. If more devices are generating broadcast messages on the network at the same time, these messages will saturate the available bandwidth on the physical network, causing other traffic types such as voice and video to be discarded.
- Voice and video traffic types use **User Datagram Protocol** (**UDP**) as their preferred transport layer protocol as UDP is better for time-sensitive applications. However, since UDP does not provide reliability or guarantee of delivery, UDP traffic is most likely to be discarded when the network becomes saturated.
- To reduce the size of a broadcast domain, subnetting allows network professionals to create smaller IP networks to support fewer devices. For example, while all devices are interconnected to the same physical network within an organization, a network professional can create a unique subnet for each department within the company such that the human resource team will be on a unique IP subnet and the accounting team will be on another IP subnet.
- If a device within the human resources team is generating broadcast messages, it's limited to the human resources IP subnet and will not propagate to another IP subnet within the organization. Therefore, other departments will not be affected and the broadcast messages are contained while improving the performance of the entire network.

IPv4 subnetting and VLSM

Let's imagine you're the network administrator for an organization that has a total of four offices that are interconnected using a Wide Area Network (WAN) solution, as shown in the following network topology:

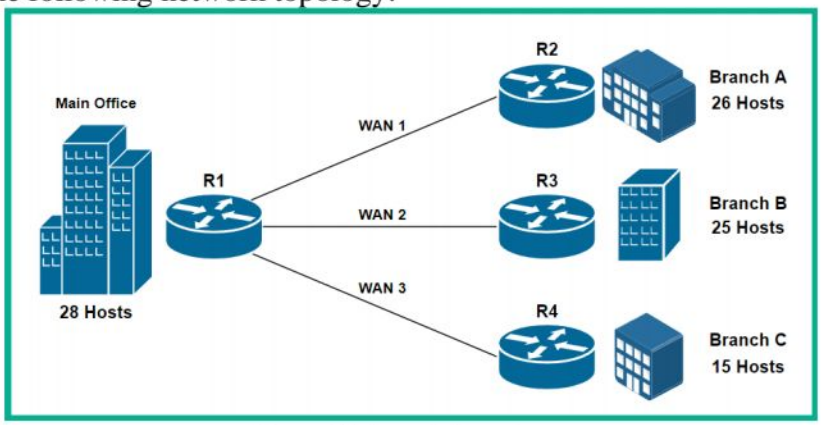


Fig. – Network topology

Your objective is to create an IPv4 addressing scheme for the entire organization, ensuring each office location has an IP subnet and that there's the least wastage of IP addresses per subnet. The following sub-sections will guide you through the process of subnetting.

Step 1 – determining the appropriate IPv4 block

You will need to determine the total number of networks within the organization and the size of the largest network. It helps you choose an appropriate address class for the organization.

Class C = 28 – 2 = 254 usable IP addresses

Scenario

- **Main Office LAN**: 28 hosts
- **Branch A LAN**: 26 hosts
- **Branch B LAN**: 25 hosts
- **Branch C LAN**: 15 hosts
- **WAN 1 (R1-R2)**: 2 IPs are needed
- **WAN 2 (R2-R3)**: 2 IPs are needed
- **WAN 3 (R3-R4)**: 2 IPs are needed

Class C address block will be appropriate for the organization.

Step 2 – creating new subnets (subnetworks)

- To create new subnets from an address block, you will need to convert some of the host bits into new network bits. This allows us to create more networks while reducing the number of IPv4 addresses that are available within each subnet.

- Let's get started by using the first available Class C address block of 192.168.0.0/24 and converting both the address and default subnet mask into binary notation, as shown in the following table:

Network block	11000000 . 10101000 . 00000000 . 00000000
Subnet mask	11111111 . 11111111 . 11111111 . 00000000

- The first 24 bits represent the network portion and the last 8 bits represent the host portion of the number. This means that all hosts within the 192.168.0.0/24 network will have the same network portion of the IPv4 address, while the host portion will be unique to the individual host device on the network.
- To create subnetworks from a network block, you will need to convert host bits into network bits. When converting host bits into network bits, the following formula is used to determine the number of new networks:

  Number of networks = 2^N where the *N*th value represents the number of host bits that are converted into network bits.

  Number of networks = 2^N
  = 23
  = 2 x 2 x 2
  = 8

- Converting three host bits into network bits will provide eight new subnetworks which will be sufficient as we need 7 networks.

Network block	11000000 . 10101000 . 00000000 . 00000000
Subnet mask	11111111 . 11111111 . 11111111 . 11100000

Fig. – Remaining host bits

- To determine whether each of the eight new subnets will be able to support the largest network within the organization of 28 hosts, we need to calculate the total number of usable IPv4 addresses per network using the following formula:

Usable IPv4 address = $2^H - 2$
= 25 – 2
= (2 x 2 x 2 x 2 x 2) – 2
= 30

- Based on the results, each of the eight new subnets will contain 30 usable IPv4 addresses that can be assigned to devices. As a result, we have found a workable solution of using a Class C address block and using mathematical calculations to determine whether it's suitable for the organization.
- By changing the new network bits from 0s to 1s within the IP address, we can create all the possibilities for new network IDs. The following are the calculations for creating the eight new subnets:

Subnet 1	11000000 . 10101000 . 00000000 . 00000000	192.168.0.0/27
Subnet 2	11000000 . 10101000 . 00000000 . 00100000	192.168.0.32/27
Subnet 3	11000000 . 10101000 . 00000000 . 01000000	192.168.0.64/27
Subnet 4	11000000 . 10101000 . 00000000 . 01100000	192.168.0.96/27
Subnet 5	11000000 . 10101000 . 00000000 . 10000000	192.168.0.128/27
Subnet 6	11000000 . 10101000 . 00000000 . 10100000	192.168.0.160/27
Subnet 7	11000000 . 10101000 . 00000000 . 11000000	192.168.0.192/27
Subnet 8	11000000 . 10101000 . 00000000 . 11100000	192.168.0.224/27

Fig. – New subnets

Step 3 – assigning subnets to each network

In this step, you'll learn how to calculate the IP address ranges for each new subnet by determining the network ID, the first and last usable addresses, and the broadcast address per subnet.

To ensure your calculations are done efficiently, use the following guidelines:

• To determine the first usable IP address within a subnet, use the network ID + 1 formula.

In binary notation, the first bit from the left is set to 1.

• To calculate the broadcast address within a subnet, use the Next network ID – 1 formula.

In binary notation, it's when all the host bits are 1s within the address.

• To calculate the last usable IP address within a subnet, use the Broadcast Address – 1

Using these guidelines, let's calculate the network range of the first subnet and assign it to the main office LAN network:

Subnet 1	**11000000 . 10101000 . 00000000 . 00000000**	**192.168.0.0/27**
First usable IP	**11000000 . 10101000 . 00000000 . 00000001**	**192.168.0.1/27**
Last usable IP	**11000000 . 10101000 . 00000000 . 00011110**	**192.168.0.30/27**
Broadcast	**11000000 . 10101000 . 00000000 . 00011111**	**192.168.0.31/27**

Fig. – Subnet 1 network range

Next, applying the same mathematical technique, let's determine the network range of the next subnet that will be assigned to the Branch A LAN network:

Subnet 2	**11000000 . 10101000 . 00000000 . 00100000**	**192.168.0.32/27**
First usable IP	**11000000 . 10101000 . 00000000 . 00100001**	**192.168.0.33/27**
Last usable IP	**11000000 . 10101000 . 00000000 . 00111110**	**192.168.0.62/27**
Broadcast	**11000000 . 10101000 . 00000000 . 00111111**	**192.168.0.63/27**

Fig. – Subnet 1 network range

Next, applying the same mathematical technique, let's determine the network range of the next subnet that will be assigned to the Branch A LAN network:

Subnet 2	**11000000 . 10101000 . 00000000 . 00100000**	**192.168.0.32/27**
First usable IP	**11000000 . 10101000 . 00000000 . 00100001**	**192.168.0.33/27**
Last usable IP	**11000000 . 10101000 . 00000000 . 00111110**	**192.168.0.62/27**
Broadcast	**11000000 . 10101000 . 00000000 . 00111111**	**192.168.0.63/27**

Fig. – Subnet 2 network range

Next, repeating our technique, let's calculate the network range of the third subnet that will be assigned to the Branch B LAN network:

Subnet 3	**11000000 . 10101000 . 00000000 . 01000000**	**192.168.0.64/27**
First usable IP	**11000000 . 10101000 . 00000000 . 01000001**	**192.168.0.65/27**
Last usable IP	**11000000 . 10101000 . 00000000 . 01011110**	**192.168.0.94/27**
Broadcast	**11000000 . 10101000 . 00000000 . 01011111**	**192.168.0.95/27**

Fig. – Subnet 3 network range

Next, let's determine the network range of the fourth subnet that will be assigned to the Branch C LAN network:

Subnet 4	**11000000 . 10101000 . 00000000 . 01100000**	**192.168.0.96/27**
First usable IP	**11000000 . 10101000 . 00000000 . 01100001**	**192.168.0.97/27**
Last usable IP	**11000000 . 10101000 . 00000000 . 01111110**	**192.168.0.126/27**
Broadcast	**11000000 . 10101000 . 00000000 . 01111111**	**192.168.0.127/27**

Fig. – Subnet 4 network range

Three WAN networks are used to interconnect each branch router to the main office router. These WAN links are point-to-point connections that require only two IP addresses per WAN connection:

- **WAN 1**: Main office router to Branch A router – only two IP addresses are needed
- **WAN 2**: Main office router to Branch B router – only two IP addresses are needed
- **WAN 3**: Main office router to Branch C router – only two IP addresses are needed

- If we were to assign the remaining subnets to any of the WAN networks, there will be a lot of wastage of IPv4 addresses. Since each subnet has 30 usable IPv4 addresses and each WAN link requires only two IP addresses, there will be a wastage of 28 IPv4 addresses per WAN link.
- To further avoid wastage of IPv4 addresses within our new subnets while being able to assign IPv4 addresses to our WAN networks, we can use a technique known as **Variable Length Subnet Masking** (**VLSM**), which allows us to further break down a subnet into smaller subnetworks.
- Think of it as subnetting a subnet even further to reduce IPv4 address wastage on a network. We can use any of the remaining following subnets for VLSM:

Subnet 5	**11000000 . 10101000 . 00000000 . 10000000**	**192.168.0.128/27**
Subnet 6	**11000000 . 10101000 . 00000000 . 10100000**	**192.168.0.160/27**
Subnet 7	**11000000 . 10101000 . 00000000 . 11000000**	**192.168.0.192/27**
Subnet 8	**11000000 . 10101000 . 00000000 . 11100000**	**192.168.0.224/27**

Fig. – Unallocated networks

Since these unallocated subnets are equal in size, we can use any one of these remaining subnets to perform our VLSM technique. To keep everything simple and easy to understand, the following subnets will be documented and reserved for future office locations:

Subnet 5	**11000000 . 10101000 . 00000000 . 10000000**	**192.168.0.128/27**
Subnet 6	**11000000 . 10101000 . 00000000 . 10100000**	**192.168.0.160/27**
Subnet 7	**11000000 . 10101000 . 00000000 . 11000000**	**192.168.0.192/27**

Fig. – Subnet reservations

The following subnet will be broken down using VLSM to create smaller subnetworks:

Subnet 8	**11000000 . 10101000 . 00000000 . 11100000**	**192.168.0.224/27**

Fig. – Eighth subnet

Step 4 – performing Variable-Length Subnet Masking (VLSM)

- In this step, you will learn how to further break down a subnet to create smaller IP networks with smaller broadcast domains while efficiently distributing IP addresses with the least wastage.
- Since each of the three WAN links are point-to-point networks that require only two IP addresses, we can determine the number of host bits needed within an IP address to provide two usable IP addresses.
- To calculate the number of usable IP addresses within a network, use the following formula:

  Number of usable IPv4 addresses = $2^H - 2$

Number of usable IPv4 addresses = $2^H - 2$
= $2^2 - 2$
= (2 x 2) – 2
= 4 – 2
= 2

- Using two host bits provides two usable addresses. At this point, we have a solution for creating new subnets from the 192.168.0.224/27 network block, which has two usable IP addresses per new subnet.
- The following formula provides the number of new subnets when converting three host bits into network bits:

  Number of networks = 2^N
  = 23
  = 2 x 2 x 2
  = 8

- By creating eight new with two usable addresses, we can assign three of the eight new subnets to the existing WAN links; the remaining subnet can be documented as a reservation for the future growth of the organization.
- The following table shows the effects of converting three host bits within the subnet mask into network bits to create eight new subnets from the 192.168.0.224/27 network block:

Network ID	**11000000 . 10101000 . 00000000 . 11100000**	**192.168.0.224**
Subnet mask	**11111111 . 11111111 . 11111111 . 11111100**	**255.255.255.252**

Fig. – Creating new network bits

- The two host bits are remaining within the host portion of the addresses. These host bits will ensure there are two usable addresses within each of the new subnets.
- The following table shows all the possibilities of modifying the new network bits from the address by changing the 0s to 1s, creating eight new subnets from the 192.168.0.224 network block:

VLSM Subnet 1	**11000000 . 10101000 . 00000000 . 11100000**	**192.168.0.224/30**
VLSM Subnet 2	**11000000 . 10101000 . 00000000 . 11100100**	**192.168.0.228/30**
VLSM Subnet 3	**11000000 . 10101000 . 00000000 . 11101000**	**192.168.0.232/30**
VLSM Subnet 4	**11000000 . 10101000 . 00000000 . 11101100**	**192.168.0.236/30**
VLSM Subnet 5	**11000000 . 10101000 . 00000000 . 11110000**	**192.168.0.240/30**
VLSM Subnet 6	**11000000 . 10101000 . 00000000 . 11110100**	**192.168.0.244/30**
VLSM Subnet 7	**11000000 . 10101000 . 00000000 . 11111000**	**192.168.0.248/30**
VLSM Subnet 8	**11000000 . 10101000 . 00000000 . 11111100**	**192.168.0.252/30**

Fig. – VLSM networks

- The following are the calculations used to determine the network range of the first subnet that will be assigned between the main office router and Branch A router:

Subnet 1	**11000000 . 10101000 . 00000000 . 11100000**	**192.168.0.224/30**
First usable IP	**11000000 . 10101000 . 00000000 . 11100001**	**192.168.0.225/30**
Last usable IP	**11000000 . 10101000 . 00000000 . 11100010**	**192.168.0.226/30**
Broadcast	**11000000 . 10101000 . 00000000 . 11100011**	**192.168.0.227/30**

Fig. – WAN 1 allocation

- The following are the calculations used to determine the network range of the second subnet that will be assigned between the main office router and Branch B router:

Subnet 2	**11000000 . 10101000 . 00000000 . 11100100**	**192.168.0.228/30**
First usable IP	**11000000 . 10101000 . 00000000 . 11100101**	**192.168.0.229/30**
Last usable IP	**11000000 . 10101000 . 00000000 . 11100110**	**192.168.0.230/30**
Broadcast	**11000000 . 10101000 . 00000000 . 11100111**	**192.168.0.231/30**

Fig. – WAN 2 allocation

- The following are the calculations used to determine the network range of the third subnet that will be assigned between the main office router and Branch C router:

Subnet 3	**11000000 . 10101000 . 00000000 . 11101000**	**192.168.0.232/30**
First usable IP	**11000000 . 10101000 . 00000000 . 11101001**	**192.168.0.233/30**
Last usable IP	**11000000 . 10101000 . 00000000 . 11101010**	**192.168.0.234/30**
Broadcast	**11000000 . 10101000 . 00000000 . 11101011**	**192.168.0.235/30**

Fig. – WAN 3 allocation

- The following five subnets will be documented and reserved within the company to support future growth:

VLSM Subnet 4	**11000000 . 10101000 . 00000000 . 11101100**	**192.168.0.236/30**
VLSM Subnet 5	**11000000 . 10101000 . 00000000 . 11110000**	**192.168.0.240/30**
VLSM Subnet 6	**11000000 . 10101000 . 00000000 . 11110100**	**192.168.0.244/30**
VLSM Subnet 7	**11000000 . 10101000 . 00000000 . 11111000**	**192.168.0.248/30**
VLSM Subnet 8	**11000000 . 10101000 . 00000000 . 11111100**	**192.168.0.252/30**

Fig. – Reserved WAN subnets

Exploring Network Protocols and Services

Network protocols

- Network protocols are simply the underlying technology, rules, and procedures that define how a sender can package and format a message to be sent across a network to a destination host.
- Without protocols for communication on a network, devices will not format or address a message properly.
- When the receiver accepts the incoming message, the receiver may misinterpret the message due to a lack of formatting or addressing.
- Each application layer protocol is associated with a unique service port number that helps devices deliver a message to the appropriate application layer protocol.
- These service ports are the doorways used by the operating system of a device to send and receive messages on a network.
- The following table shows the major categories of service numbers and their ranges according to the **Internet Assigned Numbers Authority** (**IANA**):

Port Groups	Range	Description
Well-known Ports	0 - 1,023	Used by common and popular services and applications
Registered Ports	1,024 - 49,151	These ports are assigned to specific entities for use with specific processes and applications
Private/Dynamic Ports	49,152 - 65,535	These are ephemeral ports which are used when a client application is communicating with a server

Fig. – Service port numbers

File protocols

- Within the networking industry, there are various application and network layer protocols that are designed with the functionality to allow file transfer between devices over a network.

File Transfer Protocol

- It is a file sharing protocol that operates in a client-server model, allowing users to connect to a file server to upload and download files over a network.
- It operates on service port 20 to allow data transfer between an FTP client and the FTP server, while service port 21 is dedicated to controlling commands and functions from the FTP client and FTP server.

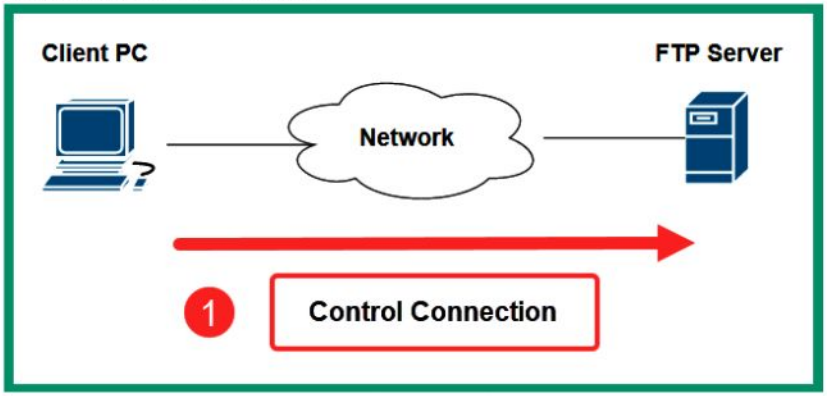


Fig. – Phase 1 of FTP

- As shown in the preceding diagram, the computer with the FTP client application opens the connections to the FTP server on service port 21.
- Next, the client opens another connection to the server on service port 20 to transmit data traffic, as shown in the following diagram:

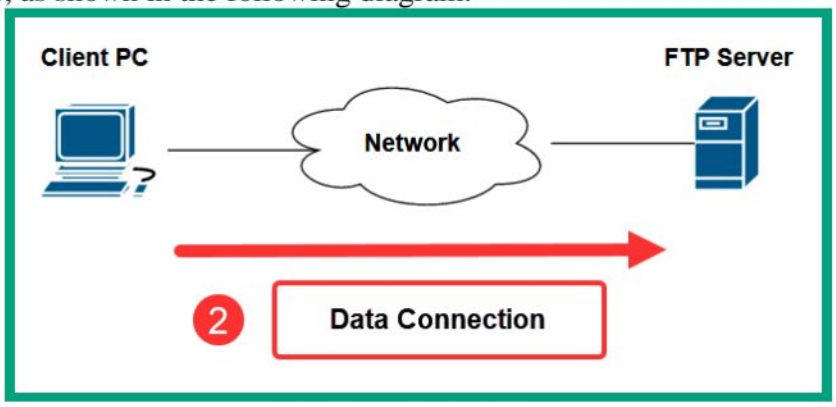


Fig. – Phase 2 of FTP

- Lastly, the data is transferred from the FTP server on service port 20 to the client, as shown in the following diagram:

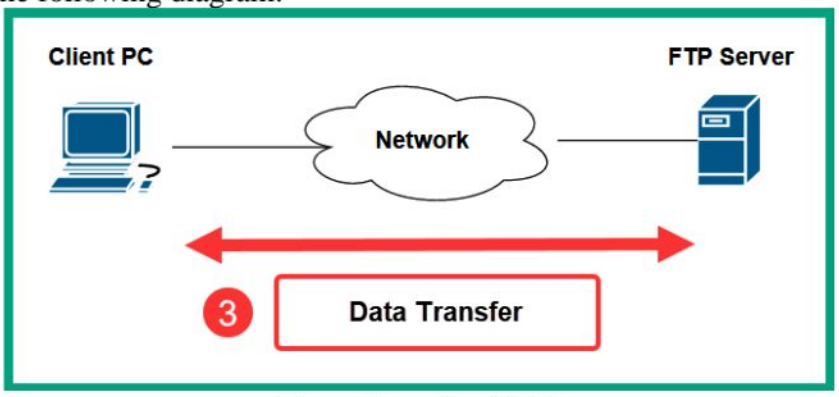


Fig. – Phase 3 of FTP

- Whenever a network professional has to update the firmware of a router or a modem, these networking devices usually support FTP as a method to transfer the firmware from a computer to the modem over a network.
- It does not provide any data encryption and sends the traffic in plaintext. If an attacker can intercept the traffic that's being exchanged between an FTP client and an FTP server, he/she will be able to capture all the data and user credentials that were exchanged between devices. So, FTP is vulnerable to **Man-in-the-Middle** (**MiTM**) attacks.

SSH File Transfer Protocol

- It allows a client to establish an encrypted tunnel using **Secure Shell** (**SSH**) to a file server that supports the SFTP protocol.
- Once the SSH connection is established between the client and server, both devices encapsulate the FTP packets within the SSH tunnel for file transfer over the network.
- The following diagram shows a visual representation of SFTP over a network:

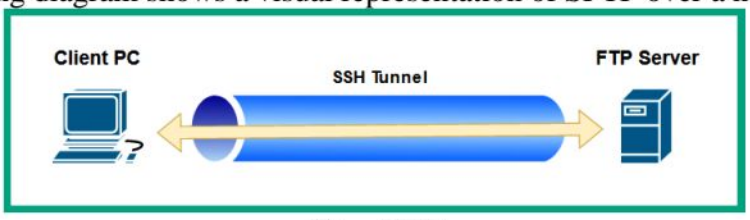


Fig. – SFTP

- As shown in the preceding diagram, the computer establishes an SSH tunnel to the server on port 22 over the network and uses FTP to transfer files within the encrypted SSH tunnel.
- Using SFTP prevents an attacker from identifying any confidential or sensitive data that's being exchanged over a network.
- The attacker will be able to intercept the traffic, but all the packets will be encrypted and the data will be unreadable.

File Transfer Protocol Secure (FTPS)

- It is referred to as **FTP over SSL (FTP/S)**, that allows users to securely transfer files between a client and server over a network. SFTP uses **Secure Sockets Layer (SSL)** or **Transport Layer Security (TLS)** to encrypt the FTP messages that are being sent over the network between a client and server.
- There is no secure connection/tunnel; each FTPS packet is individually encrypted using SSL/TLS. The FTP server will decrypt each FTPS message as they are received from the network and reassemble the messages into data.
- FTPS operates on service port 990 and 21.
- If a client on the network establishes a connection to the server on service port 990, it is considered to be **implicit FTPS**, which indicates the client intends to use SSL. As a result, the SSL handshakes will be exchanged between the client and server immediately.
- If the client establishes a connection to the server on service port 21, it is known as **explicit FTPS**. When using explicit FTPS, the client connects to port 21 on the server and wants to use SSL with the server, additional steps are taken by sending either an AUTH SSL or AUTH TLS command from the client to the server.
- Once the server receives the AUTH SSL or AUTH TLS command from the client over the network, the client and server will begin exchanging SSL handshakes and establish a secure connection.

Trivial FTP

- It is a connectionless, lightweight version of FTP that allows network professionals to quickly upload and download files between a client and networking device over a network.
- Network professionals update the operating systems and firmware of routers/switches to fix any bugs and security issues and improve the stability of the device.
- Enterprise-grade networking devices allow network professionals to configure switches and routers to load their operating systems from a remote TFTP server over a network at the boot time.
- When a networking device is powered on, it will check for a remote TFTP server and download the operating systems over the network and load it into the memory of the router.
- Whenever a newer version of the operating system or firmware is available, network professionals can simply download the newer version and replace the older version on the TFTP server.
- TFTP uses service port 69 by default.

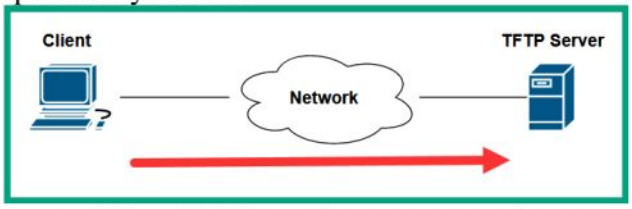


Fig. – TFTP service on a network

- The client is connecting to the TFTP server on its default service port, 69, to upload or download files over the network.
- Being a connectionless protocol, TFTP uses UDP as the preferred Transport layer protocol. So, it is lightweight and does not need acknowledgment messages when sending messages.

Server Message Block

- It is a common protocol that operates in a client-server model, allowing shared network resources such as printers, files, and directories to be shared in a Microsoft Windows environment.
- The following are the three core functions of SMB:
  - Starting, authenticating, and terminating sessions between a client and server
  - Controlling access to files and printers
  - Allowing applications to exchange information between devices on a network

The following diagram shows a visual representation of the client-server model of SMB:

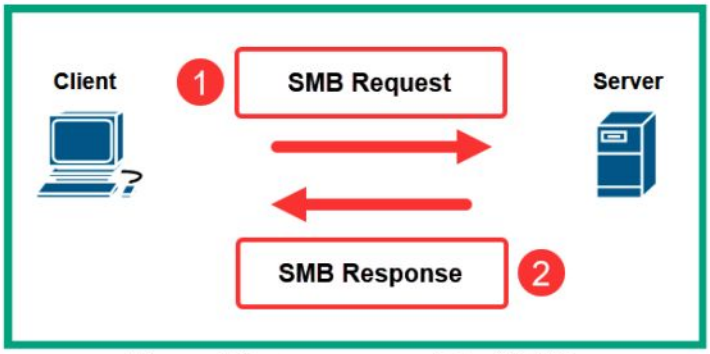


Fig. – Client-server model of SMB

- As shown in the preceding diagram, the client devices send an **SMB Request** to the server to request the shared network resources on the server.
- The server responds with an **SMB Response** to the client, providing requesting additional information for authentication and providing access to the resources.
- The SMB protocols operate on service ports 137 (UDP), 138 (UDP), and 445 (TCP).

SMB - Microsoft Windows environment
SAMBA - Linux-based operating systems
SMB - Apple's macOS

Remote access protocol

- It allows IT professionals to remotely access and manage devices over a network.
- IT professionals usually configure remote management on these devices, which allows them to remotely connect and implement new configurations or perform troubleshooting to resolve any issues.
- If an issue occurs within any part of the network, a network engineer will remotely connect to various networking devices within the service provider's network and perform troubleshooting to resolve the issues.
- It saves a lot of time from physically visiting the location of a server or network device.
- It also provides a security risk if an IT professional is using an unsecure remote access protocol to connect to a networking device.
- Unsecure protocols do not provide security features such as data encryption and sending messages in plaintext, allowing hackers to capture usernames and passwords.

Telnet

- It is an unsecure remote access protocol that allows IT professionals to remotely connect to devices such as computers, servers, networking devices, security appliances, and IoT devices.
- While Telnet is a legacy protocol and should not be used due to security concerns, many organizations still implement Telnet as a remote access protocol on their corporate networks.
- If a hacker retrieves or guesses the correct user credentials for any device, the hacker will be able to access the target device over the internet.
- Telnet uses service port 23 by default.
- Telnet does not provide any data encryption, so it's an unsecure remote access protocol.

Secure Shell

- It is a secure remote access protocol that allows IT professionals to securely connect to devices over a network to perform configuration changes and troubleshooting.
- Unlike Telnet, SSH encrypts all the messages that are exchanged between the client and the device that's running the SSH service, such as the networking device or the server on the network.
- It encrypts all messages, so a hacker can still intercept the communication between a source and destination, but they will not be able to decrypt the message to view the secret data.
- SSH uses service port 22 by default.

Remote Desktop Protocol

- Within a Microsoft Windows environment, IT professionals enable **Remote Desktop Protocol** (**RDP**), a native secure remote access protocol that is built into Microsoft Windows operating systems.
- Using RDP within an organization allows IT professionals to remotely manage Windows servers and desktop devices using a **Graphical User Interface** (**GUI**).
- This differs from SSH and Telnet, which provide a **Command-Line Interface** (**CLI**).
- RDP operates on service port 3389.
- The RDP message is encrypted using TLS, a security protocol that provides data security and privacy on a network.

Email protocols

To ensure emails are transported and delivered over a network, various email protocols help devices format messages for transportation and delivery between a sender and destination address.

Simple Mail Transfer Protocol (SMTP)

The SMTP is an email protocol that is used for sending emails from clients to email servers, and email servers to other email servers. The following process provides an overview of each phase of sending an email between a sender and destination:

1. When a user wants to send an email message to another person, the sender uses an email application such as **Microsoft Outlook** to compose and send the message.
2. The email application on the sender's computer uses SMTP to establish a connection to the sender's email server. When the connection is established, the email application uses SMTP to forward the email message to the sender's email server, which has service port 25 open by default.
3. When the sender's email server receives the email message, it also uses SMTP to forward the email message to the recipient's email server, which has service port 25 open by default.

4. When the email arrives on the recipient's email server, the server uses SMTP to send the message to the email application on the intended recipient's device.

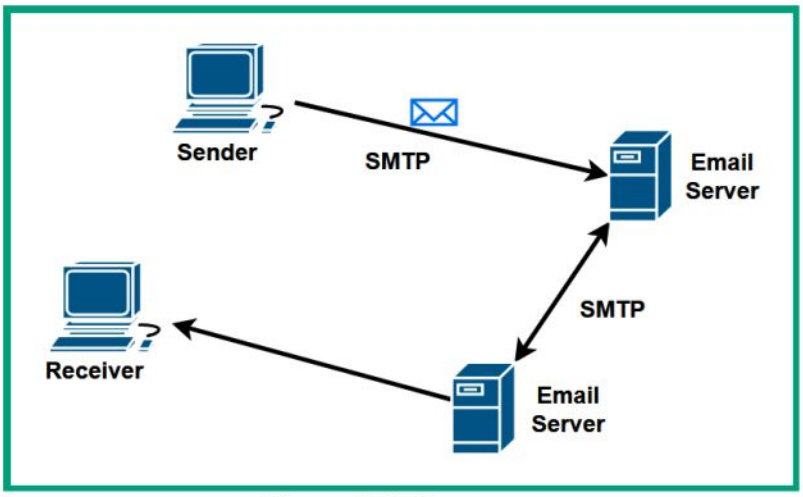


Fig. – SMTP process

Post Office Protocol (POP)

- It allows email clients such as Microsoft Outlook to download messages from email servers over a network.
- It passively listen on TCP service port 110 for inbound requests from email client applications.
- Once a TCP connection is made between the client application and the email server on service port 110, the client downloads the email messages from the mailbox to the client.
- Once the emails have been downloaded, the email messages are deleted from the email server.
- There is no centralized location for storing the messages on a network.
- POP is not recommended for organizations that need a centralized backup solution for their resources.

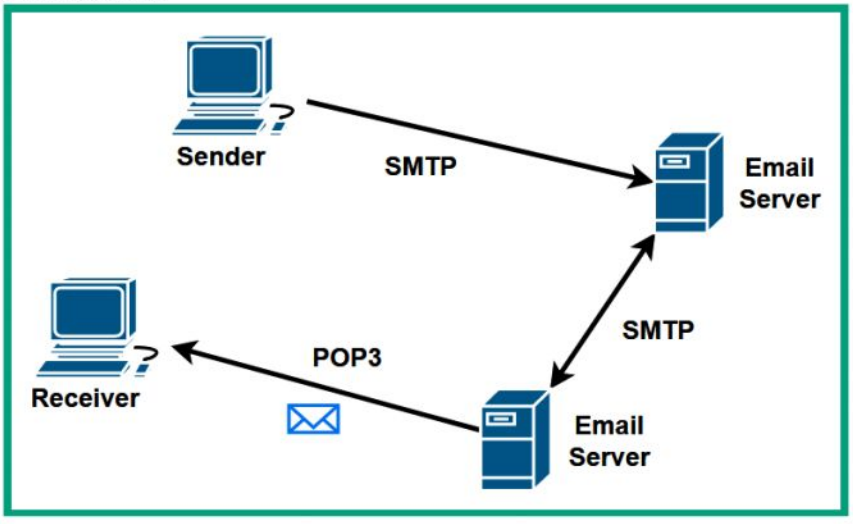


Fig. – POP operations

Internet Message Access Protocol (IMAP)

- It is another common email protocol that allows email clients such as Microsoft Outlook to synchronize the email messages between the client application and email server via service port 143 by default over a network.

- When using IMAP on a network, the email messages are kept on the email server until they are manually deleted or removed from a user's mailbox on the server.

Note

Email protocols such as SMTP, POP, and IMAP do not encrypt the messages and send them in plaintext over a network, so a hacker who is intercepting the messages over a network will be able to view the content of emails exchanged between users.

Simple Mail Transfer Protocol Secure (SMTPS)

It is a secure email protocol that uses TLS to encrypt outbound emails over a network and uses service port number 587 by default.

Post Office Protocol Secure (POPS)

It is a secure email protocol that uses SSL to encrypt the email messages that are being downloaded from an email server to an email application on the client and uses port 995 by default.

Internet Message Access Protocol Secure (IMAPS)

It is a secure email protocol that operates on service port number 993 and uses SSL to encrypt the email messages between the client and server during the synchronization process.

HTTP

When communicating with a web server on a network or the internet, a user will typically open a web browser application on their device that uses HTTP to create a message that is recognizable to the web application running on the web server.

- HTTP is an unsecure protocol that does not provide confidentiality or data privacy and sends messages in plaintext over a network to a web server.
- It uses service port number 80 by default.
- HTTP does not encrypt the messages and sends them in plaintext.

HTTP over SSL (HTTPS),

- It is a secure version of HTTP that establishes a secure connection between the web browser and web server over the network.
- It uses service port number 443 by default.
- HTTPS can use either SSL or TLS when connecting to a web server.

Network protocol types

- Network protocol types are simply the set of rules that are used to describe how a device such as a computer communicates with another device over a network.
- If two devices are used, whether they are the same type of devices or different, both systems need to negotiate on a common set of rules.
- These common rules are referred to as the network protocol type.

Internet Control Message Protocol

- It is defined by RFC 792, which is typically used to provide error reporting on a network.
- Common networking tools such as Ping and Traceroute are built into many operating systems and allow network professionals to invoke ICMP to check end-to-end connectivity between hosts on a network, identify the path a packet is traveling between a source and destination and even measure the latency between hops on a network.
- The following table provides a breakdown of each ICMP type by name, code, and description:

Type	Name	Code
0	Echo Reply	0
3	Destination Unreachable	0 - Nework Unreachable
		1 - Host Unreachable
		2 - Protocol Unreachable
		3 - Port Unreachable
		4 - Fragmentation needed and "Don't Fragment" was set
5	Redirect	0 - Redirect for the Network
		1 - Redirect for the Host
8	Echo Request	0
11	Time Exceeded	0 - Time to Live (TTL) exceeded
		1 - Fragment reassembly time exceeded

Fig. – ICMP codes and types

TCP

Discussed in Chapter-1

UDP

Discussed in Chapter-1

Network services

- These are the services that organizations rely upon each day to ensure their devices can exchange messages over a network.
- Some of these network services help organizations synchronize time on all devices within their network, while other network services provide IP addressing configurations to clients that are connecting to a network.

Network Time Protocol (NTP)

- It is a network protocol that allows IT professionals to configure devices to synchronize their system clock to the same time on a network.
- It operates on a client-server model that uses UDP service port 123 by default.
- Without NTP manually configuring the time on each device can be very time consuming, which can lead to misconfigurations and mismatches in the time set on many devices.
- When time is synchronized on the system clocks on all devices, it ensures all devices have the same time set. This is important for ensuring automated tasks are executed on time and in the proper sequence.
- When a device is generating Syslog messages, it's important to include the time and date in each log message to determine when an event has occurred. Without time synchronization, the time inserted into Syslog messages will not correlate with the events on other networking devices. This will create a challenge for network professionals to determine the actual sequence of events that occurred on the network.
- It is an unsecure protocol that allows hackers to exploit its security vulnerabilities. However, NTP allows authentication between an NTP server and NTP clients over a network.
- The following diagram shows the NTP architecture and hierarchical structure:

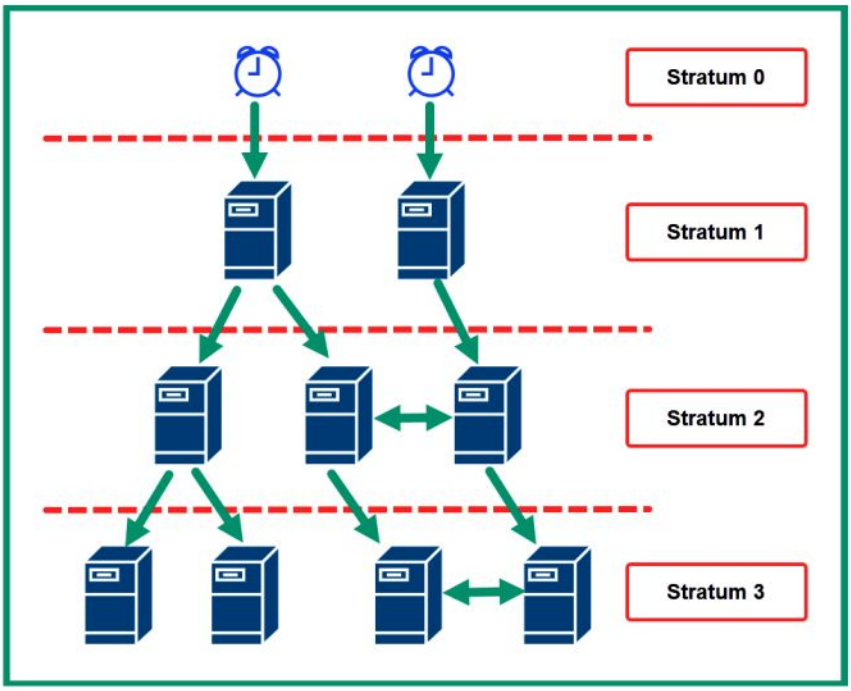


Fig. – NTP hierarchical structure

- It is made up of clients, servers and stratum levels. The NTP servers are devices that provide the time for NTP clients on a network.
- Each stratum level 0 contains the primary time servers and are known as the authoritative sources on the network that have the most accurate time.
- Servers at stratum level 1 synchronize their time clocks with devices on stratum 0, while devices on stratum 2 synchronize their time with those devices on stratum 1 and so on.

Dynamic Host Configuration Protocol (DHCP)

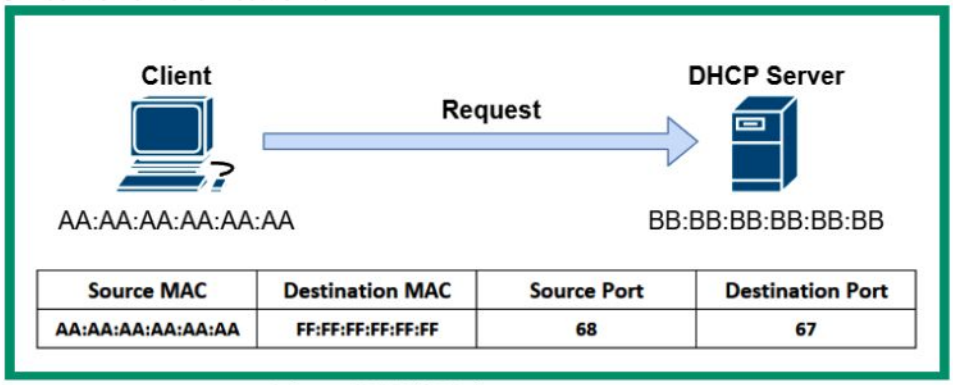
- It is a protocol that allows network professionals to automatically distribute IP addresses to client devices on a network.
- When an end device is connected to a network, it requires an IP address, subnet mask, default gateway address, and Domain Name System (DNS) server address.
- These IP addresses allow the client to communicate with devices on the same network and remote networks.
- Network professionals implement a DHCP server, which allows them to configure the following:

• **Scope**: The range of IP addresses (pool)
• **Exclusion ranges**: The IP addresses that should not be distributed on the network
• **Reservation**: Reserves IP addresses from the pool
• **Dynamic assignment**: Dynamically assigns an IP address to a client on the network
• **Static assignment**: Statically configures an IP address on a client
• **Lease time**: Sets the time that the client can use the IP address given from the DHCP server
• **Scope options**: Additional operations that can be configured when creating the scope
• **Available leases**: Identifies the IP addresses available for lease

- A DHCP client sends a DHCP message from a source service port of 68 and the DHCP server operates on service port 67 by default.

DHCP 4-way handshake Process

1. The client connects to the network and sends a DHCP Discover message, seeking a DHCP server on the network:

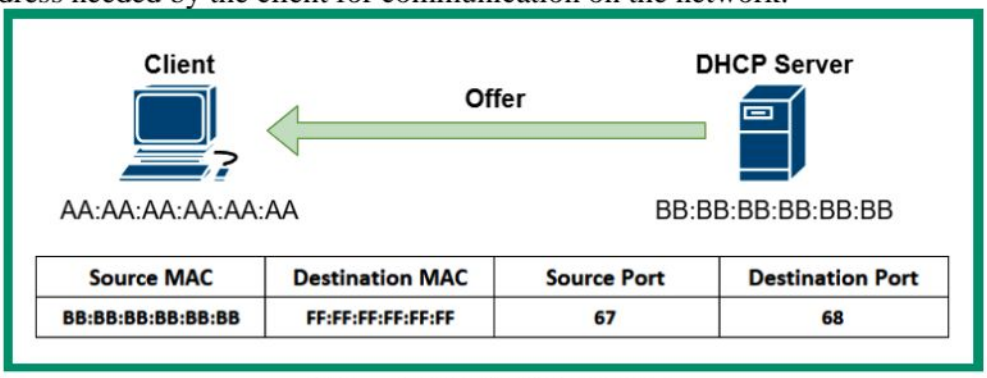


Source MAC	Destination MAC	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	68	67

Fig. – DHCP Discover message

The source IP address on the packet is left blank while the destination IP address is set to 255.255.255.255.

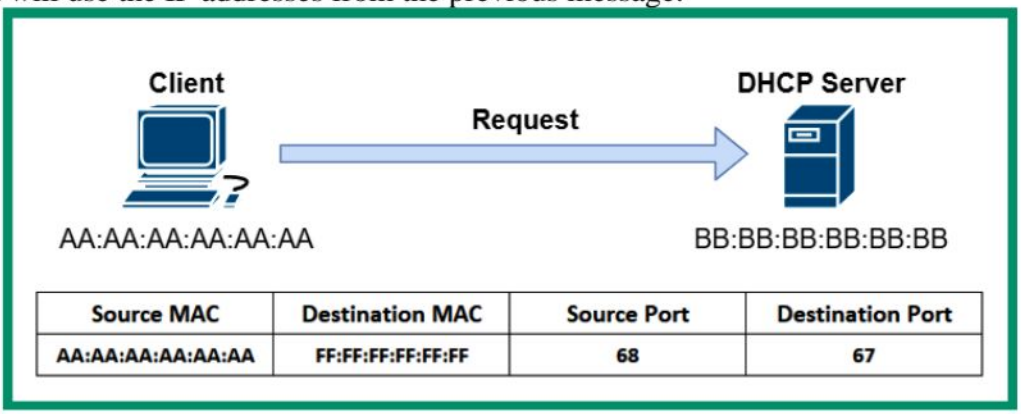
2. Next, the DHCP server responds with a DHCP **Offer** message, which contains the IP address needed by the client for communication on the network:



Source MAC	Destination MAC	Source Port	Destination Port
BB:BB:BB:BB:BB:BB	FF:FF:FF:FF:FF:FF	67	68

Fig. – DHCP Offer message

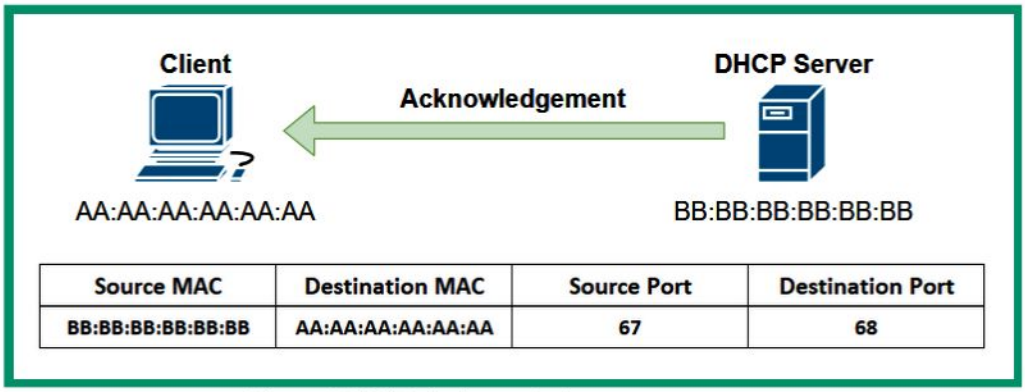
3. Next, the client sends a DHCP **Request** message to the DHCP server, indicating that it will use the IP addresses from the previous message:



Source MAC	Destination MAC	Source Port	Destination Port
AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	68	67

Fig. – DHCP Request message

4. Lastly, the DHCP server responds with a DHCP **Acknowledgment** unicast message to confirm the client can use the IP address provided from the addressing pool on the server:



Source MAC	Destination MAC	Source Port	Destination Port
BB:BB:BB:BB:BB:BB	AA:AA:AA:AA:AA:AA	67	68

Fig. – DHCP Acknowledgement message

What if a client connects to the organization's network but the DHCP server is located on another IP subnet? How will the client be able to get the IP addresses from the server?

The following diagram shows a router blocking a **DHCP Discover** message from propagating to another network:

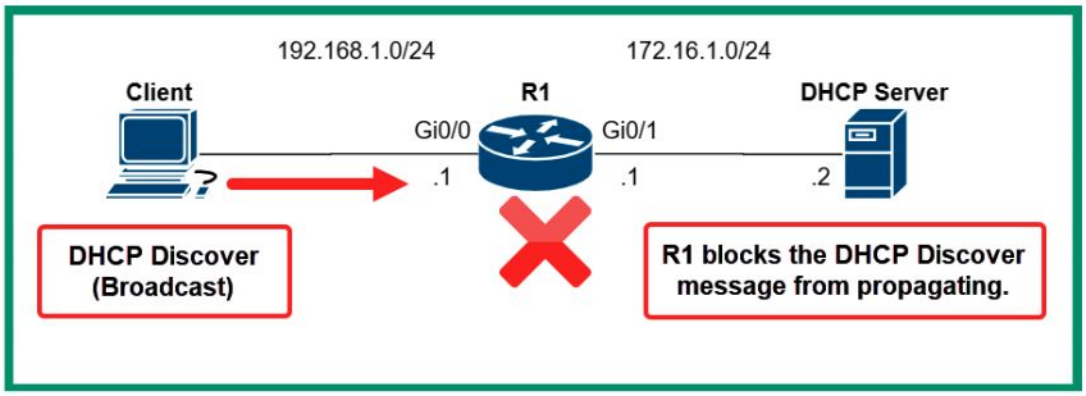


Fig. – Router blocks Layer 2 broadcast message

Solution

To solve this issue, configuring the router to be a DHCP Relay agent will allow the router to forward DHCP messages between clients and DHCP servers over a network, as shown here:

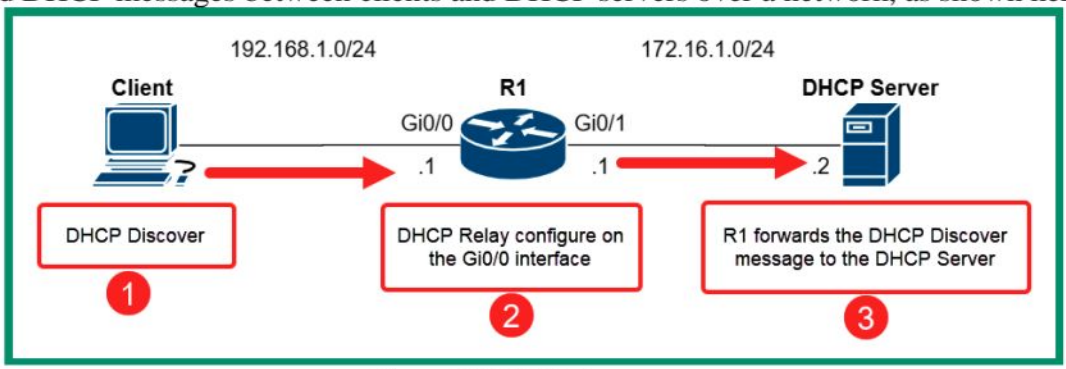


Fig. – DHCP Relay agent

- The GigabitEthernet 0/0 interface on the router is configured with the following configurations to allow the router to relay the DHCP messages between the 192.168.1.0/24 network and the DHCP server:

R1(config)# **interface GigabitEthernet 0/0**
R1(config-if)# **ip helper-address 172.16.1.2**
R1(config-if)# **exit**

- The ip helper-address command is applied to the interface on the router that receives DHCP Discover messages from clients.

DNS (Domain Name System)

- It allows a device to resolve a Fully Qualified Domain Name (FQDN) or a hostname to an IP address over a network.
- Using DNS allows network professionals to implement a DNS server on a network. This is like a directory that contains a listening of various hostnames that maps to IP addresses.
- DNS servers use port UDP port 53 by default. However, a DNS server can exchange zone records with another DNS server by using TCP port 53.
- The following diagram shows a typical DNS transaction between a client and DNS server:

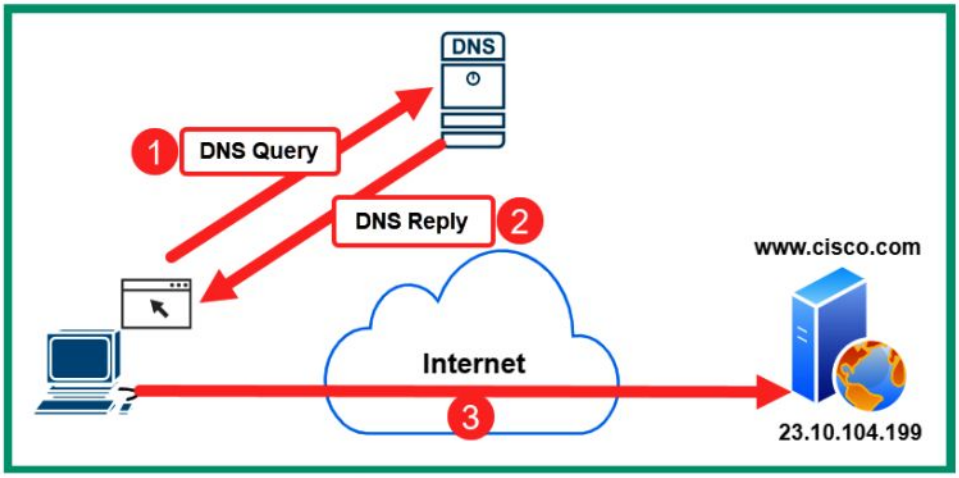


Fig. – DNS operations

The following is a breakdown of the DNS operations shown in the preceding diagram:

1. The client wants to establish a connection to www.cisco.com but does not know the IP address of the web server. Therefore, the client sends a **DNS Query** message to the DNS server on service port 53, requesting the IP address of www.cisco.com.
2. The DNS server receives this **DNS Query** and performs a lookup within its database and finds the record. The DNS server responds with a **DNS Reply** that contains the IP address of www. cisco.com.
3. The client receives the **DNS Reply** information and connects to the IP address found in the response from the DNS server.

Within a DNS server, network professionals can create various types of records containing specific IP addressing information. The following are a list of record types and their purpose:

- **Address (A versus AAAA):** The A record maps a hostname to an IPv4 address, while the AAAA record maps a hostname to an IPv6 address
- **Canonical name (CNAME):** The CNAME record allows an alias to be mapped to a domain name
- **Mail Exchange (MX):** The MX records contain the addresses of mail exchangers on a domain
- **Start of Authority (SOA):** The SOA record specifies the authority of the domain
- **Pointer (PTR):** The PTR record maps an IP address to a hostname
- **Text (TXT):** The TXT record contains text information that helps a domain owner validate ownership of a domain

• **Service (SRV):** The SRV record contains the service records for the domain
• **Name Server (NS):** The NS record contains the name servers for a domain

Authoritative DNS server:

It is the final holder of an IP address for a domain name or hostname on a network. It contains the original DNS records that are associated with a domain.

Recursive DNS server or **non-authoritative DNS server:**

It does not hold the original DNS records for a domain but queries an authoritative server when needed.

- Each domain name that's available on the internet contains the root (.) and a **Top-Level Domain** (**TLD**) such as .com, .net, or .org within the name, such as cisco.com.
- However, hostnames are usually assigned to servers such as www.cisco.com. This is commonly referred to as an FQDN since it contains a TLD, the hostname, and the domain.
- Using an FQDN allows network professionals and devices to specify the location of a device on a network.

The following diagram shows an example of a global hierarchy of root DNS servers, which contains the record for their corresponding TLDs:

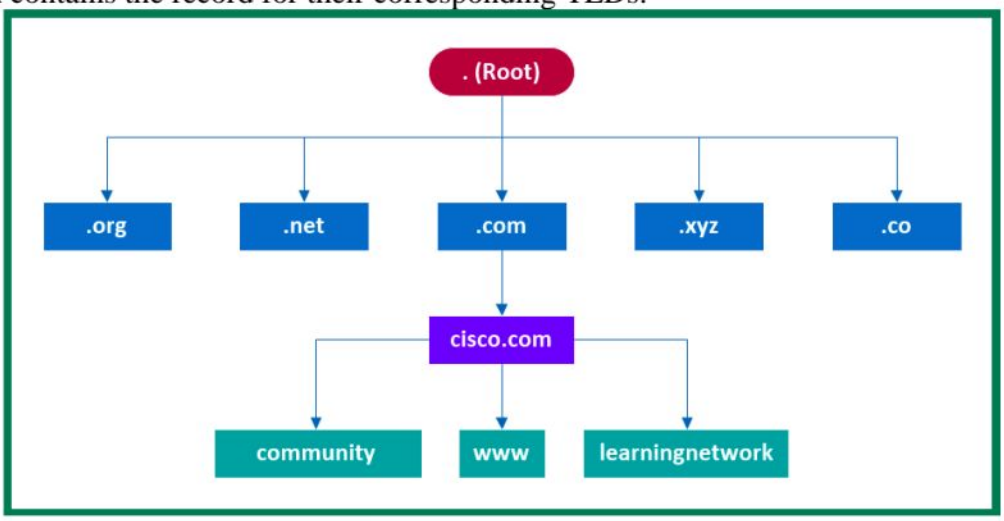


Fig. – Root DNS servers

There are many trusted DNS servers on the internet that provide improved performance, speed, and security. The following are some examples of trusted DNS servers:

• **Cloudflare DNS**: https://1.1.1.1/
• **Quad9 DNS**: https://www.quad9.net/
• **OpenDNS**: https://www.opendns.com/
• **Google Public DNS**: https://developers.google.com/speed/public-dns

Simple Network Management Protocol (SNMP)

- It is a common network protocol that allows network professionals to remotely manage and monitor networking devices, security appliances, and servers within their organization.
- It helps network professionals collect information about the performance and status of a device to determine whether an issue exists, as well as how long the issue has been occurring based on historical data.
- It operates on UDP service port 161 by default. However, the SNMP manager uses UDP service port 162.
- When working with SNMP, three main components need to work together to create a Network Management System (NMS):

- Manager
- Agent
- Management Information Based (MIB)

Fig. – SNMP messages

Manager

- The Manager is an application that's installed on the network professional's computer or centrally on a server.
- It has the role and function to both collect information and make configurations on devices that are running the agent.
- It can retrieve information from agents on the network by sending an SNMP GET message that instructs the agent to respond with the requested information.
- It sends SNMP SET messages to an agent when configuration changes are needed.

SNMP Agent

- It is configured on the networking device, such as a switch or router.
- It is the actual component on the networking device that communicates with the SNMP manager application and vice versa.

Management Information Based (MIB)

- It is a database that contains the information needed by the agent to find and retrieve data from a device.

The following are the three current versions of SNMP:

- **SNMPv1**: Has bad security features such as no data encryption or authentication mechanisms
- **SNMPv2**: This version of SNMP also contains bad security features
- **SNMPv3**: Supports data encryption and authentication

Data Center Architecture and Cloud Computing

Understanding network architecture

- It's essential to understand the importance of designing an optimal network architecture to support both the current and future demands of an organization.
- It all begins with a great network architecture design to ensure various issues such as network congestion, slow response times, security concerns, and network outages are reduced.
- It's important to consider the following factors:
  - Fault tolerance and redundancy
  - Scalability
  - Security
  - QoS

Fault Tolerance

- It defines the ability of a device to continue functioning and providing its services to a network when one or more components are affected.
- Networks must be designed with fault tolerance to ensure if a networking device such as when a router or a switch has a failure, the network is built to quickly detect the failure and recover to forward traffic between its source and destination.
- The following diagram shows a simple network that supports fault tolerance using redundancy:

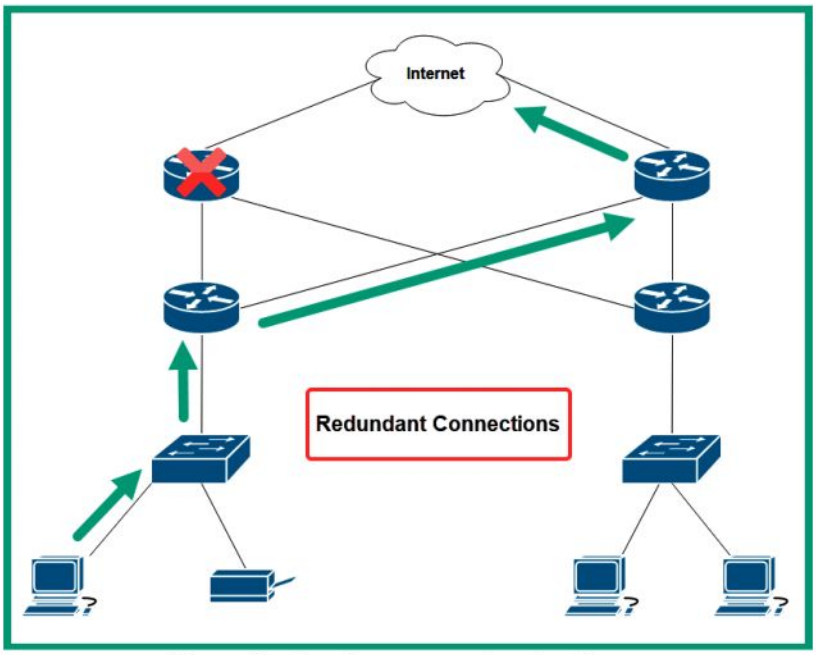


Fig. – Fault tolerance and redundancy

- Network professionals can implement fault tolerance on their network by creating **redundancy** of multiple paths between a source and a destination. Therefore, if a path is no longer available due to a faulty network cable or device, the existing networking devices can detect the failure and redirect network traffic through a different path while ensuring the availability of network services.
- When using a packet-switching network, each packet may use a different path based on the current network conditions such as available bandwidth, reliability, and load on the network.

- With a fault tolerance network that uses redundancy, packet switching is possible and provides better delivery of messages from the source to the destination.

Scalability

- Implementing scalability allows a network to easily grow to support new devices, applications, and services while not impacting the performance of existing services that are being accessed by current users within the organizations.
- Network professionals will implement additional switches to allow new end devices to connect to the network, allowing users to access the resources and services.

Daisy-chain

- If the original network design did not support scalability, network professionals may daisy-chain multiple switches together with the concept of providing a connection to all devices on the network. The following diagram shows an example of multiple switches daisy-chained together:

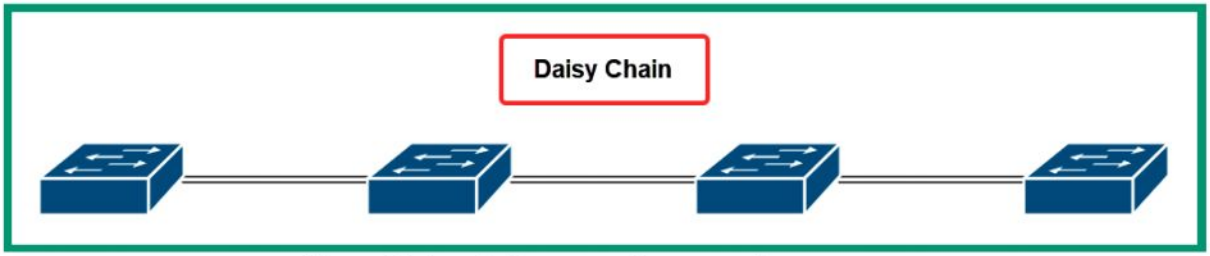


Fig. – Daisy chain network connections

- Each network switch is connected to another switch in a daisychain effect.
- While this method of interconnecting networking switches will provide end-to-end connectivity of devices on a network, it does not efficiently support scalability and redundancy. If any of the switches were to experience a failure, connectivity along the daisy chain would be affected.

Security

- With the increase in cyberattacks and newly emerging threats, organizations need to safeguard their assets from threat actors such as hackers.
- Designing a network to support network security and cybersecurity solutions is needed. Security solutions such as firewall appliances, **Intrusion Prevention Systems** (**IPSs**), and endpoint security solutions are simply forms of security solutions needed for organizations to mitigate again cyberattacks.

Quality of Service (**QoS**)

- It is a common technology that allows network professionals to configure networking devices such as routers and switches to prioritize network bandwidth for specific traffic types.
- Many protocols use **User Datagram Protocol** (**UDP**) as their preferred transport layer protocol. Because of this, if a network becomes congested, messages sent have a higher probability of being discarded.
- QoS is implemented on the network to ensure specific traffic types are guaranteed allocated network bandwidth for prioritization over other network traffic types.

Cisco has a wide range of validated design guides that help network professionals to use a **proof of concept** (**POC**) model with best practices and recommendations to implement a suitable network design within their organization.

Cisco 3-tier architecture

- It contains three layers of network switches. Each layer has a specific role and function.

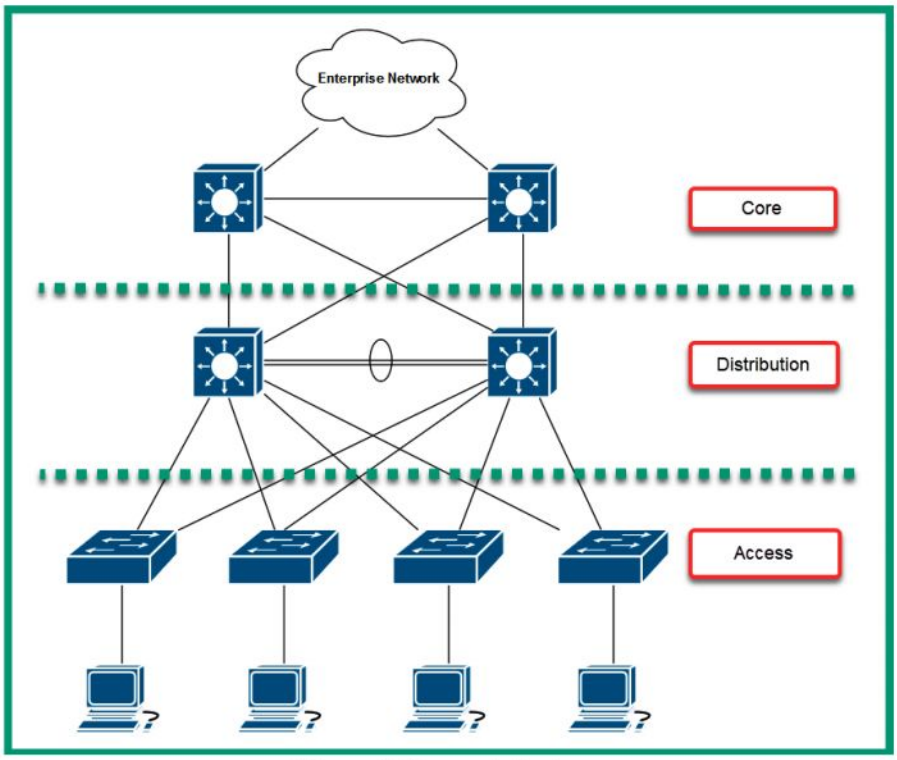


Fig. – 3-tier architecture

Access Layer

- It is also known as the edge layer which is responsible for providing network connectivity and access from end devices to the network and resources.
- Network professionals implement access layer switches that operate at Layer 2 of the OSI and TCP/IP network models.
- At the access layer, there is no redundancy for end devices that are connected to the network as a typical computer has a single Network Interface Card (NIC) that uses a wired connection to the network switch.

Distribution Layer

- It is also known as the aggregation layer which is responsible for providing link aggregation and redundancy for the access layer switches on the network.
- There are usually two distribution layer switches within a branch office; each access layer switch will connect to each distribution layer switch to ensure redundancy between end devices.
- When a distribution layer switch is offline/unavailable, the access layer switch can automatically detect that a path is no longer available and forward the frames to another distribution layer switch on the network.
- Typically, traffic within a branch office/network flows between the access and distribution layers.

Core Layer

- It is notably the high-speed backbone of the network architecture.
- It provides interconnectivity and redundancy for the distribution layers within an organization with many branch offices.
- Therefore, network traffic is sent to the core layer when the destination is located in another branch office.

Advantages

- Uses a multi-layered design to support scalability and redundancy while ensuring each layer is defined by its role and function
- Support modularity to help network professionals with their design elements, which can be replicated and applied within their entire organization while being consistent
- Eliminates the flat-network design, which does not support scalability and redundancy for large enterprise organizations

Cisco 2-tier architecture

- The 2-tier architecture is designed for smaller organizations that have a smaller network and budget.
- It consists of two layers instead of three.
- It provides the same benefits as the 3-tier model such as support for scalability, fault tolerance and redundancy, security, and QoS but with a smaller design.

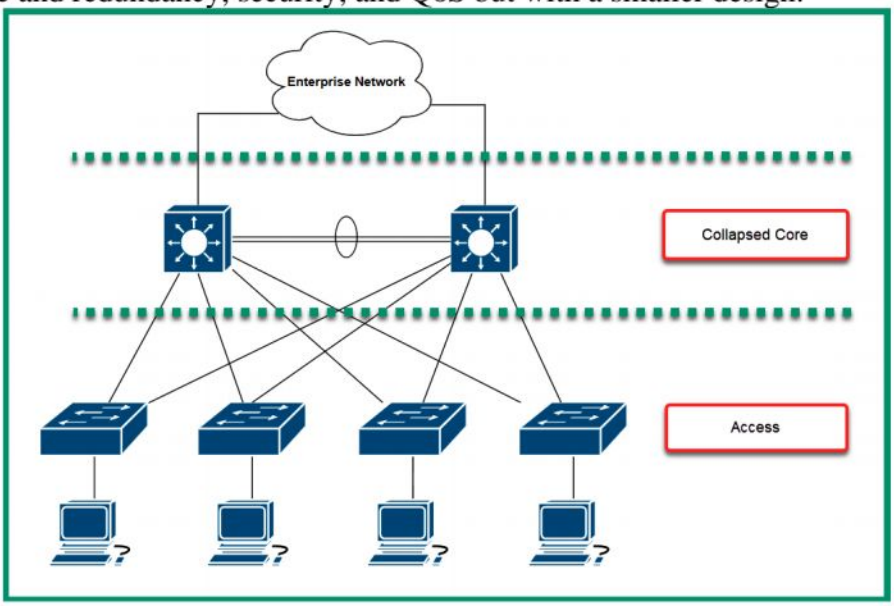


Fig. – 2-tier architecture

- 2-tier architecture contains a **collapsed core layer** and **access layer**.
- The collapsed core layer is simply a consolidation of the core and the distribution layers into a single layer.
- Network professionals can implement either core or distribution layer switches within the collapsed core layer of the network.
- The access layer has the functionality to provide network connectivity of end devices to the actual network.
- Each access layer switch is connected to each switch within the collapsed core layer to provide fault tolerance and redundancy.

Fundamentals of cloud computing

- Cloud computing can be demystified as paying for the resources you use within a cloud service provider's data center.
- Though customers cannot see the actual resources, they can use it over internet.
- It reduces time, money and physical space.
- It uses pay-as-you-go model. We can instantly deploy the server and services and terminate the services within minutes.
- Customer is only responsible for security management.
- Customers can *scale up* or *scale down* the computing resources on the server.

- Organizations that use cloud computing technologies reduce the need for a dedicated IT team. However, there is a huge demand for cloud engineers with specialized skills needed to deploy, maintain, and secure solutions on cloud platform.
- Cloud computing providers support elasticity and scalability.
- Examples of Cloud computing are Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) etc.

Elasticity:

- It simply allows a system to adapt to the workload and changes of the environment, such that a customer can quickly provision and de-provision servers and applications as needed within a cloud provider's data center.
- For instance, if your organization needs one web application to host a website, as more users connect and interact with your web server, there will be an increase in demand for computing power to process each web request.
- With elasticity, your organization can create additional web servers within a few minutes with the same web application and implement a load balancer to distribute the inbound web request between each web server.

Scalability:

- It means to increase and decrease the resources needed based on the demand.
- For instance, you may need one Linux server on the cloud to perform some tasks. As you increase the workload on the server, each task takes longer to be completed.
- Increasing the virtual number of processes and memory can allow more tasks to run at the same time while ensuring each process is allocated sufficient computing resources.

Deployment models

When deploying a cloud computing solution for an organization, four models are commonly used by cloud engineers and service providers.

1. Private Cloud
2. Public Cloud
3. Hybrid Cloud
4. Community Cloud

Private Cloud

- The private cloud model is where any organization such as your company owns the data center, and the infrastructure is managed by your IT team.
- Within the private cloud model, the resources are only accessible to the employees of the organization and no one else.
- The following diagram shows a representation of a private cloud model that can only be accessed by the organization and its employees:

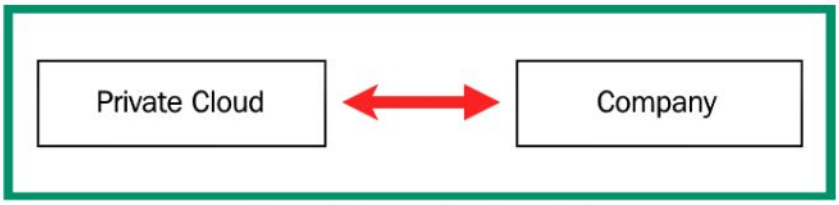


Fig. – Private cloud model

Public Cloud

- It is available to anyone on the internet.
- These are public cloud service providers such as Microsoft Azure, AWS, GCP, and many more.
- It allows anyone to create virtual servers and deploy applications and services on a data center that shares its resources with others and uses a pay-as-you-go model.

- In a public cloud model. the cloud service provider is responsible for all physical hardware maintenance.
- The following diagram shows a representation of the public cloud and your organization, which is sharing the resources with others:

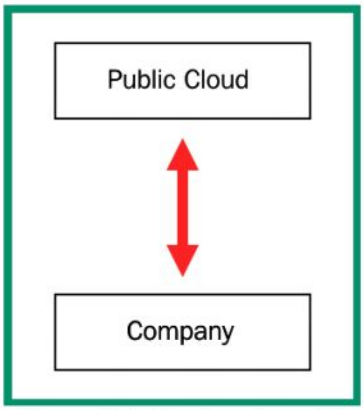


Fig. – Public cloud model

Hybrid Cloud

- It is a mixture of the private and public cloud deployment models.
- It allows an organization's data, servers, and applications to be locally backed up on its private data center and replicated to an online public cloud solution provider.
- This solution is quite costly to maintain but provides an excellent solution for disaster recovery and business continuity practices.
- The following diagram provides a representation of a hybrid cloud deployment model:

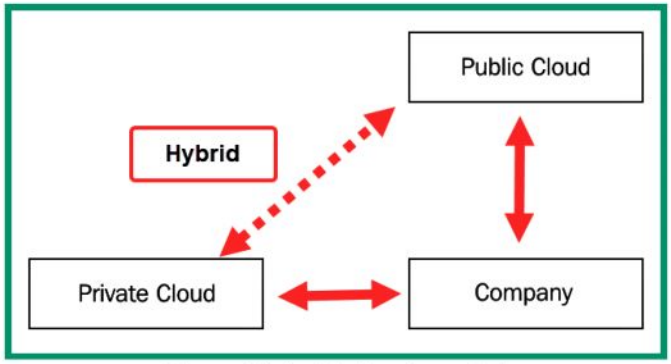


Fig. – Hybrid cloud model

Community Cloud

- The community cloud model is where several organizations share the resources on a cloud platform.
- These can be groups of companies with similar interests or partnerships all accessing and sharing resources within a data center or cloud service provider.

Cloud service models

- It defines how services, applications, and resources are delivered to users from a cloud service provider's data center.
- Various cloud service models are
  1. Software-as-a-Service (SaaS)
  2. Platform-as-a-Service (PaaS)
  3. Infrastructure-as-a-Service (IaaS)
  4. Desktop-as-a-Service (DaaS)
  5. Infrastructure as Code (IaC)

Software-as-a-Service (SaaS)

- It is a service model that allows the cloud solution provider to offer access to the user interface of the applicationthat's being hosted within the cloud provider's data center.
- For instance, organizations that use Google Workspace or Microsoft 365 do not need to install the client application on each user's computer.
- Each user can simply access the web application on their corporate email and other collaboration tools using a standard web browser.
- The user is neither concerned nor has access to manage the host operating system or the hardware components of the servers that are hosting the application.

Platform-as-a-Service (Paas)

- It is designed for developers who require a bit more control over their operating or working environments.
- The cloud service provider allows the user or developer to make changes to the operating system and the programming frameworks that are running on the host operating system.
- However, the user does not have access to the underlying hardware resources on the server.

Infrastructure-as-a-Service (IaaS)

- It allows the user to manage physical hardware and software resources on the virtual server on the cloud provider's data center.
- This model allows the user to increase and decrease the computing resources on servers, such as the number of processes, memory, storage, networking interface, and the operating system.

Desktop-as-a-Service (DaaS)

- DaaS is where a cloud service provider can deliver a virtual desktop environment to a user over the internet.
- The cloud service provider is responsible for managing all the backend maintenance such as hardware and software requirements.
- This includes backups and storage and updates.
- However, security management of DaaS solutions may be a shared responsibility between the cloud service provider and the user.
- DaaS offers a persistent desktop, which keeps the data and changes made by a user.
- So, the next time the user logs onto the virtual desktop, everything is already there.

Infrastructure as Code (IaC)

- It focuses on managing the resources within a cloud service provider's data center and the virtual machines on servers, load balancers, and networking using the same versioning method as DevOps engineers.

Cloud connectivity solutions

- Hosting applications, servers, and other resources on a cloud service provider's data center is awesome but ensuring your organization and users have secure access is very important.
- There are two methods

1. **Virtual Private Network (VPN)**
   - It allows a secure, encrypted connection to be established over an unsecure network such as the internet.
   - Setting up a VPN between your organization's network and the resources on a cloud service provider's data center is a common solution used by many organizations.
   - Using a VPN allows the company to save a lot of money while protecting data-in-motion over the internet.

- However, the company will be responsible for managing its VPN solutions and ensuring users can access the resources when needed.

2. **Private-direct connection to the cloud provider**
   - Many ISPs provide direct connectivity solutions between an organization (customer) and a data center.
   - These connectivity solutions are usually secure within the ISP network to ensure no unauthorized parties can intercept the communication channel between the customer and the data center.

Networking Devices

Understanding networking devices

- Networking devices are intermediary devices that are used to build and extend a network to allow users to access and share resources.
- There are various networking devices within the industry and it's very important to understand the role, function, and how each device forwards traffic along a network between a source and destination.

Hub

- A network hub is a legacy networking device that operates at Layer 1 of the Open System Interconnection (OSI) networking model.
- It operates like a repeater device, which simply accepts an incoming electrical signal on the wire and rebroadcasts it through all other interfaces on the hub.
- To put it simply, if four computers are connected to a hub, and PC 1 sends a message into the hub, the hub will rebroadcast the message to all other devices that are connected to the hub.
- The following diagram shows how a hub forwards a message:

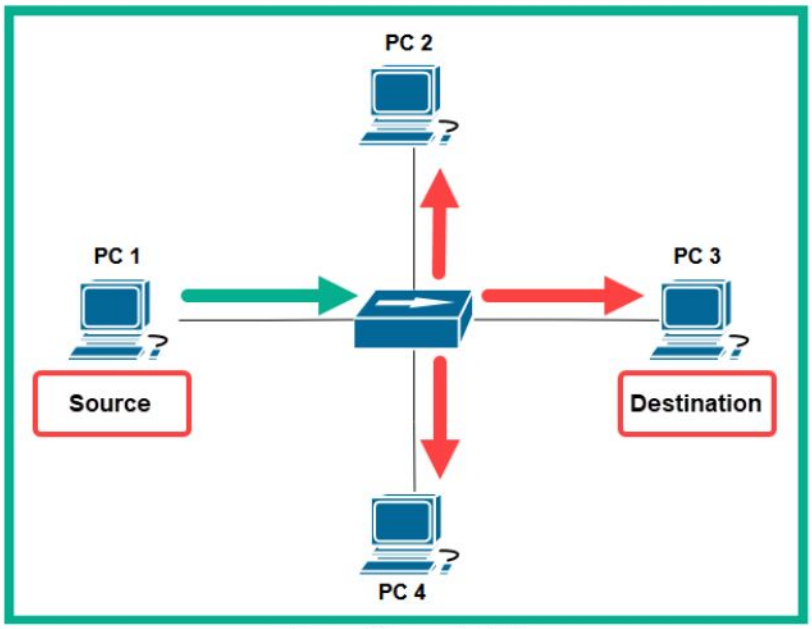


Fig. – Network hub

- A single collision domain is created for all devices that are connected to the hub.
- A **collision domain** is simply a segment of the network where a packet collision can occur due to more than one device transmitting a message at a time on a shared network segment.
- Once packet collision occurs, the message is discarded and the sender has to transmit the message again.
- To prevent issues on a hub network, end devices such as computers use **Carrier Sense Multiple Access with Collision Detection** (**CSMA/CD**).
- Before an end device places a message (electrical signal) on the media, the device checks the media for the presence of a signal.
- If a signal is detected, it means another device is already using the media/network and is transmitting a message.
- Therefore, the device waits and checks the media again until no signals are detected, and then proceeds to transmit the message. Since a hub network is a shared medium of communication,

Layer 2 switch

- Network switches are intermediary networking devices that operate at Layer 2 of the OSI networking model and allow end devices such as computers, servers, and printers to connect to a network.
- It is an intelligent device that inspects the destination MAC address found within the Layer 2 header of a frame to determine the destination host.

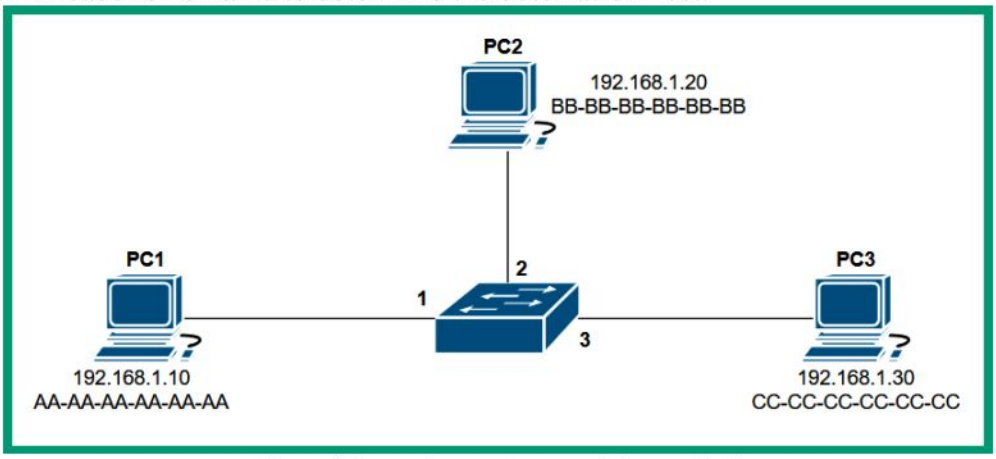


Fig. – Network topology with a switch

- Each computer is assigned an IPv4 address and has a unique MAC address on its **network interface card** (**NIC**).
- When a switch boots up, it does not know which computer is connected to any of the local interfaces on the switch.
- Only when a device such as a computer sends a message does the switch inspect the source and destination MAC addresses within Layer 2 of the frame, which is used to populate the **content-addressable memory** (**CAM**) table.

Address Resolution Protocol (ARP)

- It allows devices to resolve an IPv4 address to a MAC address on a LAN.
- PC 1 will send an ARP request message with a destination MAC address of FF:FF:FF:FF:FF:FF to the switch, which will broadcast the message to all other interfaces except the interface the message originated on, as shown in the following diagram:

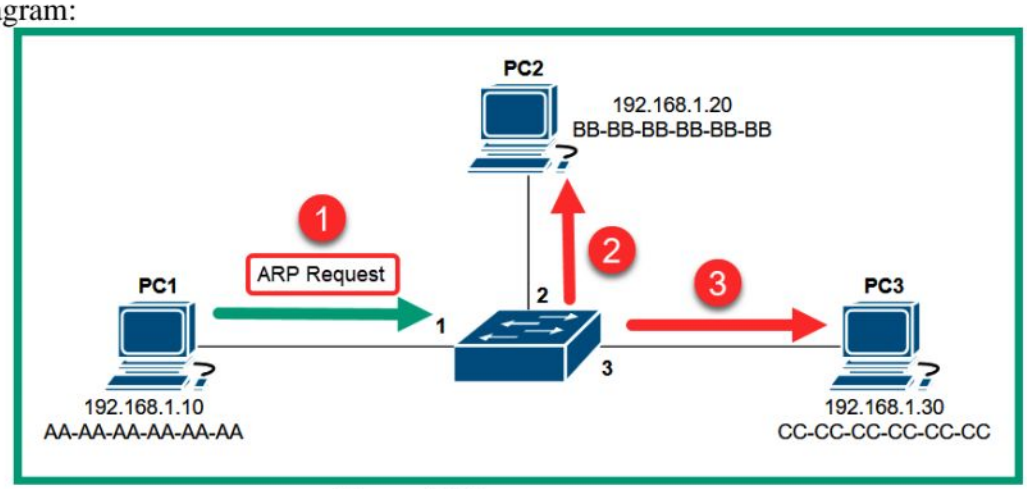


Fig. – ARP request message

- The ARP request message is sent to the switch and is broadcasted to all other interfaces.
- The source MAC address of the frame is stored on the CAM table and is mapped to interface 1, as shown in the following table:

Interface	MAC Address
1	AA-AA-AA-AA-AA-AA
2	
3	

Fig. – CAM table

- Next, PC 2 and PC 3 will receive the ARP request message and inspect the requested target IP address of 192.168.1.30.
- Since PC 2 has an IP address of 192.168.1.20, it will discard the message and not respond.
- PC 3 has the target IP address and will respond directly to PC 1 with its MAC address using an ARP reply message.
- The following diagram shows an ARP reply message:

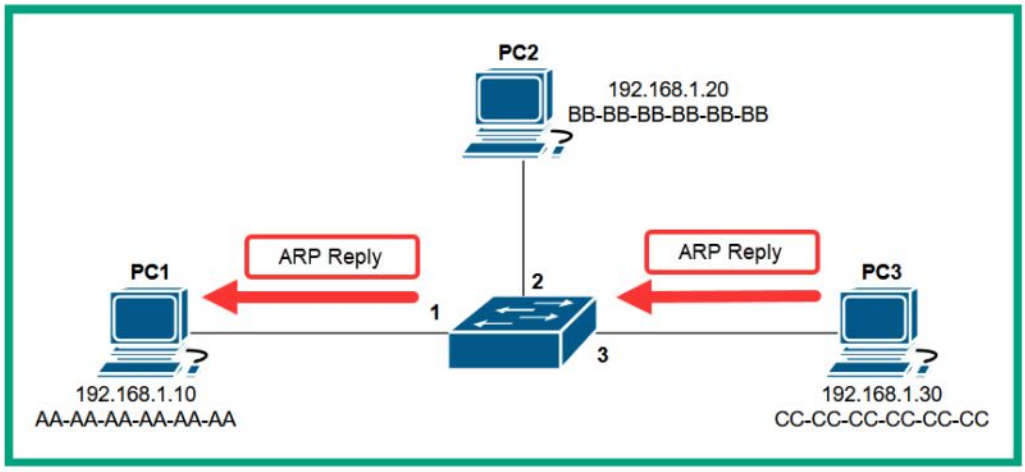


Fig. – ARP reply message

- When the switch receives the ARP reply message from PC 3, it inspects the source and destination MAC.
- PC 3's source MAC address is stored within the CAM table and is mapped to interface 3, and the switch forwards the ARP reply directly to the destination host since the switch had previously recorded PC 1's MAC address on the CAM table.
- The following table shows the entries of the CAM table after receiving the ARP reply from PC 3:

Interface	MAC Address
1	AA-AA-AA-AA-AA-AA
2	
3	CC-CC-CC-CC-CC-CC

Fig. – CAM table updated

- Once a switch already knows PC 3 is connected to interface 3, it sends the message directly to the destination host on the network.

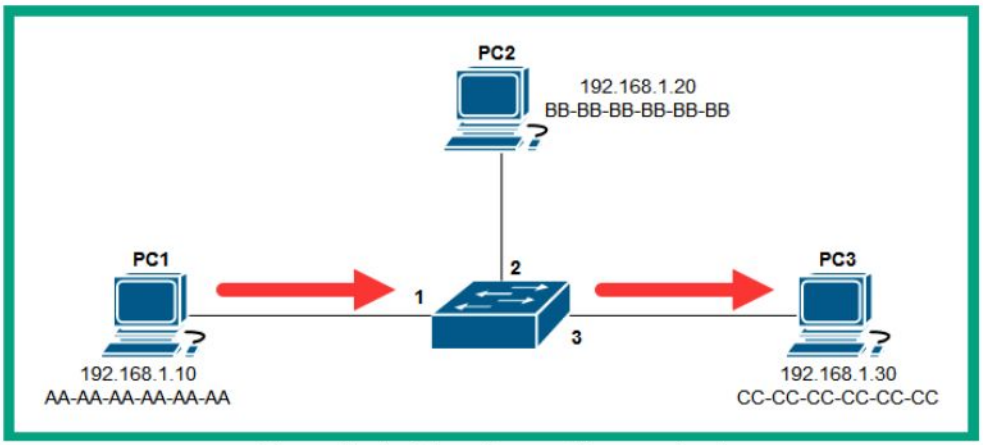


Fig. – Switching forwarding method

- Switches help reduce the size of a collision domain as compared to hubs on a network.
- Switches are able to isolate a collision to a per-interface level. Each interface/port on a switch represents one collision domain.
- Therefore, a switch with eight ports has eight collision domains.
- The following diagram shows a representation of collision domains on a switch:

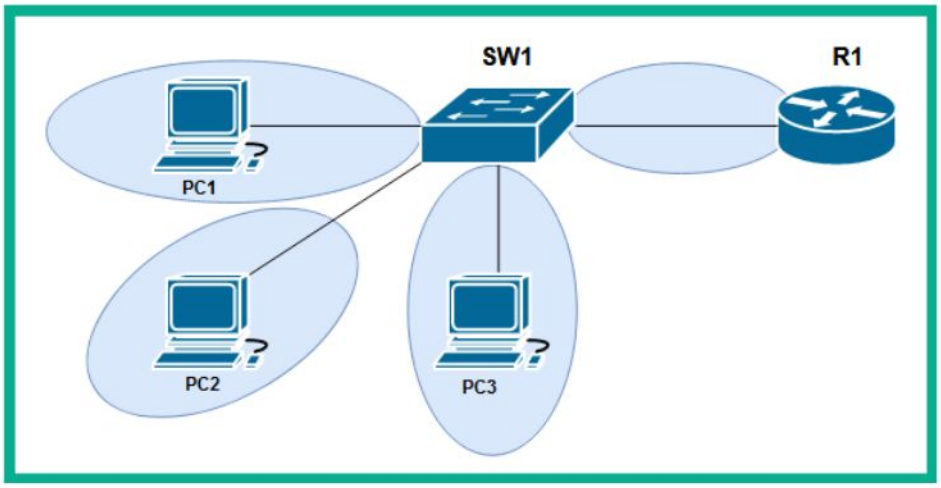


Fig. – Collision domains

- A broadcast domain is simply described as a network segment that all devices can reach by using a Layer 2 broadcast message.
- The following diagram shows a broadcast domain on a network switch:

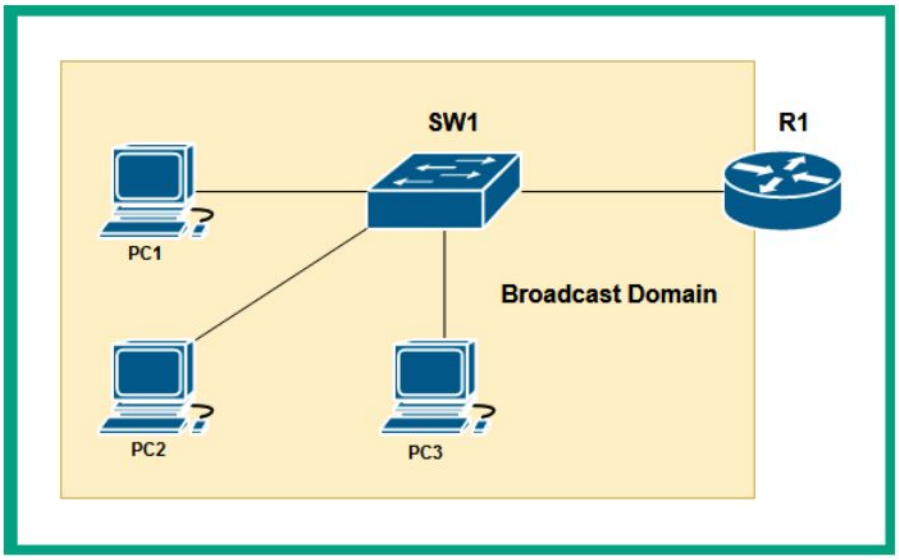


Fig. – Broadcast domain

- By default, all interfaces on a switch collectively create a single broadcast domain that allows all devices to be reached by a Layer 2 broadcast message.

Layer 3 capable switch

- There are Layer 3 network switches, which operate at the network layer of the OSI networking model.
- These Layer 3 switches allow network professionals to interconnect and perform routing between different virtual local area networks (VLANs) within an organization.
- Large organizations implement VLANs within their physical network, which allows network professionals to logically segment a physical network into small broadcast domains, allowing each department (such as human resources, sales, IT, and so on) to be on their own logical network.
- If a device within the sales VLANs generates a broadcast message, it's limited to devices within the same VLAN only.
- Since an organization may have multiple VLANs, hosts within a VLAN will not be able to communicate with devices on another VLAN.
- Using a Layer 3 switch allows the organization to reduce the cost of a dedicated router on the network to perform inter-VLAN routing.

Bridge

- A network bridge is a special networking device that operates at Layer 2 of the OSI networking model and allows network professionals to divide the network into multiple collision domains.
- Network professionals can implement a bridge into a large collision domain to create two smaller collision domains on a network.
- The following diagram shows a network topology with two collision domains that are separated by a bridge in the middle:

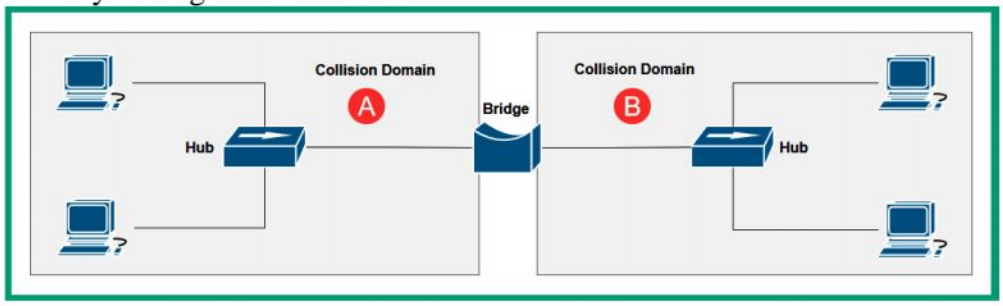


Fig. – Creating a smaller collision domain

- If PC 1 and PC 2 send a message at the same time, a packet collision will occur and affect the devices that are connected to **Collision Domain A** only, leaving **Collision Domain B** unaffected.
- However, if PC 1 sends a broadcast message, all devices (such as PC 2, PC 3, and PC 4) will receive the message because they are still connected to the same broadcast domain.

Router

- Routers are Layer 3 devices that operate at the network layer of the OSI networking model and allow network professionals to interconnect two or more different networks together.
- These are dedicated networking devices that function as the default gateway and forwarding device that allows hosts on one network to communicate with hosts on another network.
- Whenever a router accepts an inbound message such as a packet, it inspects the Layer 2 header for the destination MAC address to determine whether the message is intended for the router.
- If the destination MAC address of the message matches the MAC of the inbound interface of the router, the frame is de-encapsulated and sent up to the network layer of the OSI networking model.
- At the network layer, the router inspects the destination IP address within the Layer 3 header of the packet and checks the routing table on the router for a suitable route/path to forward the message to its destination.
- Each router contains a routing table that contains a number of routes to various destination networks and the internet.
- The router checks the routing table from top to bottom each time it has to perform lookup before forwarding a packet.
- Once a suitable route is found, the router stops the route lookup and processes the information within the matching route.
- The following diagram shows a few networks that are interconnected using routers:

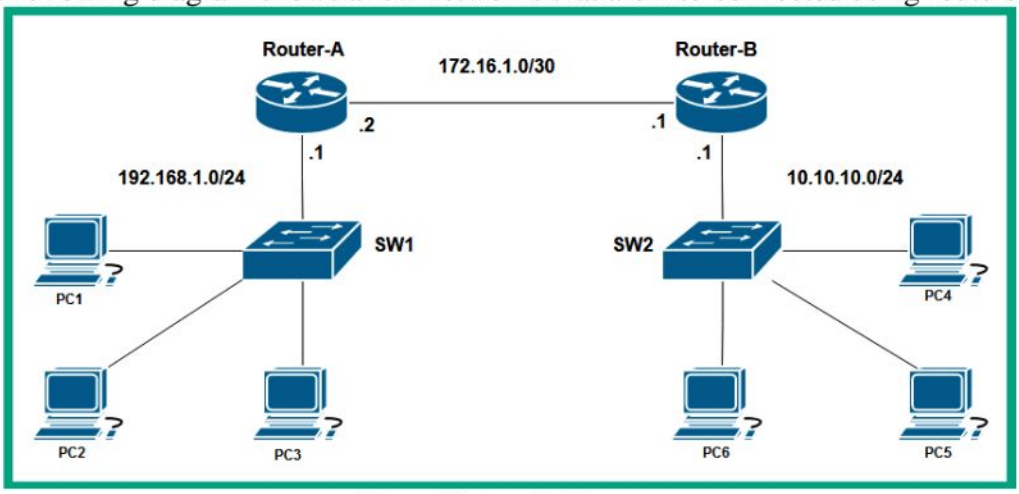


Fig. – Network diagram

- The following snippet shows the routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0/24 [110/2] via 172.16.1.1, 00:01:05, GigabitEthernet0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/30 is directly connected, GigabitEthernet0/1
L       172.16.1.2/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0

Router-A#
```

Fig. – Routing table

- As shown in the preceding figure, the routing table of a router such as **Router-A** contains the following:
  - The source of a route that is usually indicated by code
  - The destination network
  - The next hop address
  - The exit interface of the router
- Once **PC1** determines that **PC2** is on a different IP subnet from itself, **PC1** sends a message to its default gateway, which is 192.168.1.1 on **Router-A**'s GigabitEthernet 0/0 interface.
- Routers will use the destination IP address found within the packet and check the routing table.
- Each interface on a router represents a collision domain.
- Each interface on a router is also attached to a broadcast domain.
- Let's study the following network diagram and identify the number of collision domains and broadcast domains.

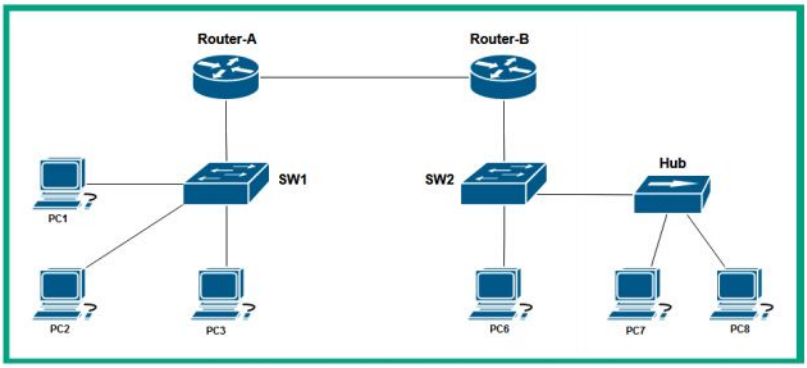


Fig. – Network diagram

- There are three broadcast domains, as shown in the following diagram:

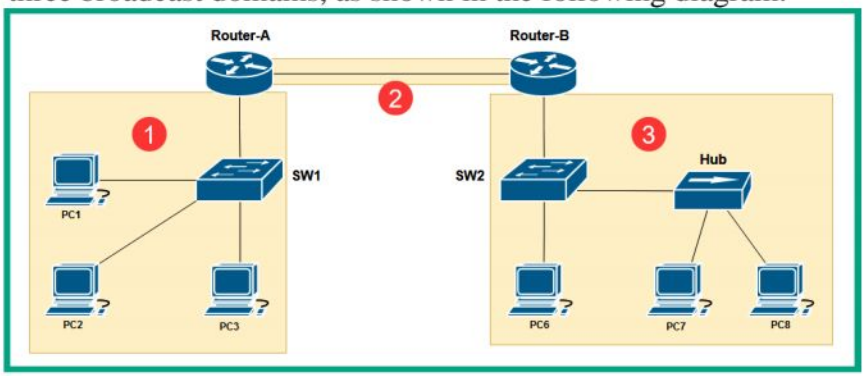


Fig. – Identifying the number of broadcast domains

- There are eight collision domains, as shown in the following diagram:

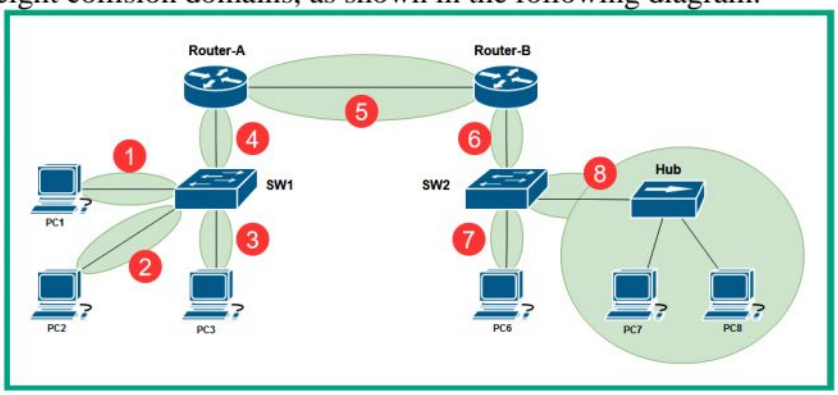


Fig. – Identifying the number of collision domains

Access point

- An access point (AP) is a networking device that allows Wi-Fi-capable devices to connect to a wired network, allowing users to share resources and access services.
- Wireless networking allows network professionals to easily extend the capabilities of a wired network to a wireless network by simply connecting an AP to a network switch.
- Since a network operates at Layer 2 of the OSI networking model, the AP simply generates wireless signals on 2.4 GHz and 5 GHz based on the IEEE *802.11* standards for wireless networking.
- The following diagram shows a small wireless network with an AP:

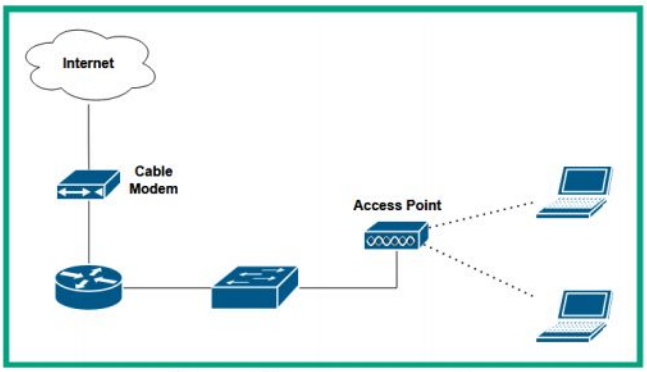


Fig. – Wireless network

- The following steps are written in layman's terms to provide clarity on how a wireless client proceeds to send a message on a wireless network:

  1. **Client-A** wants to send a message to another wireless client that is connected to the same AP.

  2. Before **Client-A** transmits the message, it sends a **Request to Send** (**RTS**) message to the AP to determine whether the wireless network is clear to send the message.

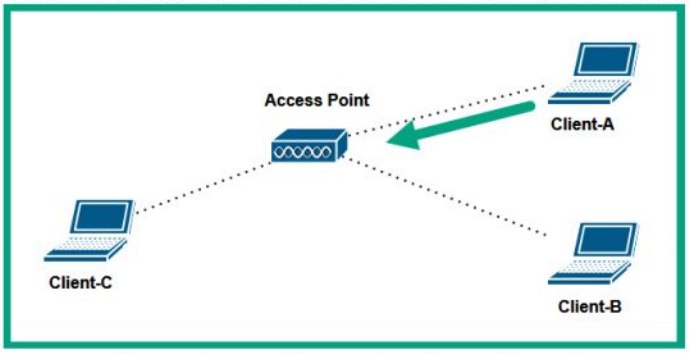


Fig. – Requesting status from the AP

3. The AP will respond with a Clear to Send (CTS) message if no other devices are transmitting on the wireless network.

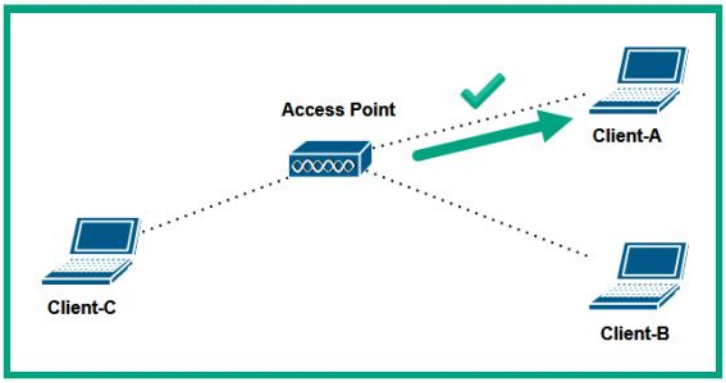


Fig. – AP providing a response

4. Then, **Client-A** will send the message to the AP that is responsible for forwarding it to the destination host on the wireless network.
5. The AP will simply rebroadcast the message to all other connected hosts similar to a hub on a wired network.

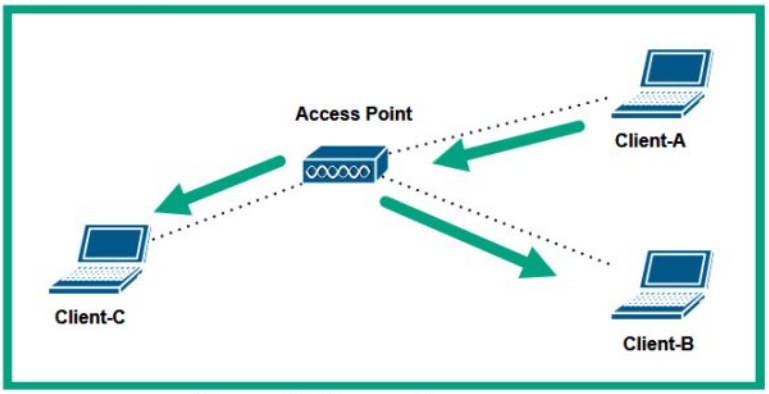


Fig. – AP forwarding message

- Wireless networks that use IEEE *802.11a/b/g/n/ac* use **Carrier Sense Multiple Access with Collision Avoidance** (**CSMA/CA**) to avoid collision of frames on a wireless network.
- With CSMA/CA, a wireless client will first check with the AP to determine whether the network is clear to send or not.
- The AP will respond to the client with an all-clear or not. This method prevents collisions of more than one client wanting to transmit a message over the wireless network.

Wireless LAN controller

- A wireless LAN controller (WLC) is a special networking device that allows network professionals to efficiently manage all the wireless access points (WAPs) within an organization from a centralized controller on the network.
- As more WAPs are implemented to support wireless clients, network professionals need to continuously monitor the performance of the wireless network to ensure the network is operating optimally.
- Using a WLC allows network professionals to configure each WAP on the network to establish a connection to the WLC.
- Network professionals can simply log in to the WLC with a web interface and centrally manage the entire wireless network.

- The WLC allows the network professional to make the changes directly on the controller, and the WLC will push the configurations to all WAPs within the network automatically to ensure the changes take effect as soon as possible.

Load balancer

- A **load balancer** is a special networking device that allows network professionals to distribute the inbound network and application traffic types across a cluster of servers that are providing services and/or resources to users.
- The following diagram shows a load balancer deployed on a network:

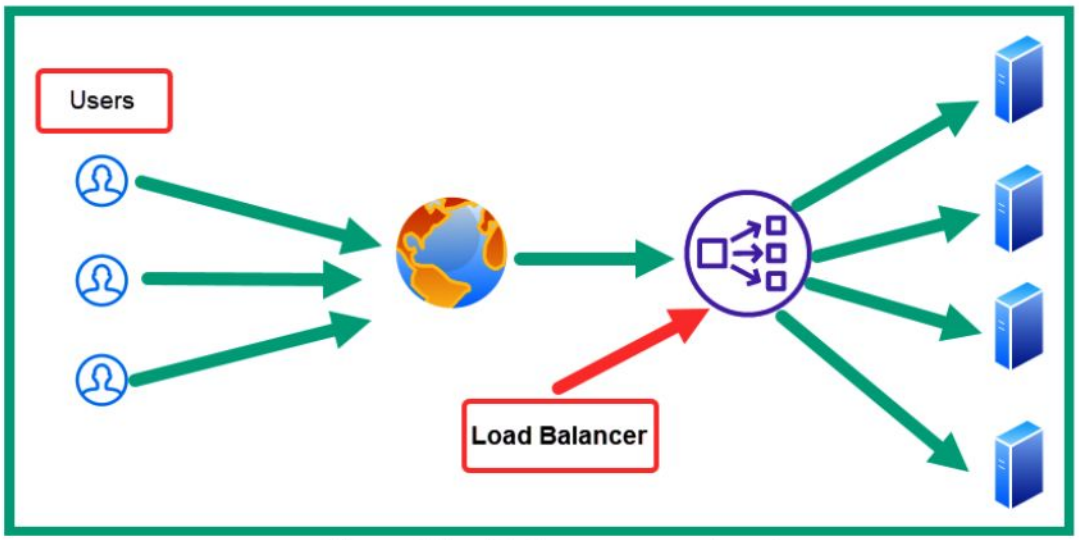


Fig. – A load balancer on a network

- Any incoming traffic from users on the internet is intercepted by the load balancer, which is responsible for distributing the network and application traffic types to the group of servers, ensuring each server is not overburdened with a lot of transactions or requests.
- Load balancers are able to provide fault tolerance; in the event of a server within the cluster being unavailable or offline, the load balancer can simply distribute the incoming load of network traffic to the available servers within the cluster.
- However, load balancers can operate in an **Active/Active** state, which allows the distribution of network and application traffic between all active servers within a cluster.
- They can also operate in an **Active/Passive** state, which allows the distribution of the load to an active server only and performs a failover to a standby server if the active server is no longer available.
- The following are the four most common algorithms that are used by load balancers that determine how the load is distributed to servers on a network:

Round robin: The round robin method simply forwards a request message from a user to each server within the group in turn, and when the load balancer reaches the last server within the group/cluster, it will start again from the first server to the second and third and so on. The load balancer assumes each server within the group or cluster is always available, has the same hardware and software specification, and is processing the same amount of load.

Weighted round robin: This allows the load balancer to distribute the load to each server within a group based on the weight that is assigned to the servers. The higher the weight value that's assigned to a server within the group, the more requests will be forwarded to that specific server and less traffic/load to the servers with a lesser weight value.

Least connections: The least connections technique is a dynamic load-balancing method that forwards a request to a server within the group that has the least active number of connections.

Least response time: It forwards a request message from a client to the server with the lowest average response time within the group of servers.

Proxy server

- A proxy server is simply a server on the network that performs the function of a relay between clients and servers on a network.
- Proxy servers are commonly implemented by network professionals to prevent hackers from invading a corporate network within an organization, and it does this by intercepting all the messages between the clients and servers.
- Within companies, proxy servers are commonly used to perform URL filtering by inspecting the destination URL that a user is trying to reach.
- If the URL is within the blacklist of web addresses, the proxy server does not forward the client request to the destination.
- However, if the destination URL exists within the whitelist of allowed web addresses, the proxy server forwards the message to the destination server.
- The following diagram shows a proxy server on a network:
-

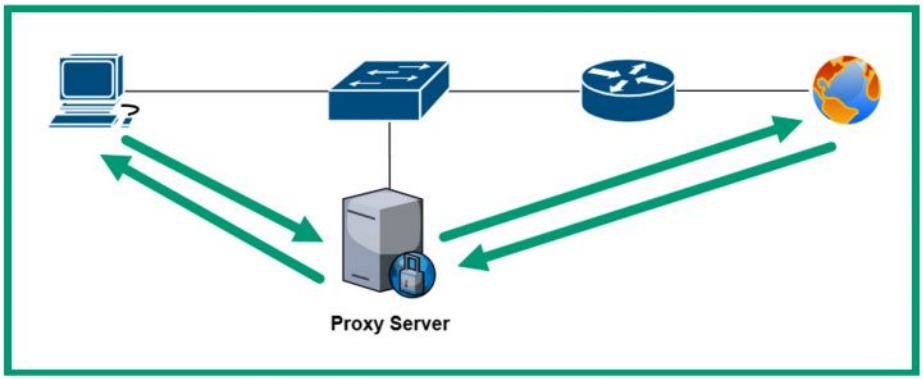


Fig. – Proxy server on a network

Internet modems

- A cable modem is simply the **customer premises equipment** (**CPE**) that is provided by an **internet service provider** (**ISP**) to terminate the **cable modem termination system** (**CMTS**) network that is distributed over coaxial cables.
- The cable modem performs the function of a router, switch, and access point in one unified device.
- The following diagram shows a simple representation of the CTMS network:

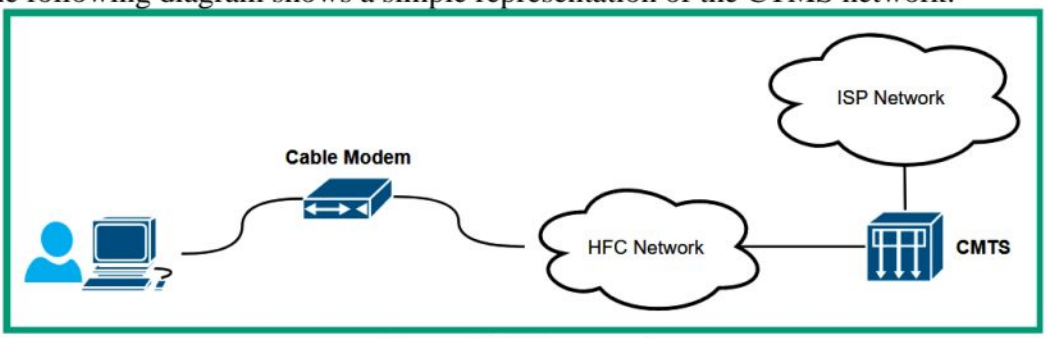


Fig. – CMTS network

- As shown in the preceding diagram, the ISP implements the CMTS network infrastructure and distributes the cable TV and internet services over the **hybrid fiber-coaxial** (**HFC**) infrastructure to their customers.

- A cable modem is installed at the customer's location to interconnect the customer's private network to the HFC and CMTS infrastructure to access internet services.
- **Digital subscriber line** (**DSL**) modems are another type of modems provided by ISPs that distributes internet services over the **public switched telephone network** (**PSTN**) lines, sometimes called the **plain old telephone service** (**POTS**) lines.
- The following diagram shows a representation of a typical PSTN network with a DSL modem:

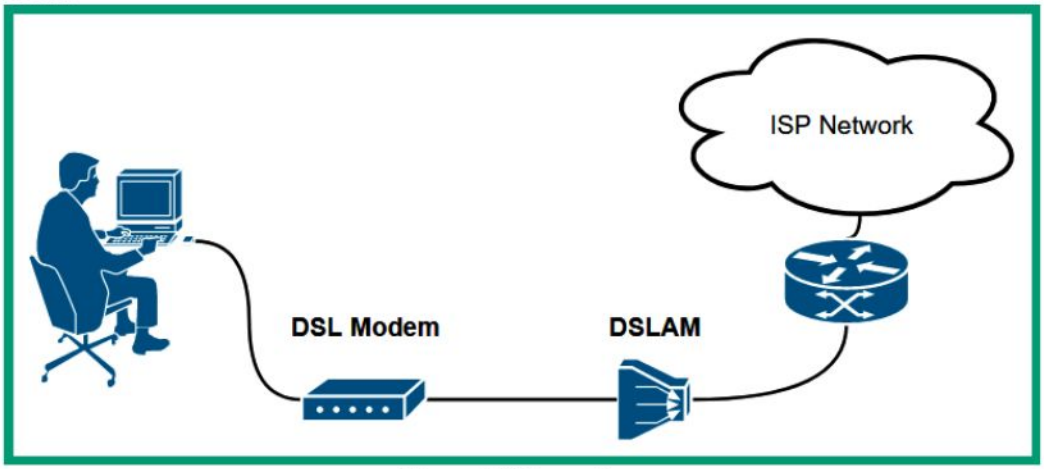


Fig. – DSL modem

Repeater

- A repeater, sometimes referred to as a Wi-Fi extender/repeater, is a Layer 1 device that simply accepts a signal and regenerates the same signal at a higher power.
- Network professionals implement repeaters in strategic locations within their building or compound to capture the signals from the APs and regenerate the same signal.
- This technique helps reduce dead zones within the wireless network, ensuring there is maximum coverage of the wireless signals for all wireless clients within the organization.

Voice gateways

- **Voice gateways** allow an organization to interconnect their enterprise **Voice over IP** (**VoIP**) network to the telecommunication service provider's network using various connectivity methods such as PSTN and **Session Initiation Protocol** (**SIP**) technologies.
- Using a voice gateway allows users to establish calls outside the organization's network using a telecommunication service provider.

Media converters

- Media converters are specialized networking devices that allow network professionals to easily convert an ethernet communication protocol from one media type to another.
- For instance, if a network professional wants to interconnect a fiber optic cable to a switch that supports only ethernet interfaces, using a media converter allows the light signals from the fiber optic cable to be converted to electrical signals for the ethernet cable, and vice versa.

Routing and Switching Concepts

Exploring routing concepts

- **Router** is a networking device that allows network professionals to interconnect two or more different networks together, and forward packets to their destinations.
- Routers are Layer 3 devices that operate at the Network layer of the **OSI** and the Internet layer of the **TCP/IP** networking models.
- For instance, routers can interconnect different IP subnets, allowing devices on one IP network to communicate with hosts on another IP network and interconnect networks with different media types, such as an Ethernet network with a fiber optic.

Operations of Router

It performs many Layer 3 operations such as

- Core function of all routers is to *route/forward* packets to their destinations efficiently using the most suitable path.
- It performs Network Address Translation (NAT) and filtering traffic using Access Control Lists (ACLs).
- Some routers support Virtual Private Network (VPN) capabilities, allowing network professionals to set up *site-to-site* and *remote access* VPNs.
- Routers are configured with routing protocols, which use an algorithm that helps them determine the best path or route to a destination.

Metric values to various factors about a path in dynamic routing

- Cumulative bandwidth
- Latency
- Reliability
- Outgoing load (TX load)
- Receiving load (RX load)
- Hop count
- Path

- The following diagram shows a computer that wants to send a message to a remote device:

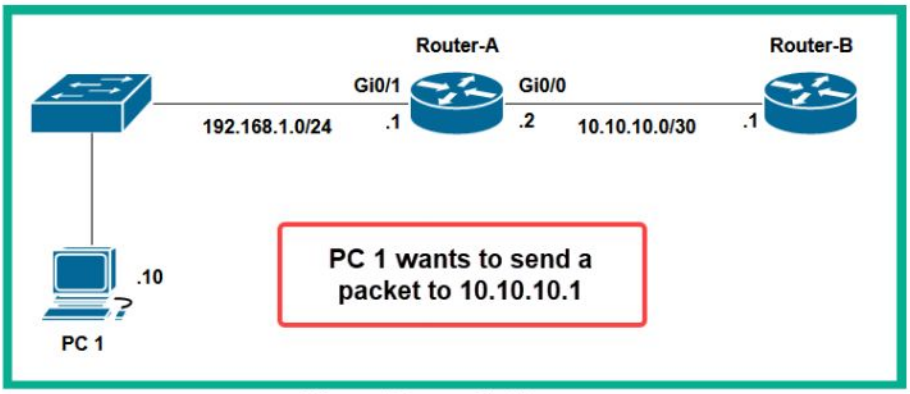
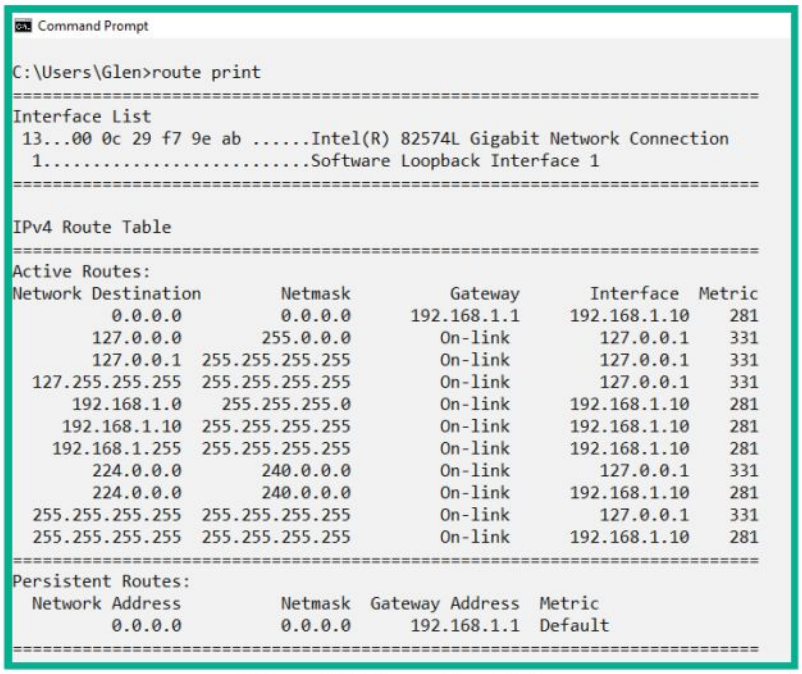


Fig. – Network diagram

- **PC 1** wants to send a message to **Router-B**, which has been configured with an IP address of 10.10.10.1.
- Before **PC 1** places the message on the network media, it checks its local *routing table* to determine whether the destination exists within the same network as **PC 1** or on a remote network.
- The following screenshot shows the routing table within **PC 1**:



```
Command Prompt

C:\Users\Glen>route print
===========================================================================
Interface List
 13...00 0c 29 f7 9e ab ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.10    281
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link      192.168.1.10    281
     192.168.1.10  255.255.255.255         On-link      192.168.1.10    281
    192.168.1.255  255.255.255.255         On-link      192.168.1.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.1.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.1.10    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.1.1  Default
===========================================================================
```

Fig. – PC 1 routing table

- Since 10.10.10.1 does not exist within the 192.168.1.0/24 network, **PC 1** sends the message to its **default gateway**, which is **Router-A** on the network.
- When **Router-A** receives the message from **PC 1**, it inspects the destination IP address within the Layer 3 header of the packet and checks its local routing table for a suitable route/path to forward the packet to its destination.
- The following screenshot shows the routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1

Router-A#
```

Fig. – Routing table of a Cisco router

- The routing table contains a list of destination routes (paths) that are known to the router.
- The code listed in the upper portion of the snippet indicates how a route was learned by the router.
- For instance, in the lower portion of the snippet, there are various *parent routes* and *child routes*.
- The child routes can easily be identified as they are indented compared to the parent routes, which are not in the routing table.
- Each child route has a code that indicates how the router was learned.
- A router will check its routing table using a top-down approach until it finds a suitable route. Once a suitable route is found, the router stops searching and forwards the packet to the destination based on the details specified within the route.

- A network route will specify the *exit interface* of the router and/or the *next hop* address.
- The *exit interface* simply indicates which port on the router should be used to forward the packet to its destination.
- The *next hop* address is the IP address of the next router to receive the packet along the way to the destination.

Understanding routing protocols

- Routers can populate their routing tables with directly connected routes or networks that are attached to the local interfaces of a router.
- However, a router is unable to determine the path/route to a destination network that is not directly connected, such as a remote network on the internet or a network that is attached to another router within an organization.
- For instance, the following screenshot shows the *routing table* of **Router-A**, which has two directly connected routes/networks on the local router:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1

Router-A#
```

Fig. – Routing table

- **Router-A** contains the 10.10.10.0/30 network, which is directly connected to its GigabitEthernet 0/0 interface, and the 192.168.1.0/24 network, which is directly connected to the GigabitEthernet 0/1 interface.
- The following diagram provides a visual representation of the *routing table* within **Router-A**:

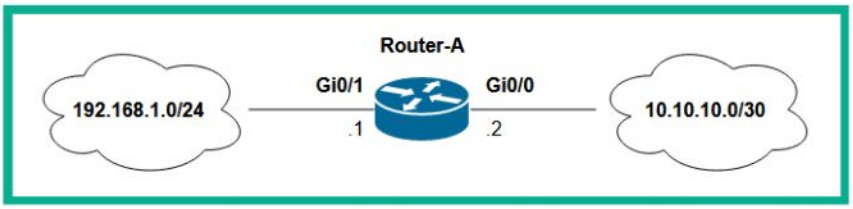


Fig. – Network topology

- Network topology was expanded to include additional networks that are interconnected with multiple routers.
- As shown in the following diagram, **Router-A** is not directly connected to the 10.20.20.0/24 and 172.16.1.0/24 networks. Therefore, if **PC 1** wants to send a message to **PC 2** over the network, **Router-A** will not be able to forward the message until those networks are known to **Router-A**.
- As a result, if **PC 1** forwards a packet to **Router-A** with the destination IP address of 172.16.1.10,
- **Router-A** will return a *Destination Host Unreachable* message to **PC 1** because a route to the destination host or network does not exist within the routing table of **Router-A**.

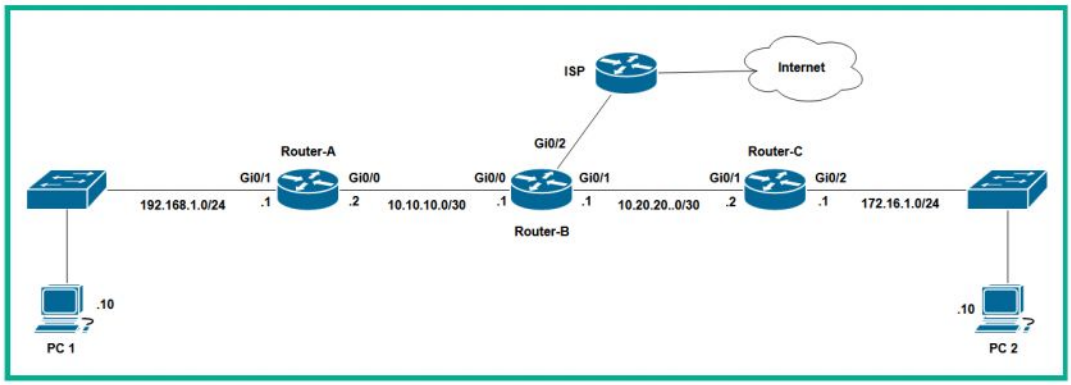


Fig. - Network Diagram

- The following screenshot shows the response from **Router-A**, which indicates it does not have a valid route to the destination host:

```
C:\>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. – Destination unreachable message from the router

- A network professional can resolve this issue by configuring **Router-A**, **Router-B**, and **Router-C** with a dynamic routing protocol that automatically shares network routes between routers, allowing them to update their routing tables of network topology changes while ensuring each router knows how to forward packets to its intended destination.

Dynamic routing

- These are designed to help routers automatically learn about designation networks by sharing routing information with other routers.
- The routing information that's shared between routers within an organization is used to add the best suitable route to a destination network within the routing table of each router.
- If a network or path is no longer available, the dynamic routing protocol automatically detects changes within the network topology, sharing updated routing information with all routers within the network to ensure their routing table is always up to date.
- If a router receives a packet with a destination IP address and the router no longer has an available route to the destination, the router informs the sender that the destination host or the network is unreachable.
- Each dynamic routing protocol is designed with an algorithm that calculates the best suitable path to a destination by determining the **metric** (cost) of each available path and choosing the path with the least metric to install within the routing table.

Benefits

- Automatically discover remote networks by sharing routing information between routers on a network
- Maintain an up-to-date routing table on all routers within the network
- Choose the best suitable destination path to forward packets to their destinations
- Can find a new best path in the event the current path is no longer available

The following diagram shows a breakdown of each dynamic routing protocol within the industry:

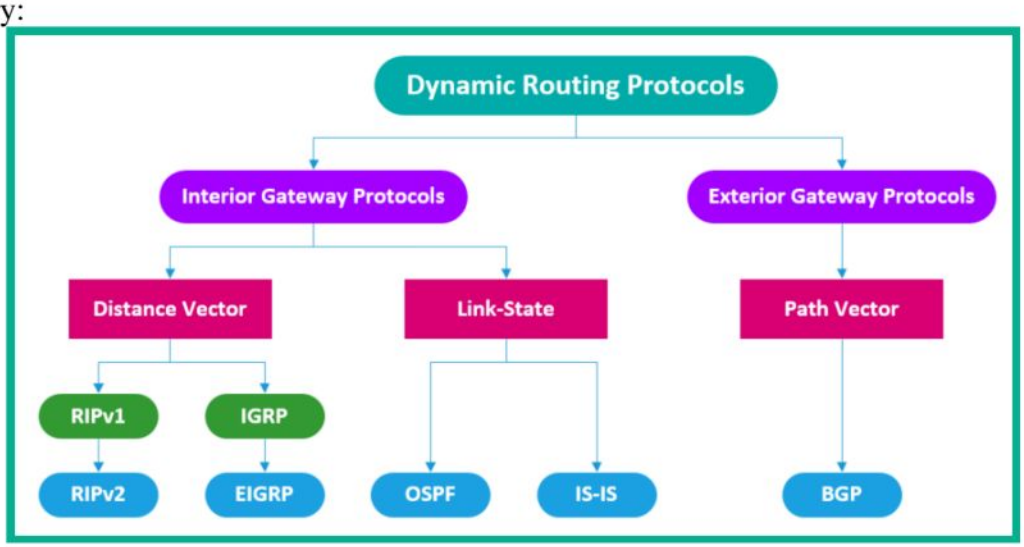


Fig. – Dynamic routing protocols

Interior Gateway Protocols (IGPs)

- IGPs are simply dynamic routing protocols that are implemented within an organization that does not share routing information on the internet.
- For instance, organizations with private networks implement IGPs on their routers to share routing information.
- When all routers know about all networks within an organization, it's commonly referred to as a **converged network**.
- IGPs are further divided into two sub-categories: **Distance-Vector** protocols and **Link-State** protocols.

Distance Vector

- The distance-vector protocols forward packets based on distance and direction.
- Each distance-vector routing protocol uses an algorithm to calculate the best path to the destination host or network and sends that information to the neighbour routers that are using the same routing protocol.
- The distance-vector routing protocols use factors that are relative to distance and direction, such as hop counts, bandwidth, reliability, outgoing and receiving load, and delays.
- Contains a mechanism for exchanging routing information between neighbour routers that are configured within the same routing protocol.
- It also sends out its entire routing table to immediate neighbour routers.
- Contains a mechanism for calculating the best path to a destination and adding the route(s) within the routing table.
- Contains a mechanism that can detect and adapt to changes within the network topology and update the routing table.
- The following are distance-vector routing protocols:
  - **Routing Information Protocol (RIP)**
  - **Enhanced Interior Gateway Routing Protocol (EIGRP)**

Link-State

- These routing protocol uses the cumulative bandwidth to a destination network as the metric.
- Each router that is configured with a link-state routing protocol builds its topological map of the entire network, which helps the router determine the shortest path to the destination.

- Link-state routing protocols will only send an update to a neighbour router if there's a change within the network topology.
- The following are link-state routing protocols:
  - **Open Shortest Path First (OSPF)**
  - **Intermediate System - Intermediate System (IS-IS)**

External Gateway Protocol (EGP)

- EGPs are dynamic routing protocols that are implemented between ISPs to share public networks. These networks are more aptly referred to as **Autonomous Systems (ASs)**.
- EGP routes between AS(s). For instance, the **Border Gateway Protocol (BGP)** is the only EGP that exists within the networking industry, and it's used between ISPs to share their public networks with other ISPs on the internet.
- Hence, BGP is the path-vector routing protocol that allows ISP routers to learn about other public networks and maintain an up-to date routing table with BGP routes.

Administrative distance

Each dynamic routing protocol is assigned a unique AD value, which helps the router determine which route source is most trustworthy compared to others.
The following table shows the AD values for each route source for Cisco IOS routers:

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Fig. – Administrative distance chart

RIP

- It uses the **Bellman-Ford** algorithm, which uses hop count as the metric to calculate the best path to a destination network.
- It uses a maximum hop count of 15, which decrements by 1 each time a router has to forward the packet to the next hop along the way to the destination.
- If the hop count value on the packet reaches 0, the last router to change it to 0 will discard the packet.
- It uses UDP port 520 to exchange messages between RIP-enabled routers.
- The following diagram shows a network topology that contains routers that have been configured with the RIP dynamic routing protocol:

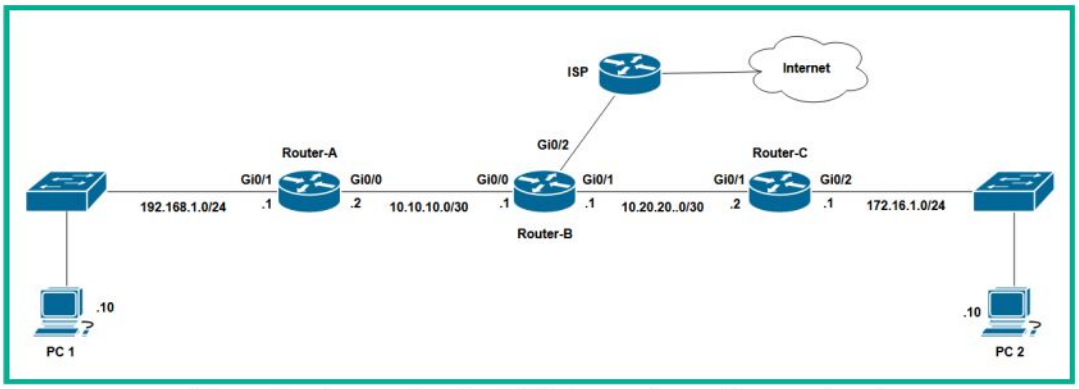


Fig. – Routers using the RIP dynamic routing protocol

- Let's assume **Router-A**, **Router-B**, and **Router-C** are all managed by an organization and have been configured with RIP as the preferred dynamic routing protocol.
- The following screenshot shows the RIP routes that have been installed within the routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
R       10.20.20.0/30 [120/1] via 10.10.10.1, 00:00:15, GigabitEthernet0/0 1
R    172.16.0.0/16 [120/2] via 10.10.10.1, 00:00:15, GigabitEthernet0/0 2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R*   0.0.0.0/0 [120/1] via 10.10.10.1, 00:00:15, GigabitEthernet0/0 3

Router-A#
```

Fig. – Routing table

- As shown in the preceding screenshot, there are three network routes that were discovered and added to the routing table of **Router-A**.
- These routes are both highlighted and labeled with numbers 1, 2 and 3. The value of 120 indicates the AD for RIP.

Drawbacks

- RIP broadcasts the entire routing of each router every 30 seconds, regardless of whether a network topology change occurred or not
- RIP does not support large networks with greater than 15 hops
- RIPv1 does not support networks that use custom subnet masks
- RIPv2 supports **Variable Length Subnet Mask** (**VLSM**) but doesn't allow you to manually specify the custom subnet mask during the configuration process

Important Note

- RIPng is the next generation of RIP and supports IPv6 routing. RIPv1 and RIPv2 support IPv4 routing on networks.
- RIPng uses UDP port 521 to exchange messages between routers.

OSPF

- **Open Shortest Path First** (**OSPF**) is a link-state dynamic routing protocol that's commonly used within many organizations' networks that are interoperable and with mixed vendor devices.
- OSPF uses its own datagrams and is tagged in the IP protocol as protocol number 89, so it does not use TCP or UDP. Additionally, OSPF uses the **Shortest Path First**

(**SPF**) algorithm, which determines the *cumulative bandwidth* to a destination network and chooses the path with the lowest cost.

- OSPF-enabled router exchanges Hello packets with their neighbour routers to establish an adjacency, which is like a mutual handshake between routers.
- Once the handshake has been established, each router will exchange **Link-State Advertisements** (**LSAs**) of their directly connected networks to their neighbour routers, which contain information about the state and the cost of how to reach the links.
- Once all the OSPF-enabled routers collect the LSAs from each router on the network, they will build the **Link-State Database** (**LSDB**), which is commonly referred to as the topology table.
- Hence, each OSPF-enabled router knows the entire network topology.
- Once the LSBD is completed, the SFP algorithm is used to determine the best path or shortest path to all known destination networks and adds those paths within the routing table of each OSPF-enabled router.

Important note

- OSPF-enabled routers send Hello packets to their neighbour routers every 10 seconds by default to indicate their presence on the network.
- However, a neighbour router is considered to be down or unavailable if a Hello packet is not received within 40 seconds.
- If a neighbour router is down, all the networks that have been learned from the neighbour router will be removed from the routing table.

The following network topology shows routers that have been configured with the OSPF dynamic routing protocol:

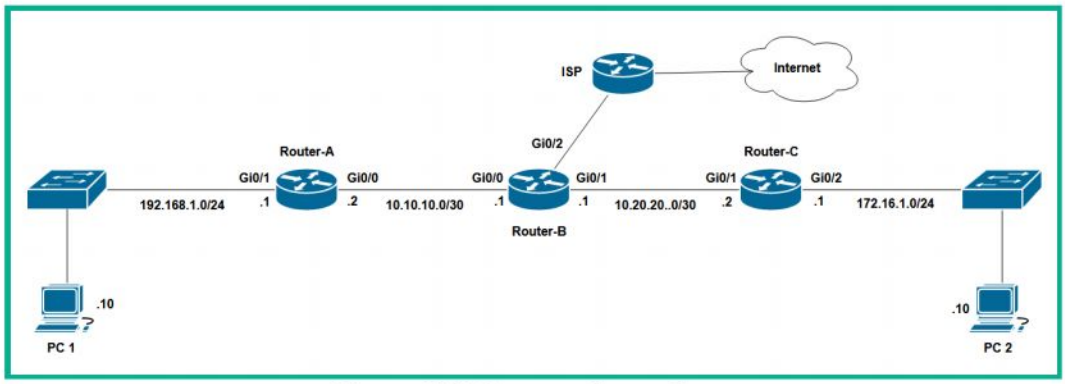


Fig. – OSPF network topology

- **Router-A**, **Router-B**, and **Router-C** are all managed by the same organization, and they are configured to use the OSPF dynamic routing protocol to share routing information.
- Therefore, each router will share routing information about their directly connected networks with their neighbour routers.
- The following screenshot shows the routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
O       10.20.20.0/30 [110/2] via 10.10.10.1, 00:00:13, GigabitEthernet0/0  1
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.1.0/24 [110/3] via 10.10.10.1, 00:00:03, GigabitEthernet0/0  2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 10.10.10.1, 00:01:28, GigabitEthernet0/0  3

Router-A#
```

Fig. – Router-A's routing table

Important note

OSPFv2 is used on IPv4 networks, while OSPFv3 is used on IPv6 networks.

EIGRP

- It is a hybrid, dynamic routing protocol that's implemented within organizations.
- It was a Cisco proprietary routing protocol until 2013.
- It uses protocol number 88, which is encapsulated directly into IP datagrams, rather than TCP or UDP.
- It uses **Diffusing Update Algorithm** (**DUAL**) to calculate the best path to a destination and a backup path to the same destination.
- DUAL uses the following factors as metrics to calculate the best path and a backup path:
  - Bandwidth
  - Delay
  - Reliability
  - **Outgoing load** (**TX load**)
  - **Receiving load** (**RX load**)
- By default, DUAL uses bandwidth and delay to calculate the metric for the best path and backup path to a destination network, while the other remaining metrics are disabled by default.
- However, network professionals have the option to enable all five metrics on Cisco IOS routers if they wish.
- The following network topology shows routers that have been configured with the EIGRP dynamic routing protocol:

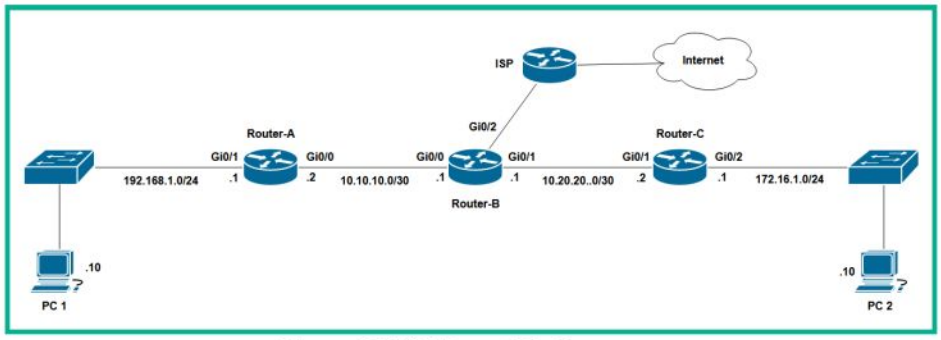


Fig. – EIGRP-enabled routers

- As shown in the preceding network topology, let's assume **Router-A**, **Router-B**, and **Router-C** have all been configured with EIGRP as the preferred routing protocol.
- DUAL will calculate the metric (cost) to reach each network and install the paths within the routing tables of each router.
- The following screenshot shows the EIGRP network routes within routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
D       10.20.20.0/30 [90/3072] via 10.10.10.1, 00:04:04, GigabitEthernet0/0 1
     172.16.0.0/24 is subnetted, 1 subnets
D       172.16.1.0/24 [90/3328] via 10.10.10.1, 00:00:15, GigabitEthernet0/0 2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
D*EX 0.0.0.0/0 [170/5376] via 10.10.10.1, 00:03:45, GigabitEthernet0/0 3

Router-A#
```

Fig. – Routing table

BGP

- It is a path-vector routing protocol that's used by ISPs to exchange routing information with each other.
- It operates on TCP port number 179.
- It is a very slow converging routing protocol that does not send updates as soon as a change occurs on the network topology.
- Hence, BGP was designed to operate between ASs such as ISPs on the network.
- Therefore, if a public network goes down an ISP, BGP will not immediately tell the other neighbours ISPs but wait a while to determine if the network will be restored.
- The following diagram shows the different ASs, such as ISPs, interconnected using BGP to share their routing information:

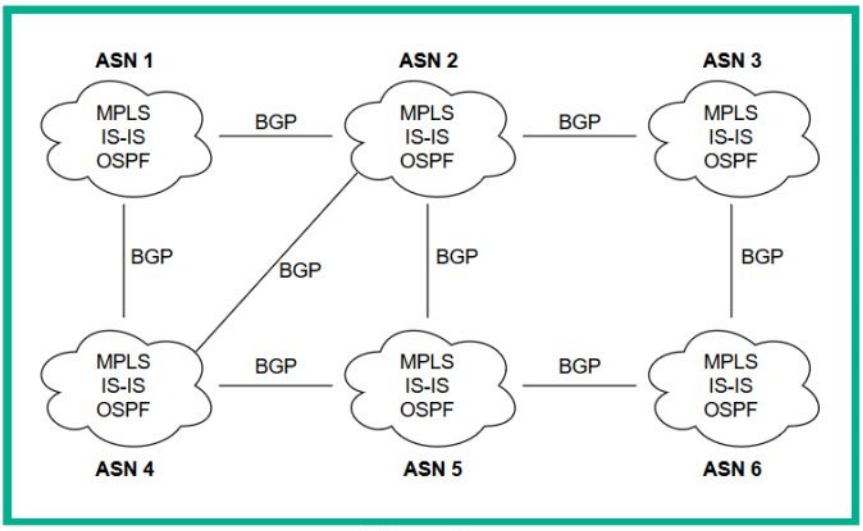


Fig. – Ass

- As shown in the preceding diagram, each ISP is assigned a unique **Autonomous System Number** (**ASN**) that allows one ISP to establish an adjacency with another ISP using BGP to share routing information of their public networks.
- An AS is a large collection of public networks that are all managed by a single organization such as an ISP.
- Within each ISP's administrative domain, they use IGPs and other service provider technologies to forward traffic within their service provider network.
- However, BGP allows an AS to advertise their public networks to other ISPs around the world, ensuring each ISP knows how to forward packets to any public network on the internet.

Important note

When discussing the topic of BGP, it's common to think this version of BGP is strictly designed for the internet. However, there are two versions of BGP: **External BGP** (**eBGP**) and **Internal BGP** (**iBGP**). eBGP is used between different ASs, while iBGP is used within an AS.

The following screenshot shows the BGP routing table of a router:

```
ACME1#show ip bgp
BGP table version is 6, local router ID is 192.168.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  1.1.1.0/30       1.1.1.1                  0      0      0 65003 ?
*> 1.1.1.4/30       1.1.1.1                  0      0      0 65003 i
*> 1.1.1.8/30       1.1.1.1                  0      0      0 65003 i
*> 172.16.10.0/24   1.1.1.1                  0      0      0 65003 ?
*> 192.168.0.0/24   0.0.0.0                  0      0  32768 i

ACME1#
```

Fig. – BGP routing table

Static routing

- Static routing allows network professionals to manually configure destination network routes within the routing table of a router.
- Static routes always take precedence over any network route that was learned using a dynamic routing protocol.
- Network professionals can configure static routes on all routers within a small network.
- If the network topology changes, the static routes within the routers will not automatically update the changes within the topology compared to dynamic routing protocols.
- Static routes do not adapt to the changes of the network – they require a network professional to always update the configurations of static routes within all the routers of an organization.
- Hence, static routing is workable for small networks that do not change frequently and where there are fewer IP networks.

Issues in static routing

- If a network professional misconfigures a static route on a router, the router will not forward packets correctly to the intended destination network.
- when using static routing is that a router will still forward packets to a network that is no longer reachable.
- The following are various types of static routes:
  Standard static route: This type of static route specifies how to reach a destination network.

Default static route: A default static route is used when no other routes within the routing table of a router match the destination IP address of a packet. This type of route is usually configured to forward packets to the internet.

Floating static route: This type of static route functions as a backup route to a primary route on a router. For instance, if a primary route is no longer available, a floating static route is usually configured with an AD that is higher than the primary route.

Summary static route: A summary static route is used to represent multiple destination IP networks in the form of a single, consolidated static route. Summary static routes are used to reduce the size of a routing table that has too many routes that are forwarding traffic to the same destination.

- The following diagram shows a simple network topology where each router has been configured with static routing to forward traffic to remote networks:

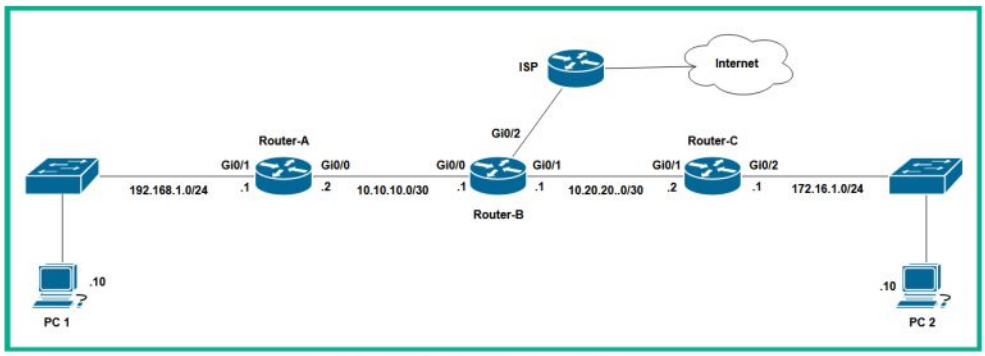


Fig. – Network topology

- As shown in the preceding diagram, **Router-A** has to be configured with static routes to forward traffic to 10.20.20.0/30, 172.16.1.0/24, and the internet, as these networks are not directly connected to the router.
- The following screenshot shows the static routes within the routing table of **Router-A** that are used to forward packets to the 10.20.20.0/30 and 172.16.1.0/24 networks:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
S       10.20.20.0/30 [1/0] via 10.10.10.1
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0/24 [1/0] via 10.10.10.1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.10.10.1

Router-A#
```

Fig. – Static routes

- Lastly, the following screenshot highlights the *default static route*, which indicates the *gateway of last resort* on the routing table of **Router-A**:

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.10.10.0/30 is directly connected, GigabitEthernet0/0
L       10.10.10.2/32 is directly connected, GigabitEthernet0/0
S       10.20.20.0/30 [1/0] via 10.10.10.1
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0/24 [1/0] via 10.10.10.1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
S*    0.0.0.0/0 [1/0] via 10.10.10.1

Router-A#
```

Fig. – Default static route

- As shown in the preceding screenshot, the default static route is used when no other routes within the routing table of a router have a match for the destination IP address within a packet.
- Additionally, the next hop address of a default static route is used as the gateway of last resort on the router.

Bandwidth management

- If a network becomes saturated or congested with too many packets, each device that wants to send a message tries to access the available bandwidth on the network to transmit its packets, which becomes an issue.
- Each networking device has two buffers for temporarily storing messages:
  - Port buffer
  - Shared buffer
- **Port buffer:** It exists on each interface of a networking device and is used to temporarily store inbound messages that have to be processed by the device. The port buffer is used to temporarily store outbound messages that have already been processed by the device and are waiting to be placed on the physical network.
- **Shared buffer:** It is simply used to temporarily store all the messages in a common buffer that is shared by all the interfaces and memory of the networking device.
- Network professionals use two types of solutions to ensure specific traffic types have a high priority of accessing the bandwidth over others on a network, as follows:
  - **Traffic shaping**
  - **Quality of Service (QoS)**

Traffic Shaping:

- It allows network professionals to create delays of some traffic types using a traffic profile.
- This technique is commonly used to improve the latency and optimize the performance of a network while increasing the allocation of bandwidth for specific traffic types.
- This allows higher priority traffic to flow with optimal speed over the network while lower priority traffic is delayed.

Quality of Service (QoS)

- It is another solution that is commonly implemented within many organizations' networks that helps control traffic on a network while ensuring the improved performance of mission-critical applications over limited network capacity.
- The following metrics are used within QoS to measure types of traffic over a network:

Bandwidth: Bandwidth is the number of bits that can be transmitted in a second between a source and a destination.
Congestion: In a network, congestion results in packets being delayed while they're arriving at their destinations. Congestion occurs when there is a lot more traffic on the network, which saturates all the available bandwidth.
Delay: Delay is used to measure the time a packet takes to travel between a source and a destination.
Jitter: Jitter measures the variation in the delay times of incoming packets on a network.
Packet loss: Packet loss measures how many packets are discarded or dropped between a source and destination over a given time.

- The following steps show how QoS prioritizes traffic on a network:

1. **Classification**: Inbound traffic on a networking device is inspected and placed within a waiting queue based on the **Differentiated Services** (**DS**) field of an IPv4 packet and the **Traffic Class** field of an IPv6 packet.
2. **Marking**: This is the process where the QoS tools on the networking device modify one or more fields within the packet header to insert a value.
3. **Queuing**: This phase is responsible for managing all the queues for outgoing messages on a networking device. Traffic is sent out of a networking device based on its priority.
4. **Policing and shaping**: The policing feature is responsible for discarding or dropping packets, while the shaping feature is responsible for keeping or holding the packets within a queue.
5. **Congestion avoidance**: This feature is used to reduce the amount of congestion that exists within a network to reduce packet loss.

- The following diagram shows the classification process when using QoS:

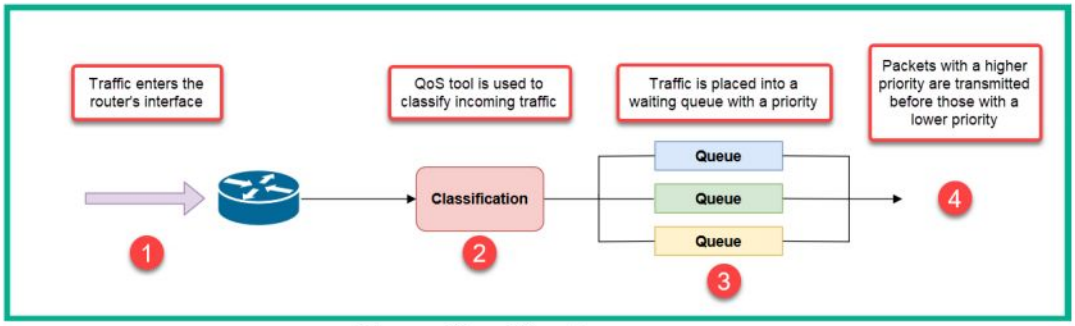


Fig. – Classification process

Delving into switching concepts

- Network switches are designed and configured to forward frames to their destinations over a network.
- Network professionals can distribute power over network cables to wireless access points and VoIP phones, prevent a Layer 2 loop on a switching network, aggregate multiple physical links into a single logical link between switches, and discover connected devices on a network.

PoE

- Power over Ethernet (PoE) is the technology that allows Direct Current (DC) power over a copper Ethernet cable to devices to reduce the need for a dedicated power supply and Alternating Current (AC) power outlets.
- PoE is defined by **IEEE 802.3af**, which was created in 2003.

- It specifies how electrical power can be delivered to another device by using the spare pairs within a copper Twisted Pair cable. These spare pairs are pins 4 and 5 or pins 7 and 8.
- However, PoE can use the data pairs of an Ethernet cable; these pairs are pins 1 and 2 or pins 3 and 6.
- PoE provides up to 15.4 watts of DC power with a maximum of 350 **milliamps** (**mA**) of electrical current.
- **PoE+**, an improved variation of PoE, was defined by **IEEE 802.3at** in 2009, which provides an increased power rating of up to 25.5 watts with a maximum of 600 mA of electrical current to devices.

Spanning-Tree

- A Layer 2 loop is formed when there are redundancy paths within a switch network.

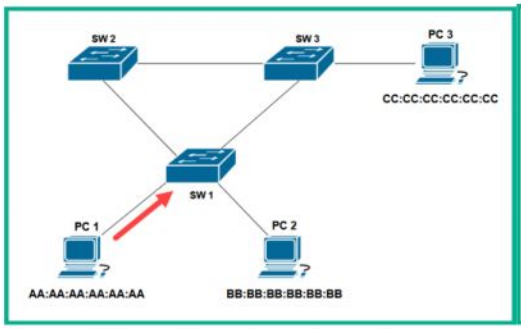


Fig. – Looping phase 1

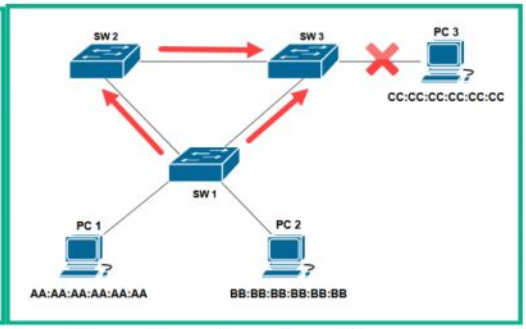


Fig. – Looping phase 2

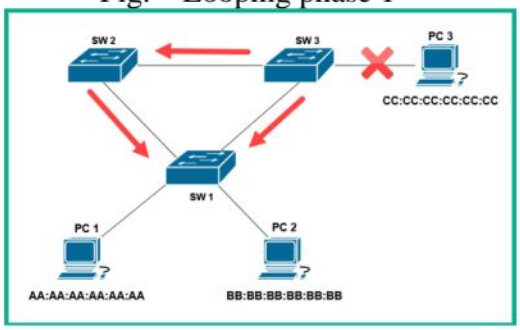


Fig. – Looping phase 3

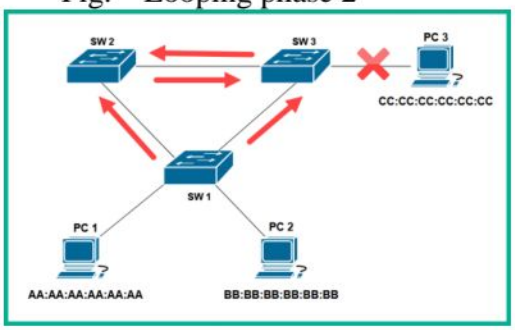


Fig. – Looping phase 4

- When a PC1 becomes unavailable SW3 does not have the MAC address of PC3.
- When destination MAC address is unavailable switch broadcasts the frames to all the interfaces except from the interface from which it is received.
- This occurs on all switches and frames fall into infinite loop.

- Another issue with redundant paths on a switch network is creating duplicate messages between a source and a destination host.

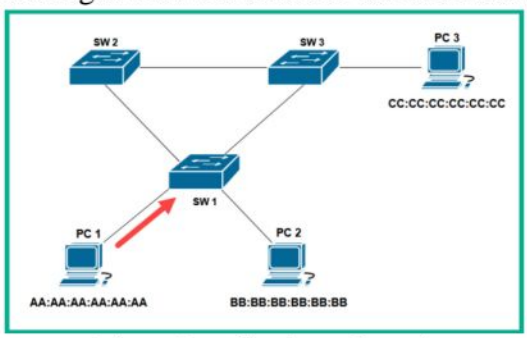


Fig. – Duplication phase 1

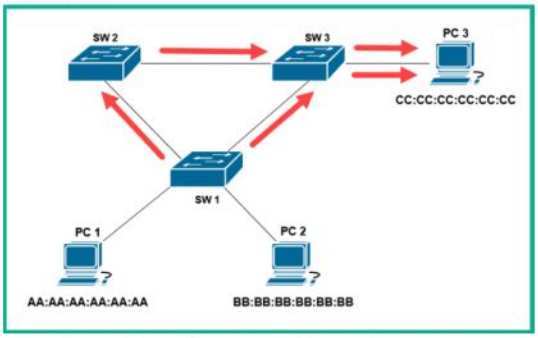


Fig. – Duplication phase 2

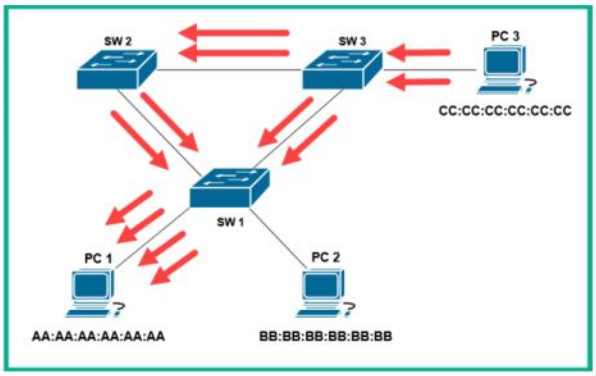


Fig. – Duplication phase 3

- To resolve the issues that are created by redundancy on a switch network, the **Spanning-Tree Protocol** (**STP**) was designed as a Layer 2 loop prevention protocol that can detect any physical Layer 2 loops on a network and logically block the redundant path.
- This ensures only one active logical path between a source and destination is available.
- STP is defined by the **IEEE 802.1D** standard for Layer 2 loop prevention on networks.
- The following diagram shows a network topology with STP enabled on all switches that have already blocked a redundant path:

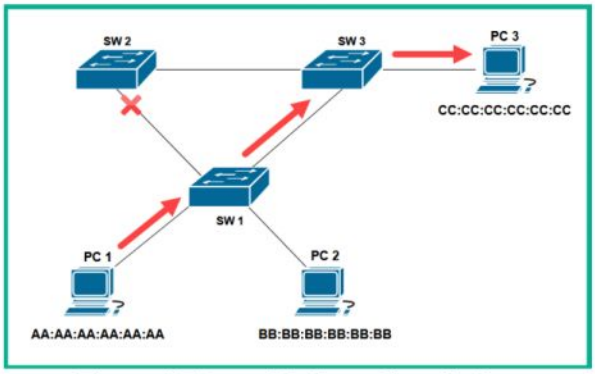


Fig. – STP enabled on all switches

- As shown in the preceding diagram, whenever **PC 1** wants to send a message to **PC 3**, there is one active logical path between both devices that prevents a Layer 2 loop on the network.
- However, if the primary path is unavailable, STP can detect whether a path is unavailable and automatically redirect the flow of traffic using a backup path, as shown in the following diagram:

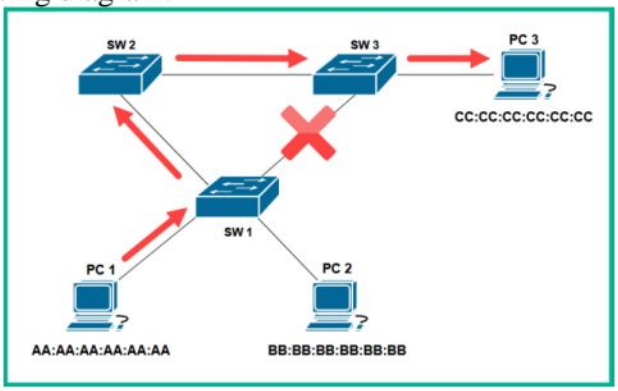


Fig. – Detecting a network failure

Spanning Tree Protocol (STP)

- Whenever a switch is powered on, it sends **Bridge Protocol Data Unit** (**BPDU**) frames every 2 seconds to their neighbor switches. A BPDU contains the switch's priority value, **Extended System ID** (**Ext- ID**), and the MAC address, as shown here:

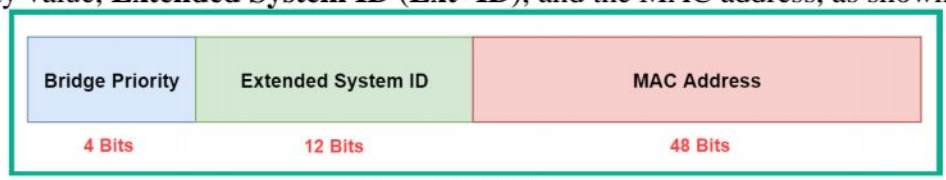


Fig. – BPDU frame

Root Bridge.

- The Root Bridge informs all other switches to create one logical, loop-free path between any devices on the network.
- Therefore, if multiple switches are interconnected to create physical redundancy, the Root Bridge will ensure all physical redundant paths are logically blocked and only one active, loop-free path is available.
- The switch with the lowest bridge priority gets elected as the Root Bridge on the network.
- Since all Cisco switches have a default bridge priority of 32768, network professionals commonly configure their core or distribution layer switches to become the Root Bridge on the network by lowering the bridge priority by decrements of 4096.
- Hence, the switch with the lowest bridge priority becomes the Root Bridge. If all the switches have the same default bridge priority of 32768, then the switch with the lowest MAC address value will be elected are the Root Bridge on the network.
- Once the Root Bridge has been elected, all the other switches on the network will create a logical path that points to the Root Bridge as it becomes the *central reference point* for all traffic within the network.
- To get a better understanding of how STP identifies redundant paths and ensures only a loop-free path is active on the network, let's take a look at the following network topology:

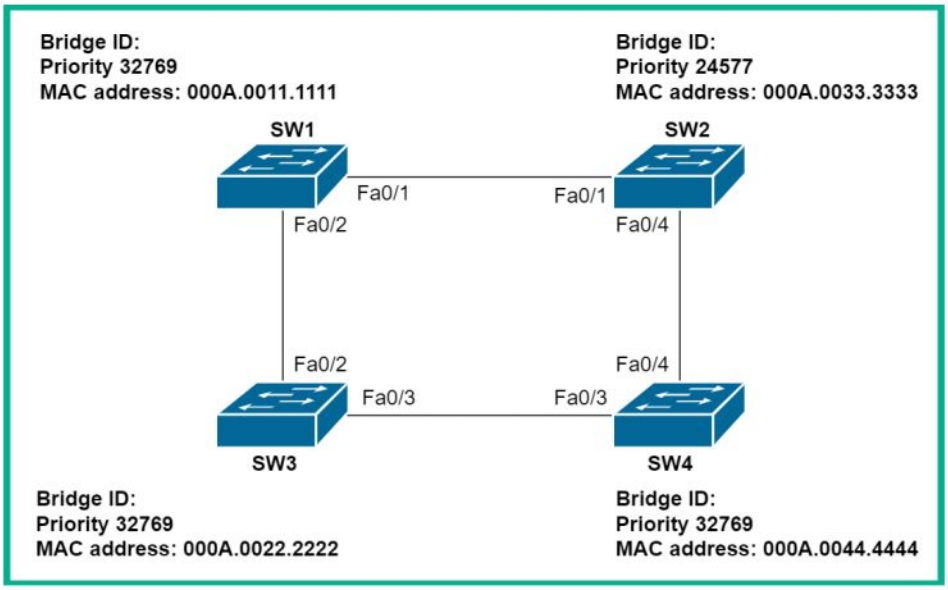


Fig. – Spanning-Tree network topology

- As shown in the preceding diagram, each switch has a priority value (priority + Ext-ID value) and a unique MAC address. The following is my strategy for identifying the root bridge and port states on a network:
- **Identify the root bridge**: The root bridge is the central reference port for all traffic within the **Virtual Local Area Network** (**VLAN**).
- **Identify root ports**: These are ports closest to the root bridge but not on the root bridge.
- **Identify designated ports**: These are non-root ports that are in a forwarding state.
- **Identify alternate/blocking ports**: These are ports that are logically blocked by STP to prevent a Layer 2 loop on a redundant path.
- We must follow these steps to identify the root bridge and port status on the topology:

1. SW2 has the lowest priority value and therefore becomes a Root Bridge.
2. Next, the root ports are those that are closest to the root bridge, therefore SW1 FastEthernet 0/1 and SW4 FastEthernet 0/4 are root ports.
3. Next, we need to determine the port roles on SW3. There are two paths from SW3 to the root bridge – that is, SW3 to SW1 and SW3 to SW4 – and both of these paths have the same interface bandwidth. The switch with a lower Bridge ID value will be the preferred path to the root bridge. SW1 has a lower Bridge ID value because its MAC address is lower compared to SW4. As a result, SW3 FastEthernet 0/2 will be a root port.
4. Since the preferred path from SW3 to the root bridge is via SW1, then SW1 FastEthernet 0/2 will become a designated port.
5. Next, all ports on the root bridge are designated ports by default.
6. Finally, the ports between SW3 and SW4 are yet to be assigned so that one will become a designated port and the other will be an alternate/blocking port. In this instance, the switch with the lower Bridge ID value will take precedence in having a designated port while the other switch will assign its port to an alternate/blocking port. Therefore, SW3 FastEthernet 0/3 becomes a designated port and SW4 FastEthernet 0/3 becomes the alternate/blocking port.

- The following diagram shows the port labels on each switch within the topology:

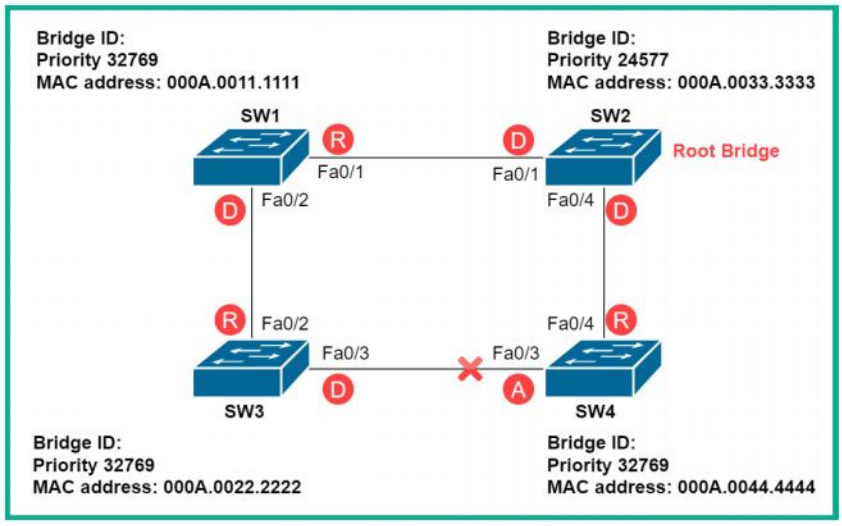
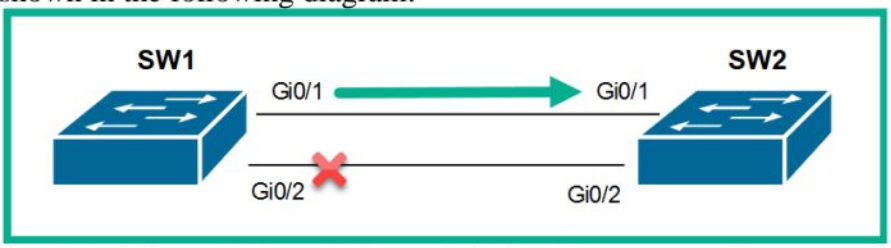


Fig. – STP port labels

Port aggregation

- EtherChannel or port aggregation allows network professionals to combine multiple physical links into a single logical connection between switches to aggregate the bandwidth between devices.
- However, if a network professional connects two network cables to each of the Gigabit Ethernet interfaces of two switches, only one link will be active for transmitting messages; the other will be logically blocked by STP to prevent a Layer 2 loop, as shown in the following diagram:



- When using EtherChannel, the existing switch interfaces are used to create the actual EtherChannel link, so network professionals do not need to upgrade the hardware components of a switch that already supports the technology.
- EtherChannels create load balancing of network traffic between switches on a network, which helps with traffic aggregation while providing redundancy.
- The **Link Aggregation Control Protocol** (**LACP**) is an open source protocol defined by **IEEE 802.3ad** that allows any vendor of switches to form EtherChannels between switches on a network.
- An LACP Etherchannel is formed when two switches use the Active LACP mode on their interfaces.
- The following table shows the results of the different LACP modes on **SW1** and **SW2**:

LACP

SW1	SW2	Status
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	No Configuration	No
On	Active	No
On/Passive	Passive	No

Fig. – LACP modes

- The following are the requirements for establishing an EtherChannel between switches on a network:
  - The same type of interface must be used between switches
  - The same number of interfaces must be used between switches
  - The speed and duplex need to be the same on all interfaces that are forming the EtherChannel
  - The same configurations must be applied to all interfaces that are forming the EtherChannel
- The following diagram shows an example of an EtherChannel that's unable to be formed because there's a duplex mismatch on **SW1**:

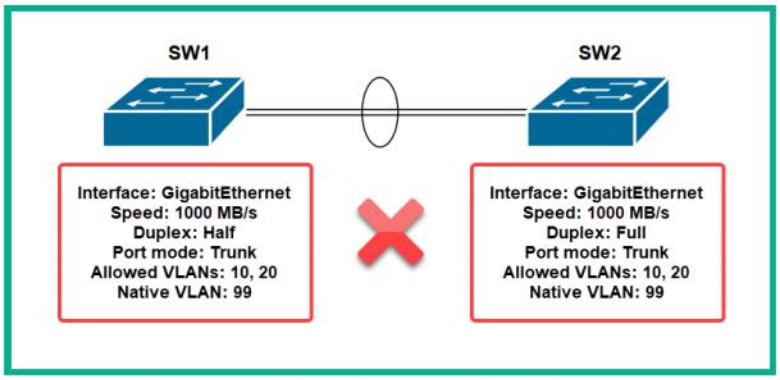


Fig. – Unable to form an EtherChannel

- When the configurations are the same on the interfaces that are being used to create the EtherChannel between **SW1** and **SW2**, the EtherChannel is established between switches, as shown here:

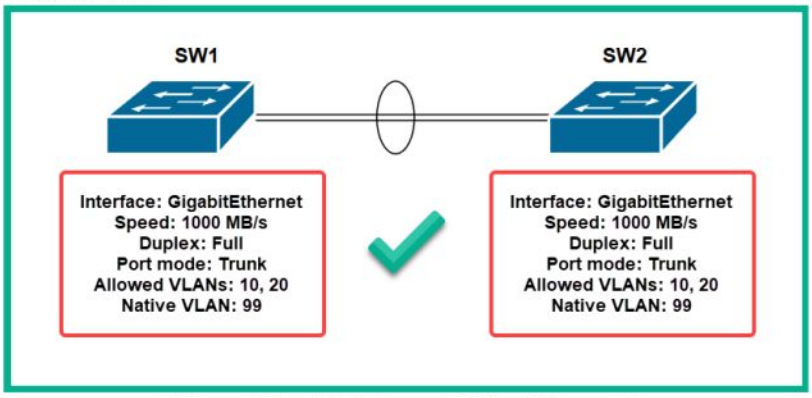


Fig. – Establishing an EtherChannel

- If one of the physical interfaces of an EtherChannel is unavailable or has any misconfigurations, the entire EtherChannel is broken and all the physical interfaces will function independently from each other.

Neighbour discovery protocol

- Neighbour discovery protocol to help both network professionals and networking devices identify the types of devices on their network.
- There are two types of Neighbour discovery protocols.
  - Cisco Discovery Protocol (CDP)
  - Link-Layer Discovery Protocol (LLDP)

Cisco Discovery Protocol (CDP)

- It is a Cisco proprietary protocol that operates between Layers 2 and 3 of the OSI networking model.
- It is used to assist Cisco switches to learn about their directly connected neighbours, such as other switches and routers.
- On Cisco devices, CDP is enabled by default to exchange advertisement messages using a multicast address of 01:00:0C:CC:CC:CC.
- A CDP message contains the following details about the sender device:
  - Cisco IOS version of the switch or router
  - Device model and type
  - Connected interfaces for both local and remote devices
  - The hostname of the device
- The following screenshot shows the devices that are connected to a Cisco switch that uses CDP:

```
SW3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme     Capability   Platform     Port ID
R1               Gig 0/1           157              R       C2900        Gig 0/1
SW1              Fas 0/24          157              S       2960         Fas 0/24
SW2              Fas 0/23          157              S       2960         Fas 0/23
R1               Gig 0/1           157              R       C2900        Gig 0/1.10
R1               Gig 0/1           157              R       C2900        Gig 0/1.20
R1               Gig 0/1           157              R       C2900        Gig 0/1.30
SW3#
```

Fig. – CDP details

- As shown in the preceding screenshot, Device ID indicates the hostname of the directly connected device, Local Interface identifies the interface used by the connected device, Holdtime indicates how long the information will remain in the table, Capability indicates the type of device, Platform indicates the model of the device, and Port ID indicates the local interface that's used to establish the connection.
- Since CDP is a Cisco proprietary protocol, it's not interoperable with non-Cisco devices on a network.

Link-Layer Discovery Protocol (LLDP)

- It is another discovery protocol that operates over Layer 2 of the OSI network model and is supported on both Cisco and non-Cisco devices.
- LLDP is defined by **IEEE 802.1AB**, which makes it interoperable on other vendor devices and provides similar details as the CDP on a network.
- The following screenshot shows the LLDP details on a Cisco switch:

```
SW3#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
SW1                 Fa0/24         120        B               Fa0/24
R1                  Gig0/1         120        R               Gig

Total entries displayed: 2
```

Fig. – LLDP details

- In many organizations with mixed vendor equipment, LLDP is the preferred neighbour discovery protocol to help both network professionals and networking devices identify the types of devices on their network.

Exploring VLAN

- Network professionals implement a **Virtual Local Area Network (VLAN)** within their switches to segment physically connected components on switches. This allows them to be logically organized.
- There are many benefits to implementing VLANs, such as the following:
    - Improving network performance and management
    - Reducing the size of a broadcast domain
    - Improving network security
    - Reducing cost
- The following diagram provides a visual representation of VLANs within a company:
- As shown in the following diagram, if **PC 2** generates a lot of broadcast messages, only **PC 5** and **PC 8** will be affected as they belong to the same VLAN as **PC 2**.

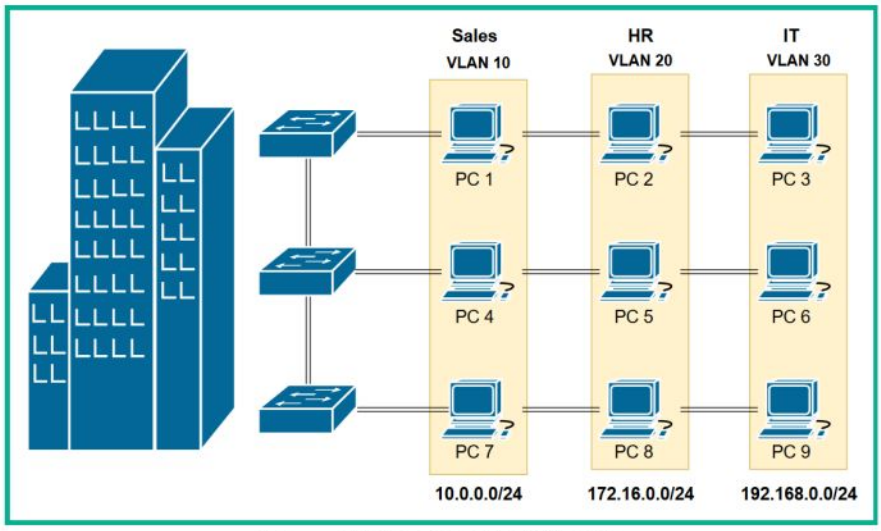


Fig. – Network with VLANs

- Therefore, any device that sends a frame to a switch interface will be assigned an **IEEE 802.1Q** tag, which contains the VLAN ID of the interface.
- This technique ensures all frames are tagged with a VLAN ID, which helps the switch logically separate one piece of VLAN traffic from another.
- To understand how VLAN tagging is used within a switch, let's take a look at the following diagram, which represents a switch:

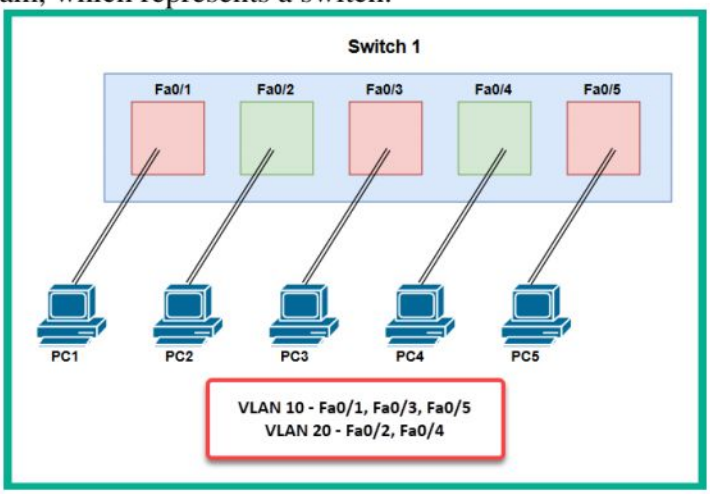


Fig. – VLAN assignment to each interface

- To ensure intercommunication between VLANs, network professionals will need to implement a Layer 3 or a dedicated router that has been configured to perform inter-VLAN routing, a technique that allows devices from one VLAN to communicate with devices on another VLAN.
- Trunk links are point-to-point connections from switch-to-switch or switch-to-router. Trunks allow multiple VLANs to carry their traffic between switches and routers.
- Access ports allow only one statically assigned VLAN on the interface, a trunk link allows many VLANs at the same time.

Types of VLANs

Default VLAN

- The default VLAN is simply the VLAN that is created by the vendor.
- The default VLAN is VLAN 1 and all the interfaces of the switch are assigned to VLAN 1 by default, so a new enterprise-grade switch will work out of the box.
- However, since all interfaces are assigned to VLAN 1 by default, it's not recommended to use the default VLAN for security reasons.

Data VLAN:

- The data VLAN is usually configured to transport traffic generated by end devices such as computers, servers, printers, and access points.

Native VLAN:

- The native VLAN is used to transport *untagged* traffic on an IEEE 802.1Q trunk link.
- Whenever an end device such as a computer sends traffic to a switch, the receiving switch port inserts an IEEE 802.1Q tag VLAN ID into the frame; this is known as *tagged* traffic.
- Untagged traffic does not originate from a VLAN; it is self-generated traffic from the switch itself, such as CDP and LLDP messages.

Management VLAN:

- The management VLAN is used to remotely access the switch over a network for management purposes.
- Simply put, the management VLAN is also referred to as a **Switch Virtual Interface** (**SVI**) and is configured with an IP address and subnet mask.

Voice VLAN:

- Voice traffic uses UDP, which does not provide any reliability for the delivery of each packet. Since a converged network is the recommended type of network infrastructure, having a dedicated network for all voice traffic is preferable.
- Using a dedicated VLAN to transport voice traffic will ensure that all the voice traffic is kept separate from the other traffic types on the physical network.
- Important note
- Only one data VLAN can be assigned to a switch port; this type of assignment will create an **access port** on the switch. Two VLANs can be assigned to an access port, but only if the other is a voice VLAN; therefore, only one data and one voice VLAN are allowed on a single access port.

Important note

- Only one data VLAN can be assigned to a switch port; this type of assignment will create an **access port** on the switch. Two VLANs can be assigned to an access port, but only if the other is a voice VLAN; therefore, only one data and one voice VLAN are allowed on a single access port.
- The following diagram shows that VLAN 10 and 20 have been configured on the network, but the connection between the two switches is an access port that's only been statically assigned VLAN 10:

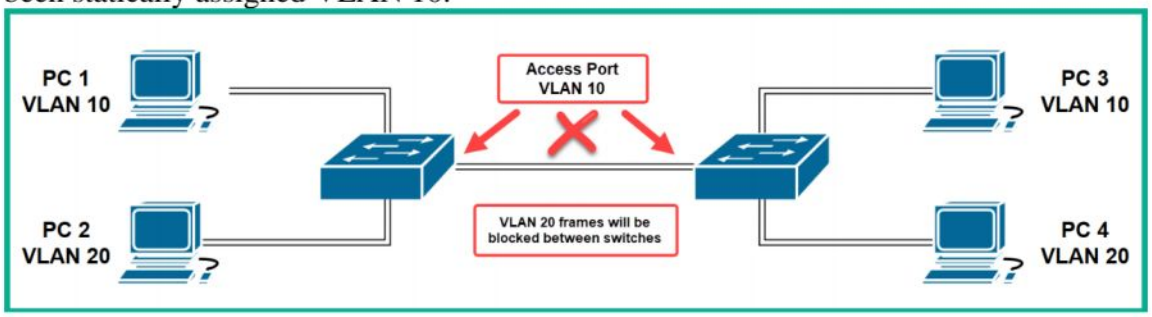
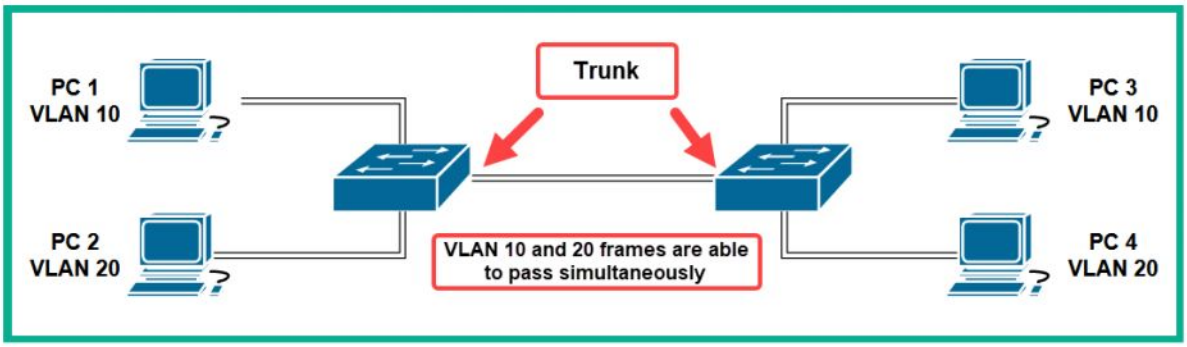


Figure 9.45 – Issues with access ports

- As shown in the preceding diagram, **PC 1** and **PC 3** will be able to exchange messages between the two switches but **PC 2** and **PC 4** will not be able to communicate with each other.
- To solve this issue, a trunk is needed between the two switches to allow both VLAN 10 and 20 traffic, as shown here:
- The following are some key points about port tagging and IEEE 802.1Q:



- When a source device such as a computer sends a frame into a switch port, the switch will insert an IEEE 802.1Q tag into the frame.
- Access ports allow network professionals to configure one data VLAN on an interface.
- The IEEE 802.1Q tag contains the VLAN ID that is assigned to the switch's interface. This tag helps the switch isolate one piece of VLAN traffic from another VLAN, so each VLAN is logically separated from the others.
- The IEEE 802.1Q tag is kept on the frame, so long as it is passing between switches. The IEEE 802.1Q tag is only removed when the switch is sending outbound traffic from an access port.
- Trunks are special interfaces that are configured on a switch to transport multiple pieces of VLAN traffic between switches.

Exploring wireless networking (Chapter-10):

Wireless Routers:

- Wireless routers are common wireless networking devices that are commonly found within Small Office Home Office (SOHO) networks.
- It is simply a router, switch, and access point within a single unified device.
- A wireless router is suitable for small wireless networks such as those within homes and small office environments.

The following snippet shows the back of a Cisco Linksys 160N wireless router:

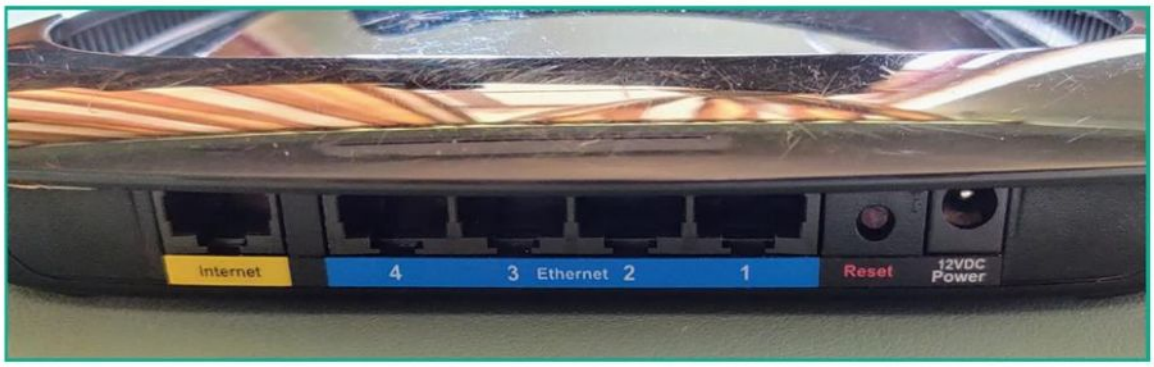


Figure 10.1 – Wireless router

- There are five interfaces that allow wired Ethernet connections.
- The **Internet port or Wide Area Network (WAN) port**, allows establishing a wired connection from the internet modem to the wireless router. It provides internet access to devices that are connected to the wireless router.
- Without internet access on the wireless router, wireless clients will be able to communicate with each other but won't be able to access any resources on the internet.

The following diagram shows the connection between an internet modem and a wireless router:

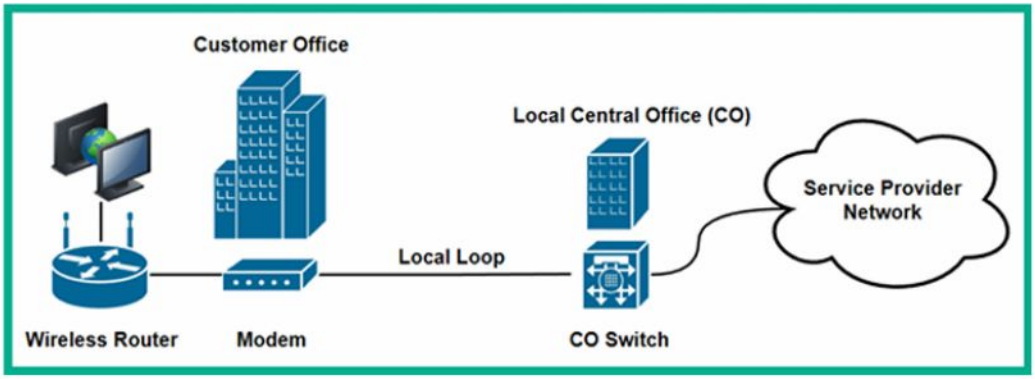


Figure 10.2 – Providing internet to a wireless router

- The wireless router has one or more **Ethernet ports** that operate like a typical network switch, allowing to interconnect clients with each other using a wired connection.

- The built-in switch within the wireless routers functions like a typical network switch that forwards frames between devices on the wired and wireless networks.
- Therefore, all devices that are connected to the wireless router, whether on the wireless or wired network, will be able to communicate and exchange messages with each other.
- The router function is used to forward packets between these different IP subnets and to the internet.

Access Points:

- Generate a radio frequency within the 2.4 GHz and/or 5 GHz band to create a wireless network.
- Allows wireless clients, such as mobile devices, to establish a connection to the access point and access the resources on the wired network.
- Unlike wireless routers, access points do not have any routing or switching functionality.
- **Thin-client access point** are used to create a wireless network and forward frames to the wired network and vice versa. They have no configuration capability. They are connected to a wireless controller.
- **Fat-client access points** can be individually configured and don't require a controller.
- Access points are simply used to allow wireless clients to access resources on the organization's network seamlessly as if they were connected to the wired network.

Beacons, probes, stations, and SSIDs:

SSID:

- The **Service Set Identifier (SSID)** is simply the name of the wireless network that allows wireless clients to identify one wireless network from another.
- When a wireless router or access point is powered on, the firmware and configurations are loaded in memory and the device begins to broadcast its presence within the vicinity.

Beacons:

- Wireless routers and access points continuously broadcast **beacons**
- Beacons contain specific information such as the SSID, wireless encryption standard, operating channel, and even their Media Access Control (MAC) address.
- The beacons are detected and inspected by any device that has a supported wireless network adapter such as smartphones, tablets, Internet of Things (IoT) devices, and laptops, therefore allowing a user to identify wireless networks within the vicinity.
- Wireless clients move into the range of the wireless signal that's generated by the wireless router or access points, they will be able to capture the beacons and inspect them to determine the wireless network that's close by.

The following diagram shows a wireless router broadcasting beacons:

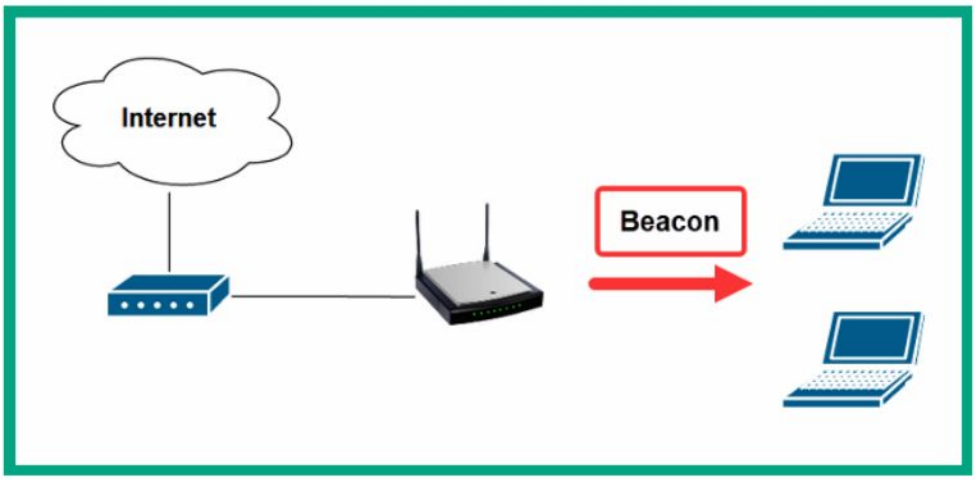


Figure 10.4 – Wireless beacons

- Wireless routers and access points provide the capability of disabling the SSID broadcast as a technique of hiding your wireless network from wireless clients.
- However, this technique does not add any layer of security as a seasoned hacker or cyber security professional can discover a hidden wireless network within a few seconds using very specialized skills, such as performing wireless reconnaissance by capturing beacons and probes.
- If an IT professional chose to disable the SSID broadcast feature, the wireless router will not insert the SSID but still include all other information within each beacon that will be broadcasted.

Probes:

- Probe requests are a type of Wi-Fi management frame.
- They are used simply for network discovery.
- The probe request will contain the SSID of a known network.
- The probes allow the client to seek any of the wireless networks via their SSIDs that are stored within the Preferred Network List (PNL).
- Once a wireless network is found within the signal range, the client will attempt to create an association with the wireless network.
- A seasoned hacker or cyber security professional can capture the probes to determine the wireless networks that are stored on a client and attempt to perform an AP-less attack to retrieve the password/ passphrase of an organization's wireless network.

The following snippet shows the basic configuration page of a wireless router:

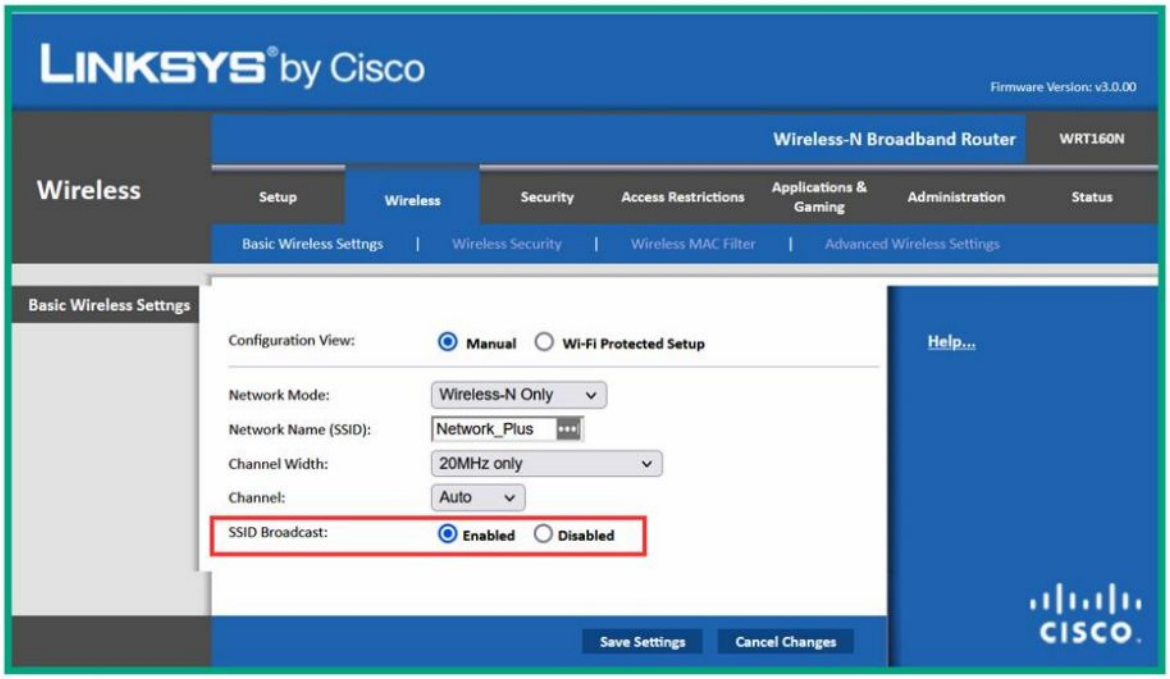


Figure 10.5 – Wireless router basic configuration page

As shown in the preceding snippet, the basic wireless configuration page allows a user to configure the wireless operating standard, SSID, channel width, channel number, and whether to enable or disable the SSID broadcast on the device.

Stations:

- When a wireless client (**station**) establishes a connection to a wireless router or access point, it's referred to as an association.
- When a client joins a wireless network, the client saves both the SSID and password into a Preferred Network List (PNL) that allows the user to easily re-join the same wireless network in the future.
- This enables the wireless network adapter on a client to begin sending probes for each entry within the PNL on the device.
- Wireless clients such as laptops, smart TVs, and IoT devices are examples of stations.

CHAPTER 11

Assuring Network Availability

Network performance metrics

➢ Performance metrics helps

- to determine whether the network is operating as expected
- to know the delivery of network resources is affected

➢ The common performance metrics used :

1. **Temperature**
2. **Central processing unit (CPU) utilization**
3. **Memory utilization**
4. **Bandwidth**
5. **Latency**
6. **Jitter**

- The more load that's being processed by a networking device,
- the more computing power,
- increases the **temperature** of each device within the organization.

- If the operating system of a device detects it is too hot, sensors will automatically turn off the device to prevent hardware failure.
- if the temperature is too low, condensation can appear on the electronic components of the device.

- If a networking device is not forwarding traffic as quickly as expected, then the **CPU utilization** needs to checked
- to determine whether the computing power of the device is being exhausted; causing lower performance of the device.

- The more **memory** that's available on a device
- allows the user to execute and run more applications simultaneously on a host.
- If there isn't enough available memory on a networking device it requires immediate attention.

- **Jitter** measures the variation of delay times of incoming packets on a network
- All packets that are received from the same sender should have the same latency.
- Jitter increases on the network as users are sending and receiving messages and saturating the network.

- **Latency** is the time between a request and response over a network.
- slow response times, there can be many possible causes.
- Once the traffic is captured, examining the response times the affected area is isolated.
- Examining the latency, any changes within each packet are observed, such as faulty packets or packets that are being retransmitted on the network.

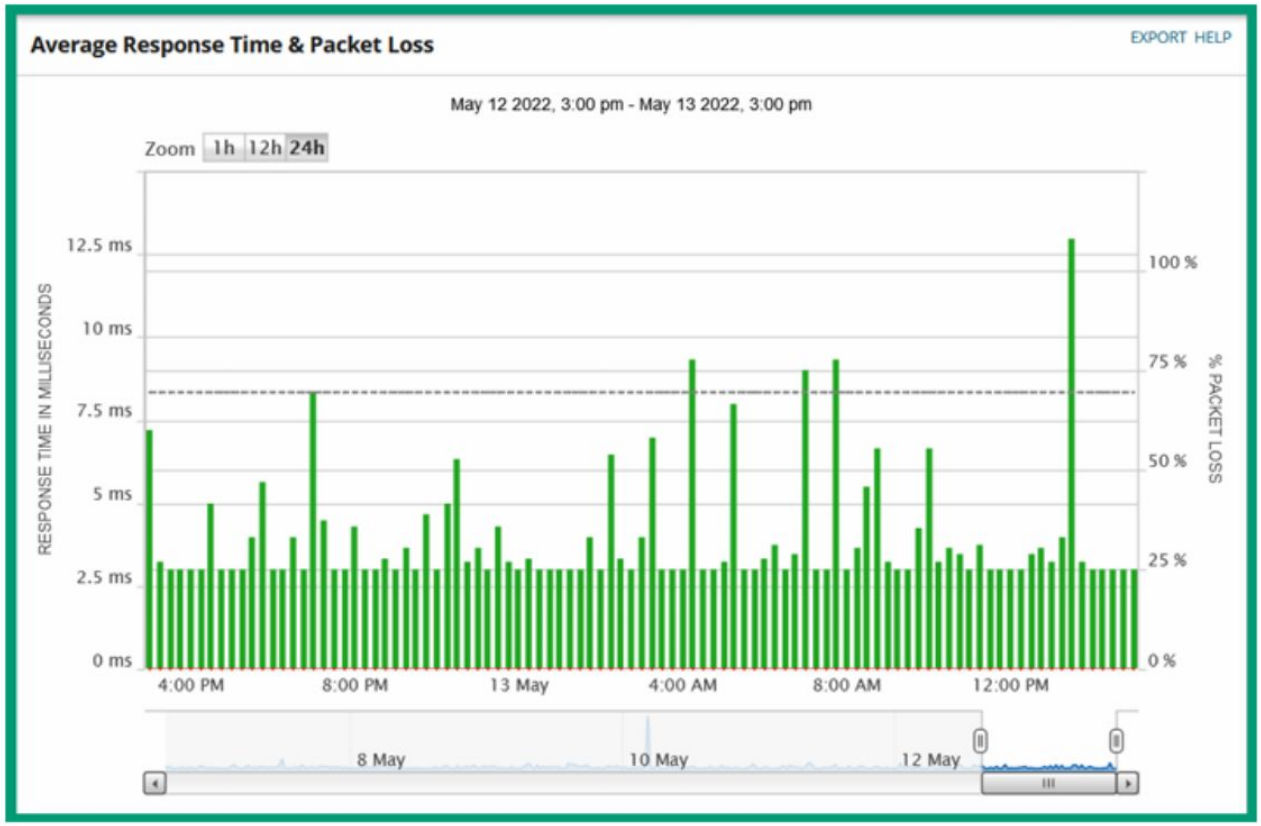


Figure 11.2 – Observing the response time and packet loss

- The network **bandwidth** is simply the total amount of packets that can be transferred from a source device to a destination device within a given time.
- Observing the bandwidth utilization and the **types of traffic** on a network helps discover any problems such as congestion, latency, physical issues, and security threat.
- Various techniques are commonly used **to collect and analyze network traffic**, such as the following:

- **Simple Network Management Protocol (SNMP)**
- **NetFlow**
- **IP Flow Information Export (IPFIX)**

Simple Network Management Protocol (SNMP)

- SNMP is a common network protocol
- It allows network professionals to easily monitor devices
- The SNMP Manager allows to easily collect statistical data from devices on the network, retrieve device statuses, and push configuration changes to network devices

- There are different versions of SNMP, as follows:
- **SNMPv1**: Does not support any security such as data encryption or authentication, hence it's not recommended for use.
- **SNMPv2**: This version of SNMP is an improvement on how SNMP handles communication between the SNMP Manager and SNMP Agent, but this version does not support data encryption or authentication. Hence, it's not recommended for use.
- **SNMPv3**: This version of SNMP is an improvement on prior versions and supports data encryption, integrity checking, and authentication.

Network Management System (NMS)

- When working with **SNMP**, three main components need to work together to create a **Network Management System (NMS):**

1. SNMP Manager
2. SNMP Agent
3. Management Information Based (MIB)

- The **Manager** is an application that's installed on the network professional's computer or centrally on a server.
- Manager must collect information and make configurations on devices that are running the **agent**.
- The SNMP agent is configured on a networking device such as a switch or router. The SNMP agent is the actual component on the networking device that communicates with the SNMP manager application and vice versa.
- The **MIB** is a database that contains the information needed by the agent to find and retrieve data from a device.
- The SNMP agent uses MIB to locate the requested information within the networking device and responds to the agent with the collected data.

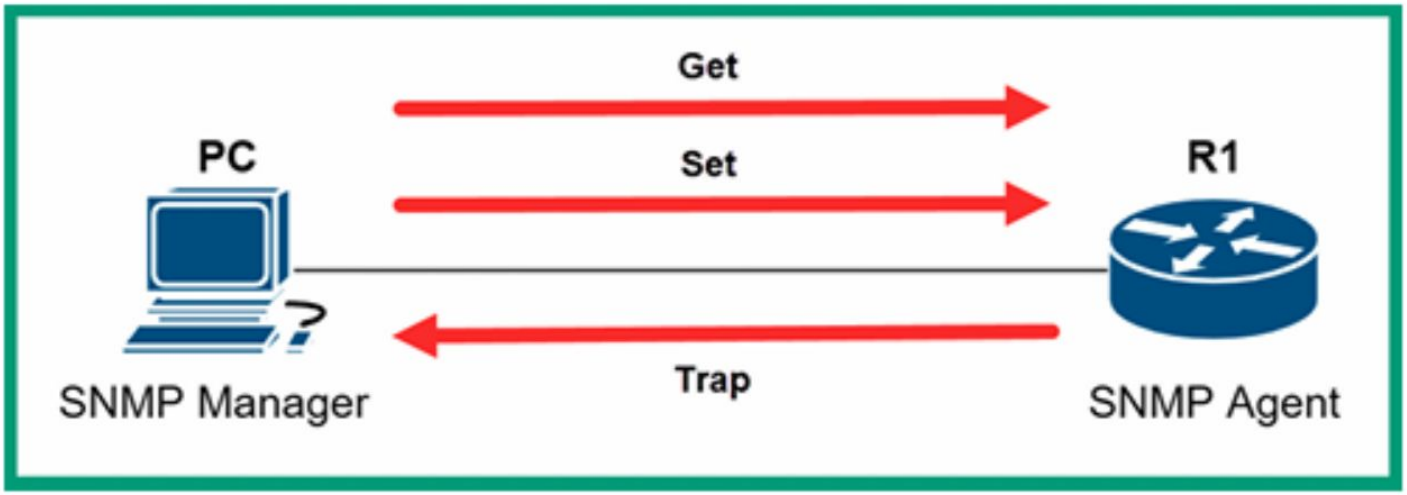


Figure 11.4 – SNMP messages

- The manager can retrieve information from agents on the network by sending an **SNMP GET** message, which instructs the agent to respond with the requested information.
- Additionally, the manager sends **SNMP SET** messages to an agent when configuration changes are needed.
- The **Trap** data units are sent from the Agent to the Manager as they contain data about changes or events that occurred on the device and only send information when a threshold has been met.
- Using traps greatly decreases network management bandwidth.

Network device logs

- Networking devices, security appliances, servers, and end devices commonly generate logs, which are records of every event that has occurred on the device.
- Network professionals depend on the logs created by a device to determine the reason for an event, as it ensures proper accountability of events and actions on a network.

- **Log messages** contain timestamps, severity levels, and descriptions of the events displayed.

Figure 11.5 – Device logs

- **Traffic logs** contain information and details about the traffic that flows between devices on a network.
- The graph shows the traffic patterns of a network switch over 24 hours, allowing a network professional to determine which time of day the network segment is mostly utilized and the average bandwidth that's being used on a daily, monthly, or annual basis.

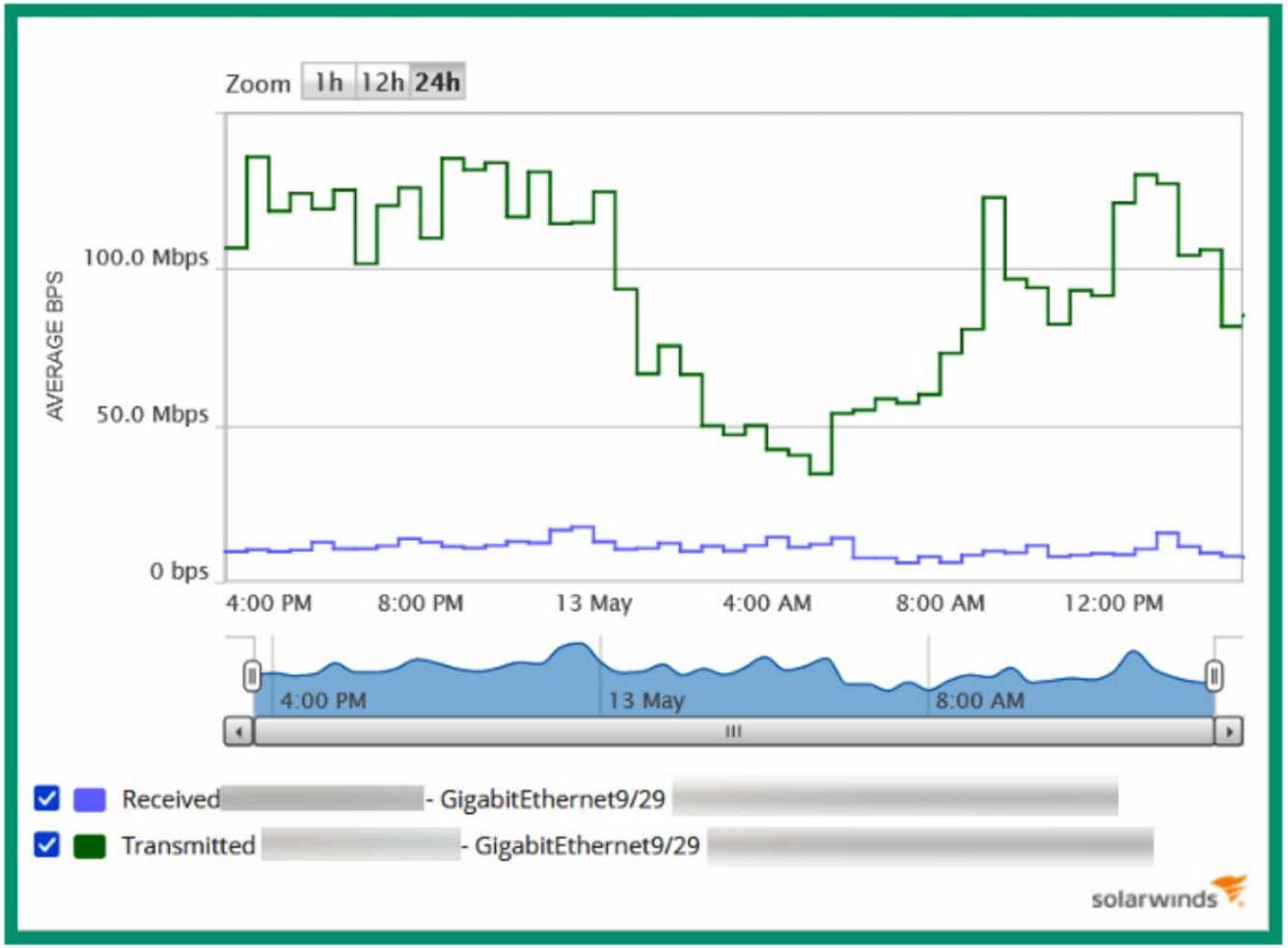


Figure 11.6 – Traffic log graph

- **Audit logs** are common for determining specific information about who, what, and when an event occurred.

- The audit logs are created on the device for every successful and unsuccessful logon attempt and special access event.

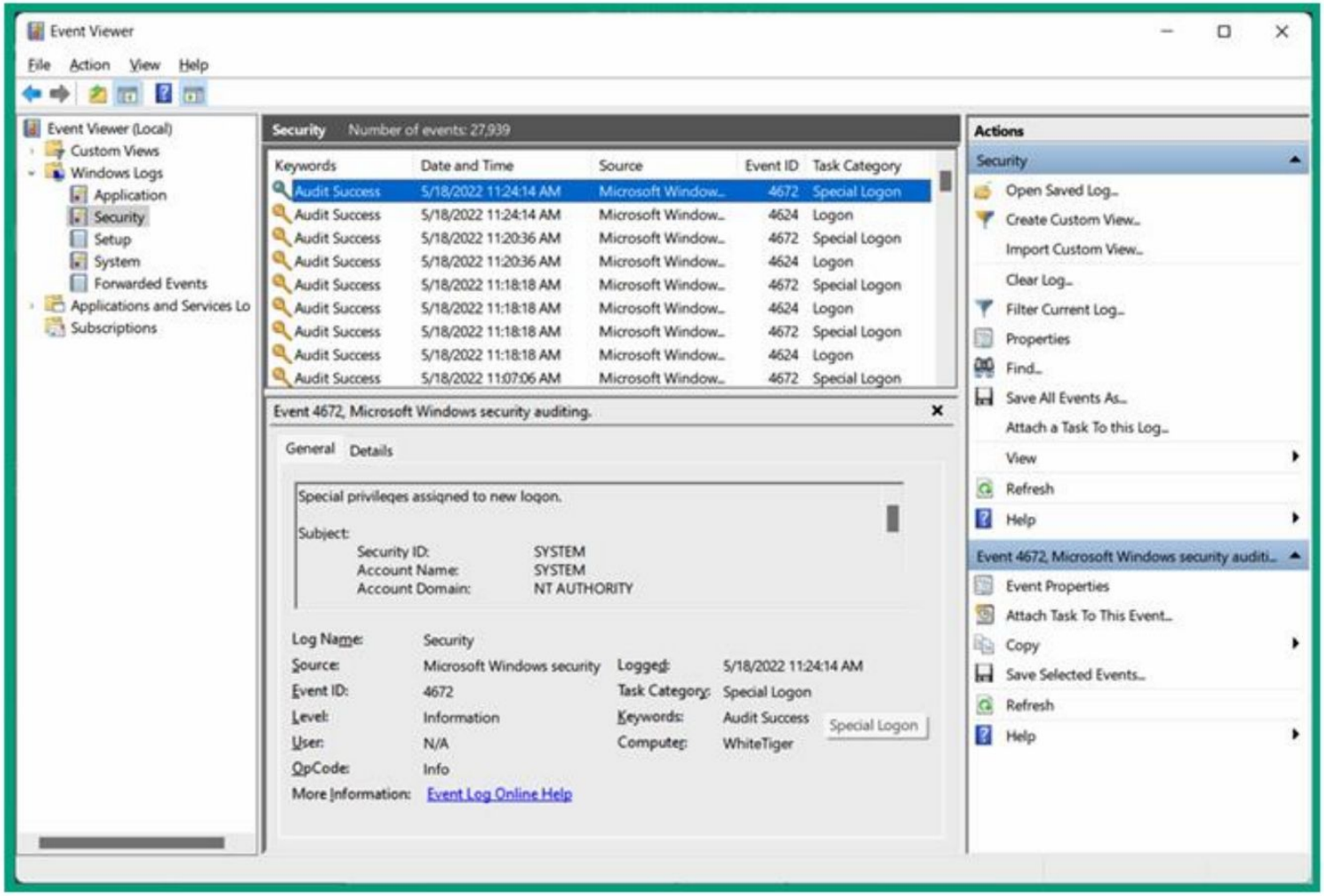


Figure 11.7 – Audit logs

Syslog

- Since each networking device generates a log message, this means a network professional will need to **manually** log into a device to view the logs for that device only.
- This process can be very time-consuming and inefficient.
- Many networking devices, servers, and end devices support a **common network protocol** that allows them to forward their log messages over a network to a centralized logging server. This protocol is known as **syslog**.
- The syslog protocol allows devices to generate logs for events that occur on a device.

Default Format Of A Syslog Message

```
seq no: timestamp: %facility-severity-MNEMONIC: description
```

The following is a breakdown of each component of a Syslog message:

- **seq no:** Represents the sequence number that is assigned to the log message.
- **timestamp:** Includes the date and time the message was generated by the device. The date and timestamp are taken from the system clock on the host device.
- **facility:** Represents what the log message is referencing regarding the event that has occurred, such as the source of the problem or protocol.
- **severity:** Includes a severity code that helps network professionals determine the importance of the event.
- **MNEMONIC:** Inserts text that is uniquely used to describe the event.
- **description:** Contains a brief description of the event.

Example of a Syslog message generated by a Cisco device:

```
*Apr 28, 15:53:58.5353: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
```

- The Syslog protocol uses UDP service port number 514 by default over a network.
- Syslog is used to gather logging information that helps network professionals with monitoring and troubleshooting issues within an organization.
- Syslog allows network professionals to configure devices so that they can send their log messages to a specific logging destination, such as a centralized logging server.

Severity Name	Severity Level	Description
Emergency	0	System is unusable
Alert	1	Immediate action is needed
Critical	2	Critical condition
Error	3	Error condition
Warning	4	Warning condition
Notification	5	Normal but significant condition
Informational	6	Informational message
Debugging	7	Debugging message

Figure 11.8 – Syslog severity levels

collection of Syslog messages on a centralized logging server

	TIME OF MESSAGE	HOSTNAME	SEVERITY	MESSAGE
☐	5/13/2022 3:24:50 PM	10.160.31.8	Error	135699: [redacted] Gi0/6: Rx power high alarm; Operating value: -0.8 dBm, Threshold value: -3.0 dBm.
☐	5/13/2022 3:24:49 PM	10.10.2.12	Critical	8773971: * Security violation on port GigabitEthernet9/30 due to MAC address [redacted] on VLAN 569
☐	5/13/2022 3:24:49 PM	10.10.2.12	Critical	8773970: * Security violation occurred, caused by MAC address [redacted] on port GigabitEthernet9/30.
☐	5/13/2022 3:24:44 PM	10.10.2.12	Critical	8773968: * Security violation occurred, caused by MAC address [redacted] on port GigabitEthernet9/30.
☐	5/13/2022 3:24:44 PM	10.10.2.12	Critical	8773969: * Security violation on port GigabitEthernet9/30 due to MAC address [redacted] on VLAN 569
☐	5/13/2022 3:24:41 PM	10.160.20.243	Error	[redacted] Junos: rpd[1832]: bgp_recv: peer [redacted] (External AS [redacted] received unexpected EOF
☐	5/13/2022 3:24:38 PM	10.10.2.12	Critical	8773967: * Security violation on port GigabitEthernet9/30 due to MAC address [redacted] on VLAN 569
☐	5/13/2022 3:24:38 PM	10.10.2.12	Critical	8773966: * Security violation occurred, caused by MAC address [redacted] on port GigabitEthernet9/30.

Figure 11.9 – Log messages

- The centralized logging server collects all the log messages from various devices on the network and performs both de-duplication and correlation, helping network professionals easily determine the sequence of events that occurred on the network.

CHAPTER 12

Organizational Documents and Policies

Plans and procedures

- Plans and procedures are created to ensure each employee follows a standard set of rules or guidelines that are used to achieve a common goal or meet an objective.

- Common plans and procedures are:

1. change management,
2. incident response,
3. disaster recovery,
4. business continuity,
5. need for standard operating procedures

Change management

- It focuses on ensuring that a change is beneficial to the organization and that it's applied as efficiently and effectively as possible.
- Also ensuring users are affected as little as possible during and after the change being made.
- Before a technical or non-technical change is implemented within an organization, the change has to go through an entire life cycle to ensure all the procedures are thoroughly followed by the people who are implementing the change – such that, the change has to be approved by the *Change Management Board*.
- During a change, things may not always go quite as planned. Having a rollback or remediation plan helps IT professionals to reverse the change in the case of some unforeseen problem with the change.
- Change management helps reduce the downtime of the network and resources while reducing the risks within an organization.

Change management (contd.)

The following are the typical phases of change management:

1. **Request** – Requesting to implement a change in the organization
2. **Evaluate** – Determining whether the change is needed to improve the business process
3. **Authorize** – Gaining authorization from the change advisory board before making the change
4. **Implement** – Performing the change within the organization (on the part of the change owner, the person who is performing the change)
5. **Documentation** – Documenting everything about the change for future reference

Incident response plans

- Incident response plan, is a set of procedures and tools that are commonly used by the cybersecurity team to efficiently identify, contain, and recover from cyber-attacks and threats.
- It is designed to help organizations quickly adapt to the ever-changing security landscape of new emerging threats and quickly respond using a uniform, systematic approach to any threat of a cyber-attack.
- The incident response team are the cybersecurity professionals who help an organization prevent and recover from a real-world cyber-attack.
- Keeping proper documentation can help a professional to determine whether a similar incident has occurred in the past and if so, what actions were taken.

Incident response plans (contd.)

- **Cyber-Incident Response Team** (CIRT), which is responsible for monitoring and resolving all security incidents within the organization.
- The CIRT is made up of professionals who are trained and qualified in various security incident response techniques.
- CIRT is focused on incident response, analysis, and reporting.
- According to the NIST SP 800-61 Rev. 2 documentation in the Computer Security Incident Handling Guide, the following are the phases of incident handling:

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery
4. Post-incident activity and analysis

Incident Response Phases

The following diagram shows the NIST incident response and handling model:

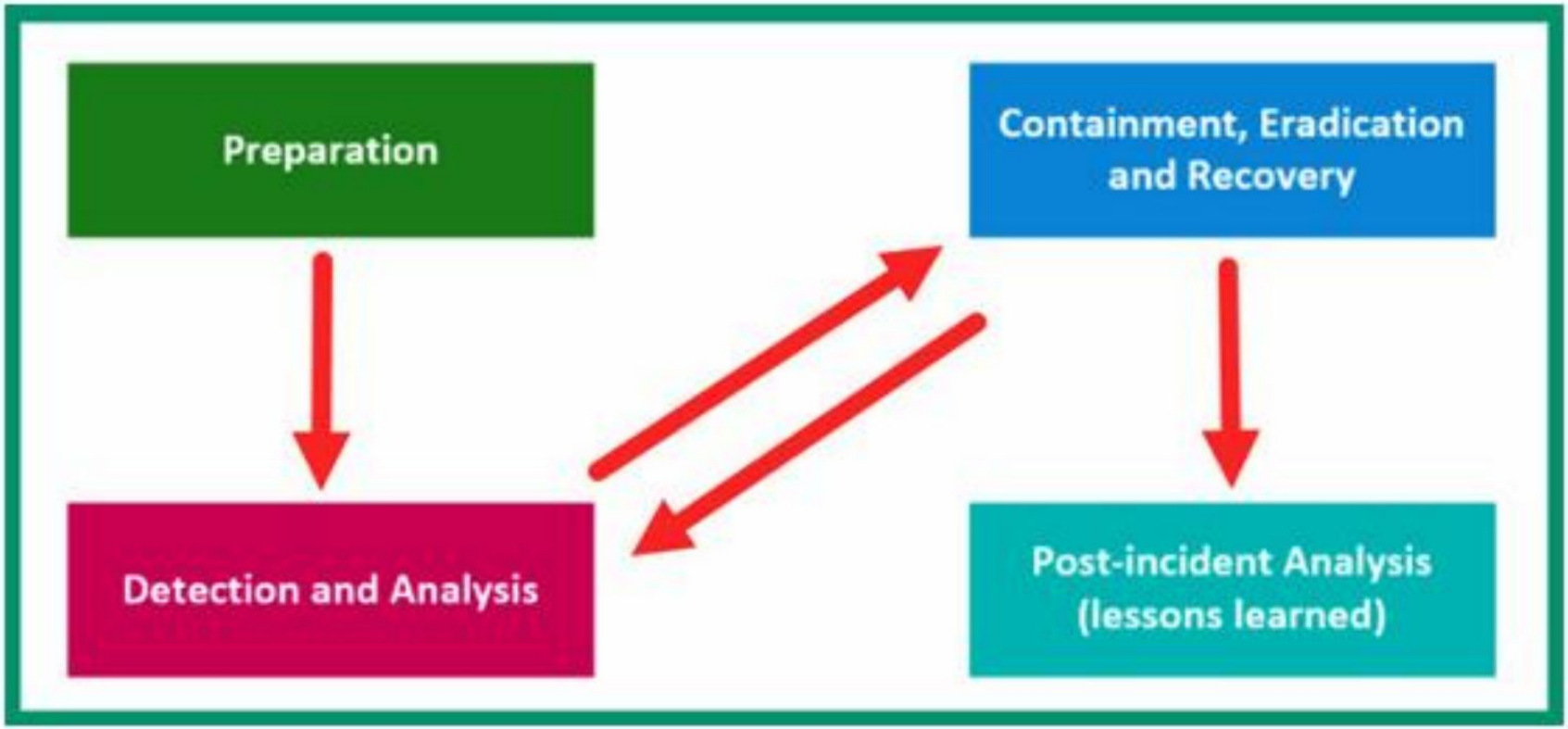


Figure 12.1 – The incident handling process

Preparation

- The preparation phase focuses on gathering a list of all the assets within the organization.
- An **asset** is simply anything that has value to the company; assets can be tangible, intangible, or people.
- **Tangible assets** are any physical objects that are valuable such as networking devices and servers.
- **Intangible assets** are digital objects that do not have a physical form such as data, license keys for applications, organization policies and procedures, business processes, and intellectual property.

Preparation (contd.)

- During the preparation phase, network and security professionals must create a **baseline** of their network and system's performance when everything is working under normal conditions.
- Baselines help to determine what is considered to be a normal traffic flow between the assets within the network.
- Develop a **communication plan** that outlines who should be contacted if a security incident should occur within the organization and a plan of action for each possible security incident that can occur.

Detection and analysis

- An **event** is simply any action or transaction that occurs on a system or network, such as a user logging into a system, or a client device establishing a connection to a server.
- An **incident** is a security event that indicates a system or network has been compromised due to a cyber-attack or a threat.
- Hence, distinguishing between events versus incidents within their network is vital.
- During the detection and analysis phase, the incident response team must be well-trained to identify a security event efficiently and quickly.

Detection and analysis (contd.)

- It is important to collect as much information as possible on the security event or incident to improve the analysis phase, such as determining whether a threat exists in the system or not.
- If a threat exists, try to determine how the threat has entered the system and network of the organization.
- Using security appliances to actively monitor systems and networks improves threat identification as they occur in real time.

Containment, eradication, and recovery

- The goal of the **containment** phase is to simply stop a threat such as malware spreading to other systems on the network or a hacker from compromising additional machines.
- The **eradication** phase ensures systems are thoroughly disinfected to ensure there are no longer any infections present on any system within the organization.
- The **recovery** process focuses on restoring systems to an acceptable working state in terms of their operating systems, applications, and data, which also includes performing data recovery from backups, replacing compromised systems, and re-installing the host operating systems and applications.

Post-incident analysis

- After an incident is resolved, it’s important to use the opportunity to learn from the experience of the cyber-attack or threat.
- The lessons learned will help improve the incident response plan and its effectiveness, and the efficiency and preparedness of the incident response team for future security events and incidents.

The business continuity plan

- The **Business Continuity Plan (BCP)** is a set of guidelines that is used to help restore the organization's services and business functions whenever a disaster has occurred.
- A **Business Impact Analysis (BIA)** is used to help professionals to identify the most critical business processes, procedures, and resources that are needed to ensure the organization can continue to operate and function.
- The BIA contains a systematic method that also helps professionals to determine the potential effects of disruption on critical business processes and operations within a company.
- It's essential to determine the availability that is needed by those business processes and resources that may be affected.

The business continuity plan (contd.)

When developing a business continuity plan, it's important to consider the following factors:

1. **Exercises (tabletop):** Tabletop exercise includes performing regular exercises to ensure everyone is prepared, it allows an organization to reduce costs and time by simply discussing a simulated disaster. In a tabletop exercise, people do not physically participate but rather discuss what happens at the reached stage of the plan.
2. **After-action reports:** This report may contain the details of each step of the methodology and any explanations of the procedures.
3. **Failover:** If a disaster occurs, you already have an alternative site and plans in place for migrating your systems. Ensure all data is fully replicated or synchronized between the organization and the failover site.
4. **Alternative business practices:** During a disaster, it's important to alternate between different methods of achieving the same task. It's important to ensure proper documentation is kept for all the primary and alternative business processes before a disaster occurs.

Disaster recovery plans

- Disaster recovery planning focuses on ensuring an organization is well prepared and equipped to recover from any possible disaster that may be a risk to the company, its resources, and assets.
- When developing a disaster recovery plan, the organization should perform continuous training and testing of the plan to ensure everyone understands their roles and responsibilities during an actual disaster.

Disaster recovery plans (contd.)

The following are key terms in disaster recovery planning:

1. **Recovery Time Objective (RTO)** – The RTO is simply the maximum amount of time that a system or resource can be unavailable before there is an unacceptable impact on other systems' resources, business processes, and critical functions of an organization
2. **Recovery Point Objective (RPO)** – The RPO is simply the point in time before the disruption or outage of a system to which the business processes or data can be recovered or restored after the outage has occurred

Disaster recovery plans (contd.)

- When creating a disaster recovery plan, it's essential that you clearly identify both the internal and external teams that are responsible for assisting the organization in restoring services and critical business functions to an acceptable level, enabling the organization to resume its operations.
- Having proper documentation of key assets of the organization helps disaster recovery professionals to reduce the time to restore business operations.
- It's important to identify the recovery and failover sites and the redundancy hardware components that will be needed in the event of a disaster.
- The disaster recovery plan is designed to be proactive, allowing professionals to be prepared to handle and respond to various types of disasters that may affect the organization.

CHAPTER 13

High Availability and Disaster Recovery

High availability concepts

- High availability (HA) is simply the ability of a system or a network to continuously operate without failure.
- A common strategy for setting up HA within an organization is to implement fault tolerance in the form of redundancy in hardware components on devices and network infrastructure.

Terminology on high availability

- **Mean Time To Repair (MTTR):** This is the time required/needed to resolve an issue.

For instance, if an IT professional spends a total of 60 hours per year repairing a server during an unplanned maintenance window and the server was repaired 8 times during that same year, then MTTR = Total repair time/number of repair = 60/8 = 7.5 hours.

- **Mean Time Between Failure (MTBF):** This is the predicted time between the outages of a system.

For instance, if a critical server operates for 8,745 hours per year and experienced 10 failures within the same year, then MTBF = Total uptime/number of failures = 8745/10 = 874.5 hours.

- **Recovery Time Objective (RTO):** This is the goal of getting the system up and running back to a specific service level after an outage has occurred.
- **Recovery Point Objective (RPO):** This is determined by how data loss is considered to be acceptable or how far back the data goes to bring the system back online.

Diverse paths

The following diagram shows an organization with a single connectivity path to the data center facility:

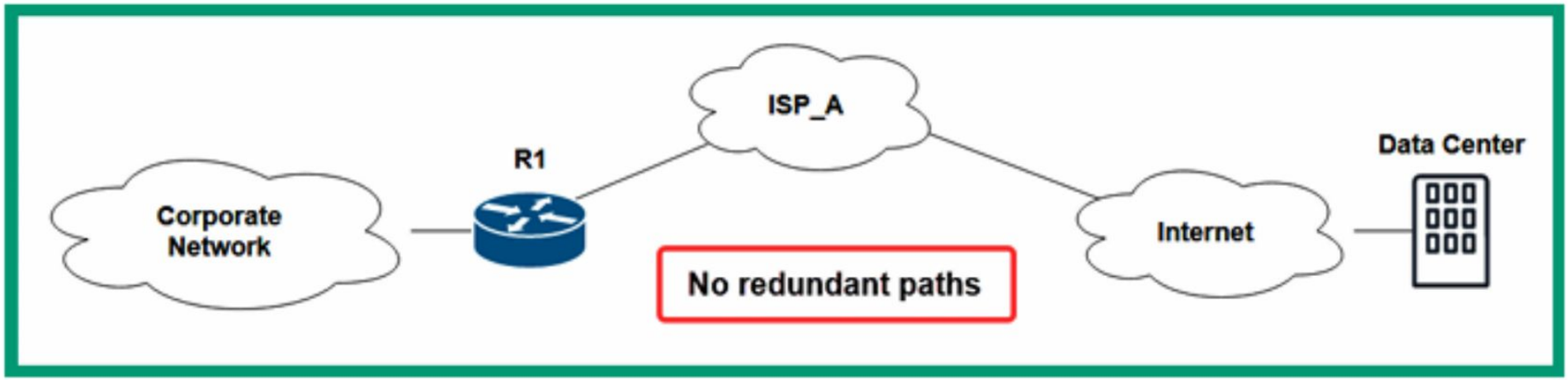


Figure 13.1 – No redundancy

- if the router between the organization's corporate network and the internet goes down, users and client devices will not be able to access the resources on the internet.
- Having multiple/diverse paths between your organization and the data center is an important factor to consider when implementing HA concepts.

Diverse paths (contd.)

The following diagram shows redundant ISPs providing connectivity:

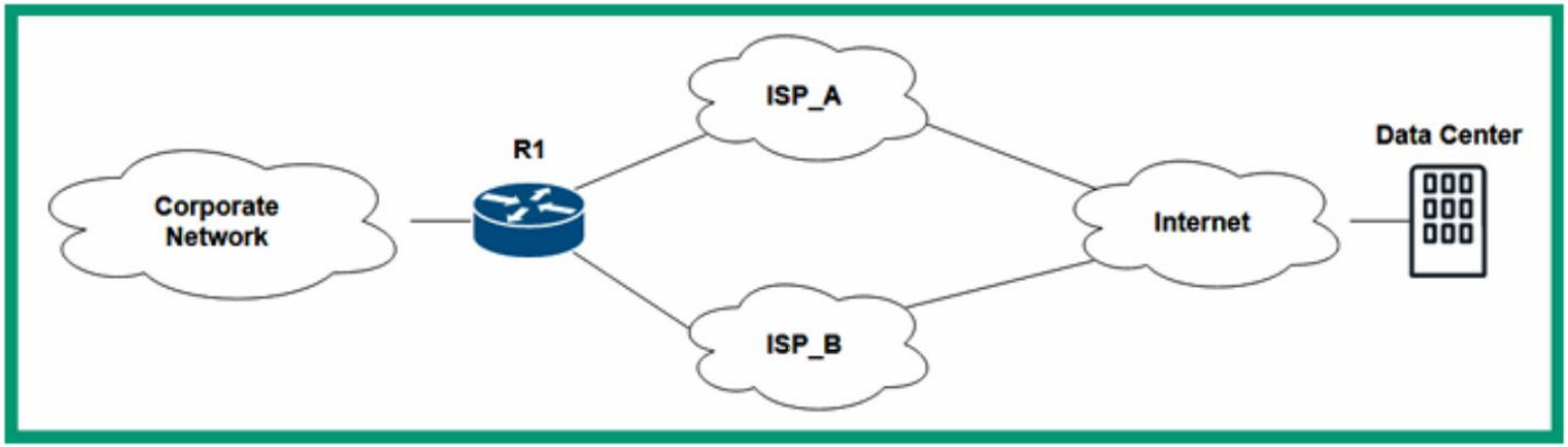


Figure 13.2 – Redundant ISP connections

- Multiple/diverse paths focus on ensuring an organization has more than one available path to and from a data center or the internet.
- Since data centers are hosting resources, servers, and devices for many customers, the data center also needs redundancy internet connections from various ISPs within the region.
- Using multiple ISPs for a data center provides greater redundancy, ensuring access to the data center resources is always available when needed.

Infrastructure redundancy

- **Fault tolerance** refers to the ability of a system to continue to operate normally, despite the failure of one or more of its constituent parts.
- One commonly implemented configuration for fault-tolerant system is load balancing.
- **Load balancing** is a configuration technique that aims to disseminate workloads among all of the available resources.
- Incoming traffic from clients is initially directed at the load balancer, which then utilizes its preconfigured balancing algorithm to determine which of its backend servers will receive the traffic.
- Common load balancing/scheduling algorithms include
  - *round-robin* (a simple algorithm where requests are sequentially distributed to servers as they arrive),
  - *weighted round-robin* (as with round-robin, but servers are assigned different weightings, and the ones with higher weightings receive larger shares of incoming requests), and
  - *least connection* (servers with smaller numbers of client connections are preferred over saturated servers).

Load Balancer

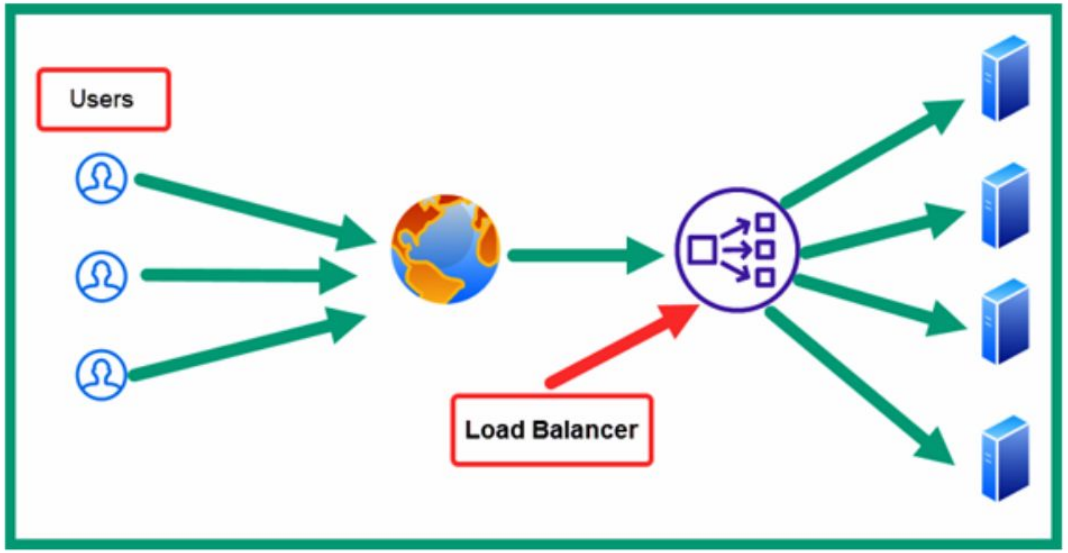


Figure 13.3 – Load balancer

- **Clustering** refers to the aggregation of several nodes into a group, such that the group of nodes behaves as though it were a single node. For example, a server cluster, is where each server delivers content to clients in the same manner as a single server would.
- Clustering adds a degree of fault tolerance to a system, so long as the cluster is configured correctly.
- Another technique commonly used to provide fault tolerance is network interface card (NIC) **teaming**.
- NIC teaming refers to a technique in which several NICs on a server are combined into a group to provide higher capacity or improved fault tolerance to the server.
- When configured to provide increased fault tolerance, NIC teaming balances traffic across all of the NICs and links in the group, allowing traffic to continue flowing if any of the individual NICs in the group fails.
- This concept of combining several links into one highly available link can also be implemented on network equipment (such as switches) through the concept of port aggregation.
- **Port aggregation** allows several physical ports on devices to be combined into one logical port on the device.
- This process can be performed through particular protocols on devices such as the link aggregation control protocol (LACP).

Active-active versus active-passive configurations

- The concept of **active-passive** configurations allows network professionals to install and configure two devices of the same type and function on the network, allowing only one device to operate at a time.
- If one of the two devices fails on the network, the secondary device can take over and become the new primary device.
- Within the active-passive configuration, there's always constant communication between both devices as they are configured as a pair.
- The configurations and real-time session information between devices in an active-passive state need to be constantly synchronized with each other as failover may happen at any time within an organization.
- In an **active-active** state, two devices of the same type are configured and operating at the same time.
- This type of configuration is usually more complex to design and operate compared to the active passive configuration.
- Since both devices are active and forwarding traffic at the same time, the packet can flow in many different directions.

active-passive mode

- Two routers have been configured to operate in an **active-passive mode**,
- where R1 is configured to operate as the **primary** router for forwarding packets between the internet and the internal network and
- R2 becomes the **standby** router.
- While these two routers are online, they both exchange keep-alive messages with each other.
- *If R2 does not receive the keep-alive messages from R1 after a specific time, R2 will automatically assume the role of the primary router for forwarding packets to and from the internet for the internal clients.*

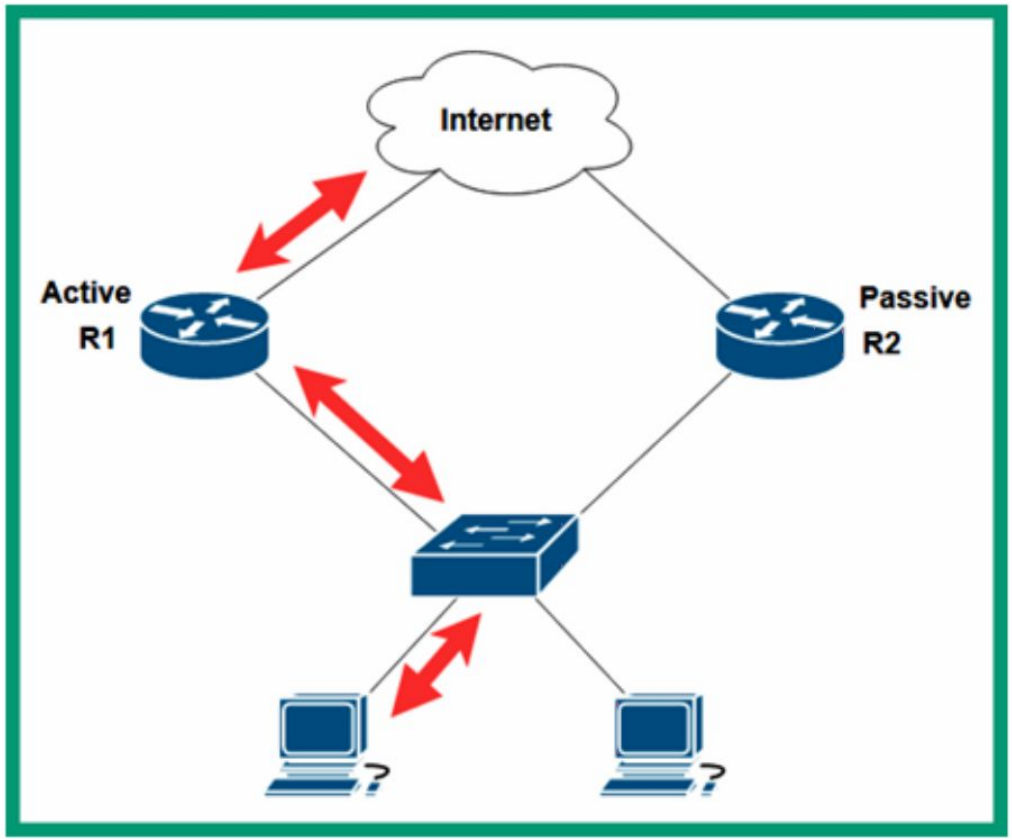


Figure 13.4 – Active-passive routers

active-active mode

- R1 and R2 are both operating in an **active-active state.**
- Therefore, traffic from one computer may take the outbound path through R1 to access the internet, and returning traffic may not take the same path but use the path through R2 and back to the computer.

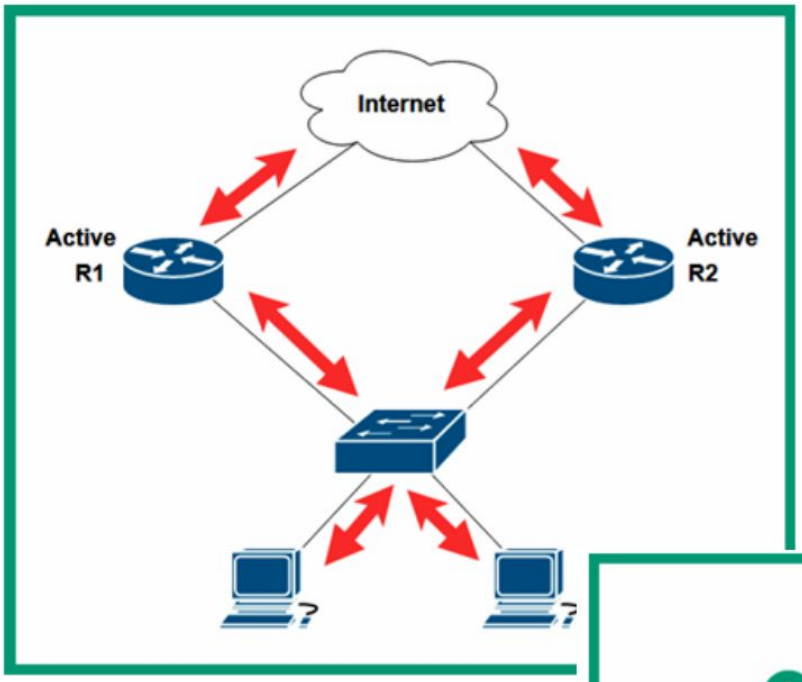


Figure 13.5 – Active-active router

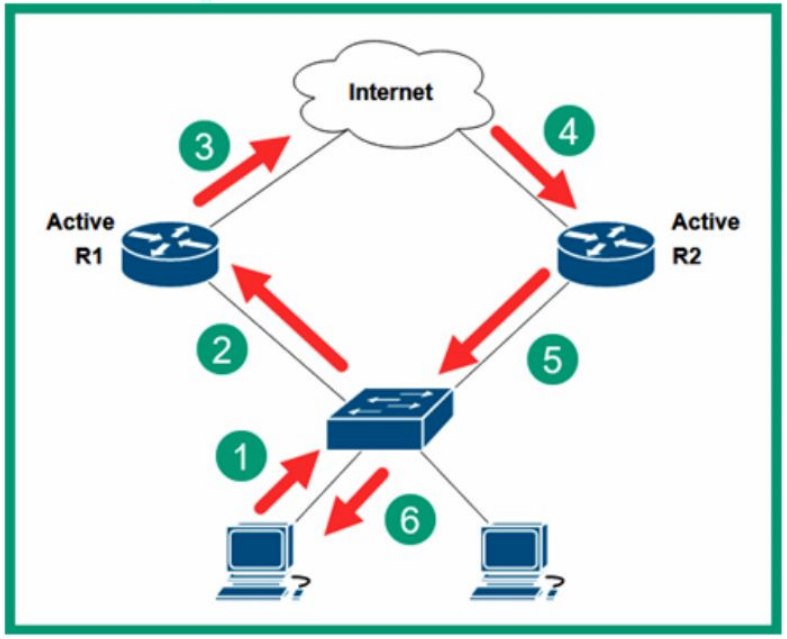


Figure 13.6 – Different paths