Elk Technologies
https://elktech.org
Scott Stephenson

Module 5: Network Fundamentals

DevNet Associate v1.0

Cisco | Networking Academy®
Mind Wide Open™

Module Objectives

- Module Title: Network Fundamentals
- Module Objective: Apply the processes and devices that support network connectivity.
- It will comprise of the following sections:

Topic Title	Topic Objective
5.1 Introduction to Network Fundamentals	Explain basic network terms and processes.
5.2 Network Interface Layer	Explain the features and functions of the OSI network layer.
5.3 Internetwork Layer	Explain the features and functions of the OSI internetwork layer.
5.4 Network Devices	Explain the features and functions of common network devices.
5.5 Networking Protocols	Explain common networking protocols.
5.6 Troubleshooting Application Connectivity Issues	Troubleshoot basic network connectivity.

5.1 Introduction to Network Fundamentals

Overview

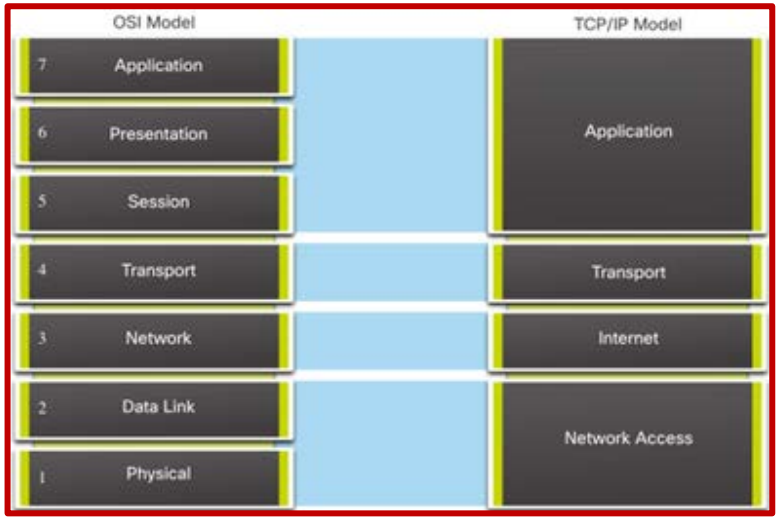
- Knowing how to troubleshoot network connectivity is crucial to both developers and administrators, so quicker resolutions to problems is critical for everyone.
- A high-level understanding of the layers, that the network traffic goes through, provides a basic knowledge needed to work on networks, applications, and automation.

What Is a Network?

- A network consists of end devices such as computers, mobile devices and printers that are connected by networking devices such as switches and routers.
- The network enables the devices to communicate with one another and share data.
- The most common LAN methods to connect to a network are wired Ethernet LANs (IEEE 802.3) or wireless LANs (IEEE 802.11). The end-devices connect to the network using an Ethernet or wireless network interface card (NIC).
- **Protocol Suite**
  - A protocol suite is a set of protocols that work together to provide comprehensive network communication services such as:
  - Internet Protocol Suite or TCP/IP
  - Open Systems Interconnection (OSI) protocols
  - AppleTalk (now replaced by TCP/IP)
  - Novell NetWare (now replaced by TCP/IP)

What Is a Network?

- Both, OSI model and the TCP/IP model use layers to describe the functions and services that can occur at that layer.
- Both models can be used with the following differences:
  - OSI model numbers each layer (bottom to top).
  - TCP/IP model uses a single application layer to refer to the OSI application, presentation, and session layers.
  - TCP/IP model uses a single network access layer to refer to the OSI data link and physical layers.
  - TCP/IP model refers to the OSI network layer as the Internet or Internetwork layer.
  - The OSI transport and network layers have the fame functionality in the TCP/IP model.

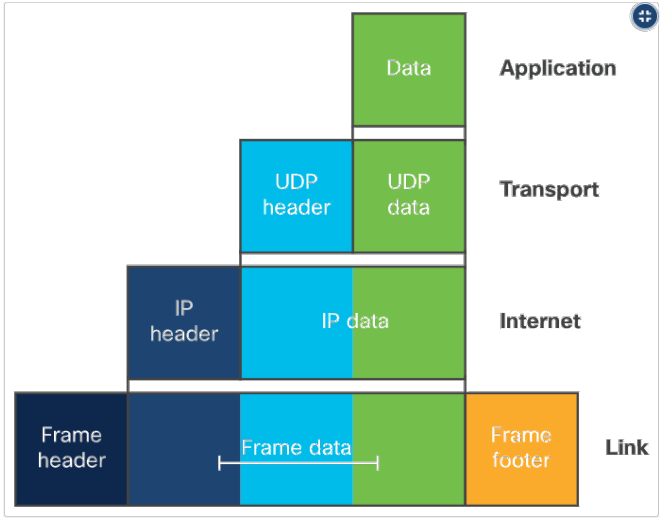


What Is a Network?

- **OSI Layer Data Communication**
  - The form that a piece of data takes at any layer is called a **Protocol Data Unit (PDU)**.
  - During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used.
  - When messages are sent on a network, the encapsulation process works from top to bottom.

What Is a Network?

- **Data Encapsulation at Each Layer of the TCP/IP model**
  - At each stage of the process, a PDU has a different name to reflect its new functions. The PDUs are named according to the following layers:
    - **Data** - The general term for the PDU used at the application layer
    - **Segment** - Transport layer PDU
    - **Packet** - Network layer PDU
    - **Frame** - Data Link layer PDU
    - **Bits** - Physical layer PDU used when physically transmitting data over the medium
  - Note: An OSI model layer is often referred to by its number.



TCP vs UDP

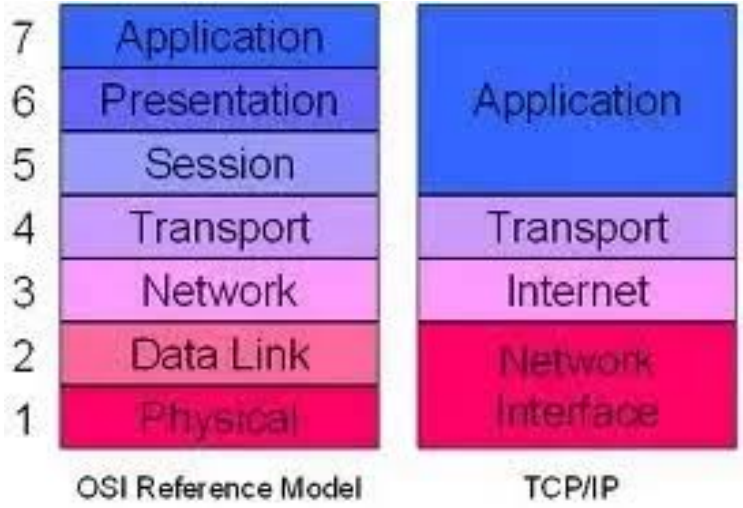
- The transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices. This layer has two protocols: **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**.
- TCP provides reliability and flow control using these basic operations:
  - **Number** and **track data segments** transmitted to a specific host from a specific application.
  - **Acknowledge** received data.
  - **Reliability** – guaranteed delivery of the data.
  - **Retransmit** any unacknowledged data after a certain amount of time.
  - **Sequence** data that might arrive in wrong order.
  - **Send** data at an efficient rate that is acceptable by the receiver.
- TCP is used with applications such as databases, web browsers, and email clients.
- TCP requires that all data that is sent arrives at the destination in its original condition. Any missing data could corrupt a communication, making it either incomplete or unreadable.

TCP vs UDP

- Why use UDP?
  - UDP is a simpler transport layer protocol than TCP.
  - It does not provide reliability and flow control, which means it requires fewer header fields.
  - UDP datagrams can be processed faster than TCP segments.
  - UDP is preferable for applications such as Voice over IP (VoIP).
  - Acknowledgments and retransmission would slow down delivery and make the voice conversation unacceptable.
  - UDP is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly. Domain Name Service (DNS) uses UDP for this type of transaction.
- Application developers must choose which transport protocol type is appropriate based on the requirements of the applications.

What Is a Network?

- An application uses a set of protocols to send the data from one host to the other. Going down the layers, from the top one to the bottom one in the sending host and then the reverse path from the bottom layer all the way to the top layer on the receiving host, at each layer the data is being encapsulated.
- At each layer, protocols perform the functionality required by that specific layer.



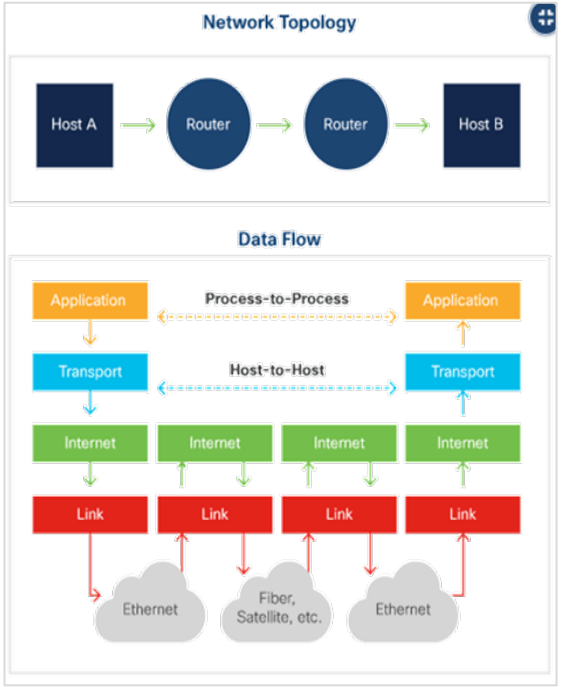
What Is a Network?

- Functionality of each layer of the OSI model:

Layer	Functionality
Physical Layer (Layer 1)	Responsible for the transmission and reception of raw bit streams.
Data Link Layer (Layer 2)	Provides NIC-to-NIC communications on the same network.
Network Layer (Layer 3)	Provides addressing and routing services to allow end devices to exchange data across networks.
Transport Layer (Layer 4)	Defines services to segment, transfer, and reassemble the data for individual communications between the end devices.
Session Layer (Layer 5)	Allows hosts to establish sessions between them.
Presentation Layer (Layer 6)	Specifies context between application-layer entities.
Application Layer (Layer 7)	This is the OSI layer that is closest to the end user and contains a variety of protocols needed by users.

What Is a Network?

- **Data Flow in Layered Models**
  - End devices implement protocols for the entire stack of layers.
  - The network access layer (shown as Link in the figure) operates at the local network connection to which an end-device is connected.
  - The internet layer is responsible for sending data across potentially multiple distant networks.
  - IP operates at the internet layer in the TCP/IP reference model and performs the two basic functions, addressing and routing.



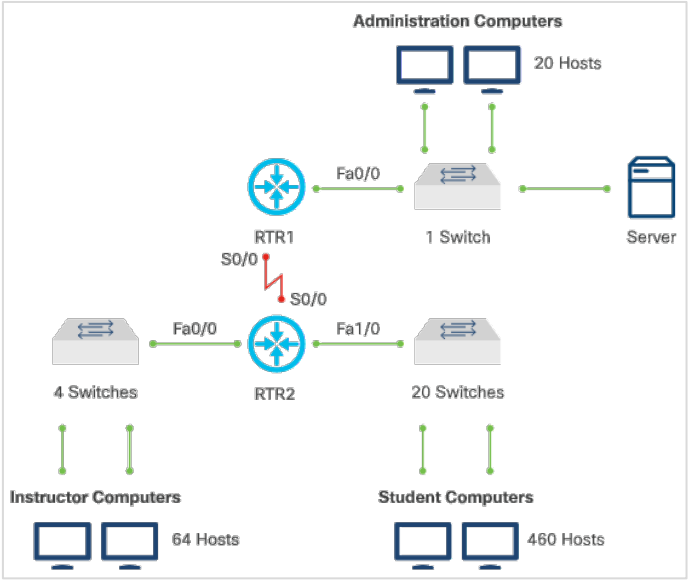
What Is a Network?

- **Planes of a Router**
  - The logic of a router is managed by three functional planes:
    - **Management Plane** – This manages traffic destined for the network device itself.
    - **Control Plane** – This processes the traffic that is required to maintain the functionality of the network infrastructure. It consists of applications and protocols and processes data in software.
    - **Data Plane** – This is the forwarding plane that is responsible for switching (forwarding) of packets in hardware, using information from the control plane.

5.2 Network Interface Layer

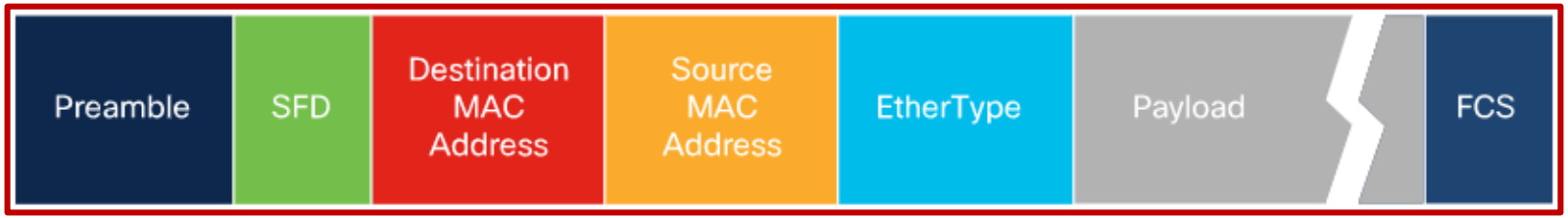
Understanding the Network Interface Layer

- **Network Topology**
  - The network enables the devices to communicate with one another and share data.
  - All host and network devices that are interconnected, within a close physical area, form a **local area network (LAN)**.
  - Network devices that connect LANs, over large distances, form a **wide area network (WAN)**.



Ethernet

- Ethernet is a set of guidelines published by the IEEE that specify cabling and signaling at the physical and data link layers of the OSI model.
- **Ethernet Frame**
  - The container in which data is placed for transmission is called a **frame**. Frame contains header information, trailer information, and the actual data that is being transmitted.
  - The most important fields of the Ethernet frame include:

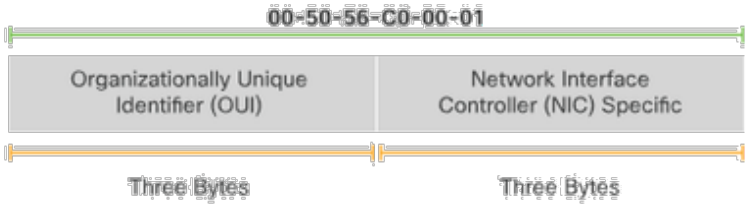


Ethernet

- MAC addresses are used in transporting a frame across a shared local media.
- If the data (encapsulated IP packet) is for a device on another network, the destination MAC address will be that of the local router (default gateway).
- The Ethernet header and trailer will be de-encapsulated by the router.
- The packet will be encapsulated in a new Ethernet header and trailer using the MAC address of the router's egress interface as the source MAC address.
- If the next hop is another router, then the destination MAC address will be that of the next hop router.
- If the router is on the same network as the destination of the packet, the destination MAC address will be that of the end device.
- When a host on an Ethernet network receives a frame with a destination MAC address that does not match its own MAC address, it will discard the frame.

MAC Addresses

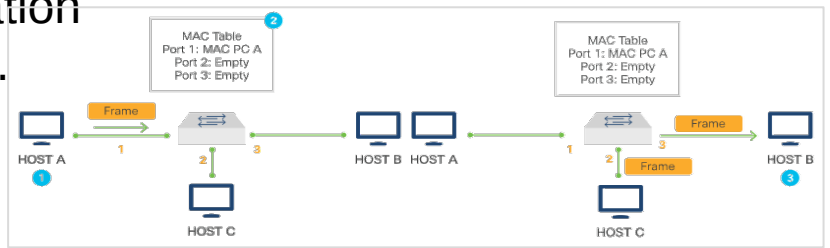
- All network devices on the same network must have a unique MAC address.
- The MAC address is the means by which data is directed to the proper destination device.
- A MAC address is composed of 12 hexadecimal numbers. There are two main components of a MAC:
  - **24-bit OUI** – The OUI identifies the manufacturer of the NIC.
  - **24-bit, vendor-assigned, end-station address** – This portion uniquely identifies the Ethernet hardware.



- Destination MAC addresses include the three major types of network communications:
  - **Unicast**
  - **Broadcast**
  - **Multicast**
- The **multicast MAC address** is a special value that begins with 01-00-5E in hexadecimal. It allows a source device to send a packet to a group of devices.

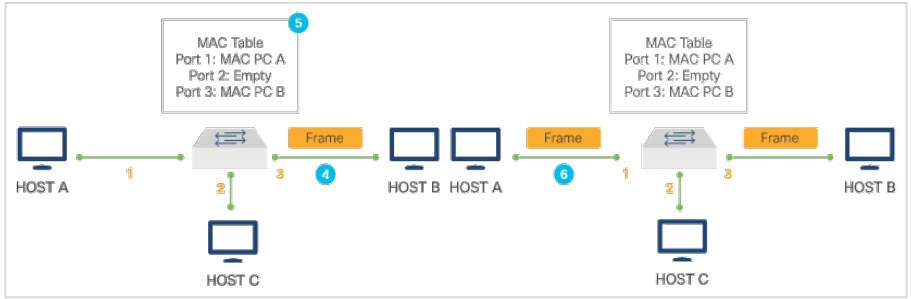
Switching

- The switch dynamically builds and maintains a table (called the MAC address table) that matches the destination MAC address with the port that is used to connect to a node.
- **Switching Process**
  - In the first topology, the switch receives a frame from Host A on port 1.
  - The switch enters the source MAC address and the switch port that received the frame into the MAC address table. The switch checks the table for the destination MAC address. As the destination address is not known, the switch floods the frame to all of the ports except the port on which it received the frame.
  - In the second topology, Host B, the destination MAC address, receives the Ethernet frame.



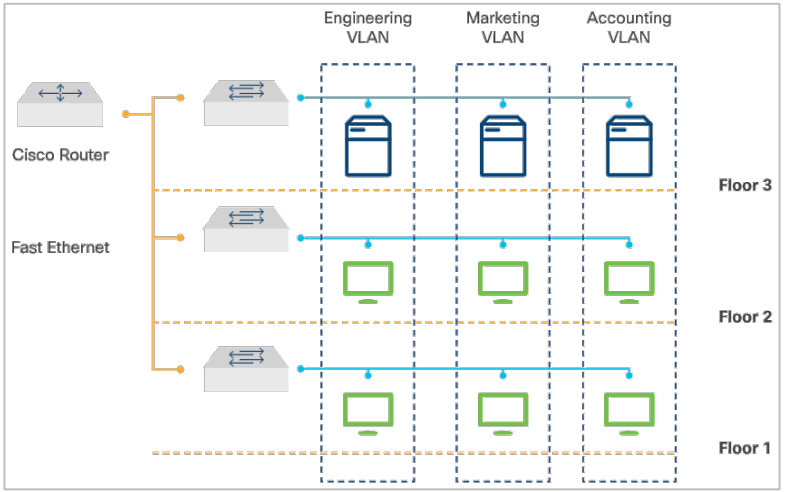
Switching

- In the third topology, Host B replies to Host A with the destination MAC address of Host A.
- The switch enters the source MAC address of Host B and the port number of the switch port that received the frame into the MAC table. The destination address of the frame and its associated port is known in the MAC address table.
- In the fourth topology, the switch can now directly forward this frame to Host A out port 1. Frames between the source and destination devices are sent without flooding because the switch has entries in the MAC address table that identify the associated ports.



Virtual LANs (VLANs)

- A **virtual LAN (VLAN)** is used to segment different Layer 2 broadcast domains on one or more switches.
- A VLAN groups devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.
- The figure shows three VLANs based on the function of its users: engineering, marketing, and accounting. It clearly shows that the devices do not need to be on the same floor.



Virtual LANs (VLANs)

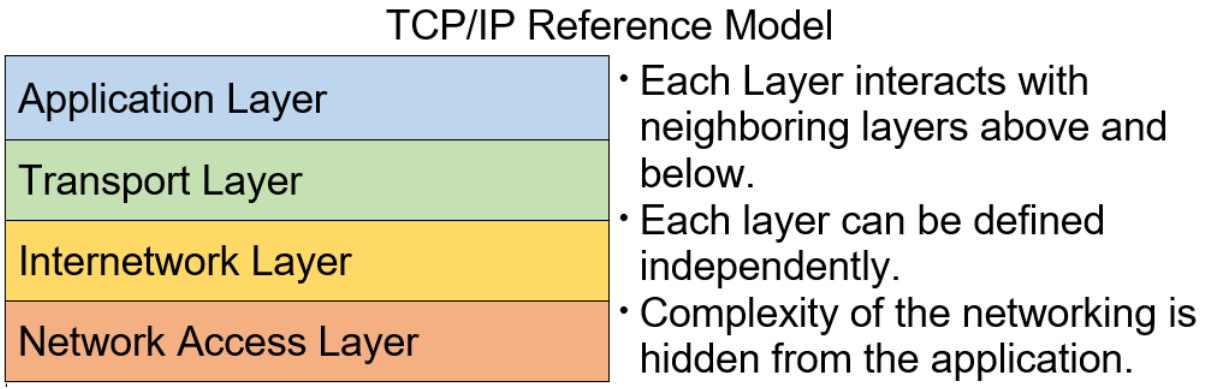
- VLANs define Layer 2 broadcast domains. VLANs on Layer 2 switches create broadcast domains based on the configuration of the switch.
- To interconnect two different VLANs, a router or Layer 3 switch must be used.
- VLANs are often associated with IP networks or subnets.
- The following table explains that the VLANs are organized into three ranges: reserved, normal, and extended.

VLANs	Range	Usage
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.
1	Normal	Cisco default. You can use this VLAN, but you cannot delete it.
2 - 1001	Normal	Used for Ethernet VLANs; you can create, use, and delete these VLANs.
1002 - 1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002-1005.
1006 - 4094	Extended	For Ethernet VLANs only.

5.3 Internetwork Layer

Understanding the Internetwork Layer

- Interconnected networks must have ways to communicate. Internetworking provides that between networks communication method.

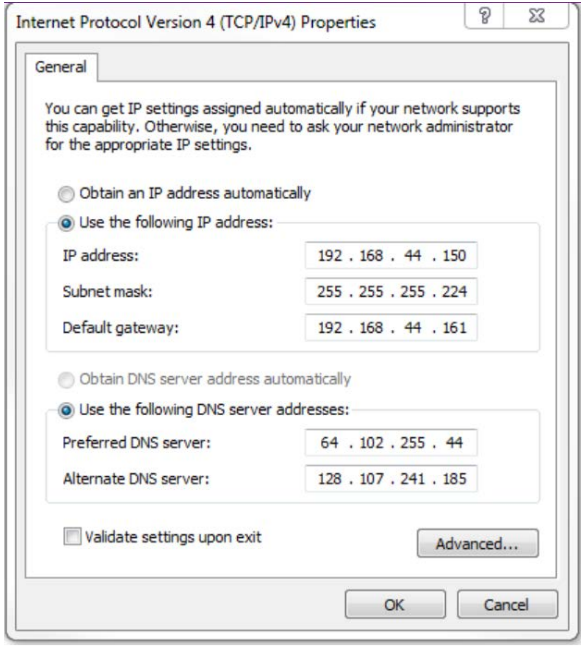


IPv4 Addresses

- An IPv4 address is 32 bits, with each octet (8 bits) represented as a decimal value separated by a dot. This representation is called dotted decimal notation.
- There are three types of IPv4 addresses:
  - **Network address** - A network address is an address that represents a specific network and contains all 0 bits in the host portion of the address.
  - **Host addresses** - Host addresses are addresses that can be assigned to a device such as a host computer, laptop, smart phone, web camera, printer, router, etc. Host addresses contain a least one 0 bit and one 1 bit in the host portion of the address.
  - **Broadcast address** - A broadcast address is an address that is used when it is required to reach all devices on the IPv4 network. It contains all 1 bits in the host portion of the address.The IPv4 subnet mask (or prefix length) is used to differentiate the network portion from the host portion of an IPv4 address.

IPv4 Addresses

- A network can be divided into smaller networks called **subnets**. Subnets can be provided to individual organizational units to simplify the network. The subnet provides a specific range of IP addresses for a group of hosts to use.
- For a device to be able to access the Internet, it must have three things:
  - Every device on a network has a **unique IP address**.
  - A **subnetmask** – to determine the network and host portions of the address.
  - A **default gateway** – the egress point out of the local network to the Internet.



IPv4 Private Addresses

- Devices using private IPv4 addresses are able to access the internet via **Network Address Translation (NAT**) or **Port Address Translation (PAT)**.
- Private addresses are not routable over the Internet.
- Private address ranges (RFC 1918):
  - Class A – 10.0.0.0 – 10.255.255.255
  - Class B – 172.16.0.0 – 172.31.255.255
  - Class C – 192.168.0.0 – 192.168.255.255
- Originally designed in a effort to delay theIPv4 address exhaustion.
- Commonly used for home, office and enterprise networks.

IPv6 Addresses

- IPv6 is designed to be the successor to IPv4. IPv6 has a larger 128-bit address space.
- The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses.
- IPv6 prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities provide an IPv6 addressing hierarchy that allows for more efficient routing.
- IPv6 address space eliminates the need for private addresses; therefore, IPv6 enables new application protocols that do not require special processing by border devices at the edge of networks.

IPv6 Addresses

- IPv6 addresses are represented as a series of 16-bit hexadecimal fields (hextet) separated by colons (:) in the format: x:x:x:x:x:x:x:x. The preferred format includes all the hexadecimal values.
- IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress these zeros at the beginning, middle, or end of an address.
- A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressed	2001:db8:0:1111::200

IPv6 Unicast Addresses

- An IPv6 unicast address is an identifier for a single interface, on a single device.
- A packet that is sent to a unicast address is delivered to the interface identified by that address.
- There are several types of IPv6 unicast addresses including:
  - **Global Unicast Address (GUA)**: This is an IPv6 similar to a public IPv4 address which is globally unique and routable on the IPv6 internet.
  - **Link-Local Addresses (LLA)**: This enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet).
  - **Unique Local Addresses**: These are not yet commonly implemented. However, unique local addresses may eventually be used to address devices that should not be accessible from the outside, such as internal servers and printers.
  - **Multicast Addresses**: These are used instead of broadcast addresses to send a single packet to one or more destinations (multicast group). Note that the multicast addresses can only be destination addresses and not source addresses.
- Note: There are other types of IPv6 unicast addresses besides the four mentioned above. These four are the most significant to for discussion in this course.

Routers and Routing

- Router is a networking device that functions at the internet layer of the TCP/IP model or Layer 3 network layer of the OSI model.
- A router generally has two main functions:

Path Determination	Path determination is the process through which routers use their routing tables to determine where to forward packets. • When a router receives an incoming packet, it checks the destination IP address in the packet and looks up the best match in its routing table. • A matching entry indicates that the destination is directly connected to the router. That router becomes the next-hop router towards the final destination of the packet. • If there is no matching entry, the router sends the packet to the default route. If there is no default route, the router drops the packet.
Packet Forwarding	After the router determines the correct path for a packet, it forwards the packet through a network interface towards the destination network.

Routers and Routing

- Routers use a routing table to route between networks.

```
D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

- A routing table may contain the following types of entries:
  - **Directly connected networks** - Routers add a directly connected route when an interface is configured with an IP address and is activated.
  - **Static routes** - These are routes that are manually configured by the network administrator.
  - **Dynamic routes** - These are routes learned automatically when a dynamic routing protocol is configured and a neighbor relationship to other routers is established. Examples of routing protocols include OSPF, EIGRP, IS-IS, and BGP.
  - **Default routes** - Default routes are either manually entered or learned through a dynamic routing protocol. Default routes are used when no explicit path to a destination is found in the routing table. They are a gateway of last resort option instead of just dropping the packet.

5.4 Network Devices

Ethernet Switches

- A key concept in Ethernet switching is the broadcast domain. A broadcast domain is a logical division in which all devices in a network can reach each other by broadcast at the data link layer.
- Ethernet switches can simultaneously transmit and receive data. This mode is called full-duplex, which eliminates collision domains.
- Switches have the following functions:
  - Operate at the network access layer of the TCP/IP model and the Layer 2 data link layer of the OSI model
  - Filter or flood frames based on entries in the MAC address table
  - Have a large number of high speed and full-duplex ports
- The figure shows an example of switches with multiple high speed and full-duplex ports.

Ethernet Switches

- The switch operates in either of the following switching modes:
  - **Cut-Through Switching Mode** – Switch forwards the data before receiving the entire frame by reading the destination details in the frame header thereby increasing switching speed.
    - **Fragment-free** switching is the typical cut-through method of switching
  - **Store-and-Forward Switching Mode** – Switch receives the entire frame, checks for errors before forwarding it which makes this mode slower than cut-through mode.
- Some characteristics of LAN switches are:
  - **High port density** - Switches have a large number of ports, from 24 to 48 ports per switch in smaller devices, to hundreds of ports per switch chassis in larger modular switches.
  - **Large frame buffers** - Switches have the ability to store received frames when there may be congested ports on servers or other devices in the network.
  - **Fast internal switching** - Switches have very fast internal switching. They are able to switch user traffic from the ingress port to the egress port extremely fast.

Routers

- Routers are needed to reach devices that are not on the same LAN and use routing tables to route traffic between different networks.
- Routers have the following functions:
  - They operate at the internet layer of TCP/IP model and Layer 3 network layer of the OSI model.
  - They route packets between networks based on entries in the routing table.
  - They have support for a large variety of network ports, including various LAN and WAN media ports.
- The figure shows a modular router with integrated switch ports.

Routers

- There are three packet-forwarding mechanisms supported by routers:
  - **Process switching** – When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then determines the exit interface and forwards the packet. This mechanism is very slow and is rarely implemented in modern networks.
  - **Fast switching** – With fast switching, a routing cache mechanism is implemented. Fast switching uses a fast-switching cache to store next-hop information. The flow information for the packet is also stored in the fast-switching cache which means, if another packet of the same destination arrives, the next-hop information in the cache is re-used without CPU intervention.
  - **Cisco Express Forwarding (CEF)** – CEF is the most recent and default Cisco IOS packet-forwarding mechanism. CEF builds a Forwarding Information Base (FIB), and an adjacency table. The table entries are change-triggered that are based on changes in the network topology.

Firewalls

- A firewall is a hardware or software system that prevents unauthorized access into or out of a network.
- Firewalls are used to prevent unauthorized internet users from accessing internal networks.
- All data leaving or entering the protected intranet must pass through the firewall to reach its destination, and any unauthorized data is blocked.
- The figure shows an example of a hardware firewall.

Firewalls

- **Stateless packet-filtering**
  - The most basic (and the original) type of firewall is a stateless packet-filtering firewall.
  - The firewall examines packets as they traverse the firewall, compares them to static rules, and permits or denies traffic accordingly.
  - This is based on several packet header fields, including the following:
    - Source and/or destination IP address
    - IP protocol ID
    - Source and/or destination TCP or UDP Port number
    - ICMP message type
  - This type of firewall works best for TCP applications that use the same static ports every time, or for filtering that is based on Layer 3 information such as source or destination IP address.

Firewalls

- **Stateful packet-filtering**
  - This type of firewall performs header inspection and also keeps track of the connection state.
  - To keep track of the state, these firewalls maintain a state table.
  - Any sessions or traffic initiated by devices on the trusted, inside networks are permitted through the firewall.
  - The firewall understands an initial request, and so an appropriate response from the server is allowed back in through the firewall. It will allow only valid response packets that come from the specific server.
  - The firewall understands standard TCP/IP packet flow including the coordinated change of information between inside and outside hosts that occurs during the life of the connection.
  - These stateful firewalls are more adept at handling Layer 3 and Layer 4 security than a stateless device.

Firewalls

- **Application Layer Packet-Filtering**
  - This is the most advanced type of firewall. The deep inspection of the packet occurs all the way up to the OSI model's Layer 7.
  - This gives more reliable and capable access control for OSI Layers 3–7, with simpler configuration.
  - The application layer firewall can determine an File Transfer Protocol (FTP) session, just like a stateless or stateful firewall can.
  - The firewall's deeper packet inspection capability enables it to verify adherence to standard HTTP protocol functionality.
  - It can deny requests that do not conform to the standards or meet the criteria established by the security team.

Load Balancers

- **Load balancing** improves the distribution of workloads across multiple computing resources, such as servers, cluster of servers, network links and so on.
- Server load balancing helps ensure the availability, scalability, and security of applications and services by distributing the work of a single server across multiple servers.
- At the device level, the load balancer provides the following features to support high network availability:
  - Device redundancy
  - Scalability
  - Security
- At the network service level, a load balancer provides the following advanced services:

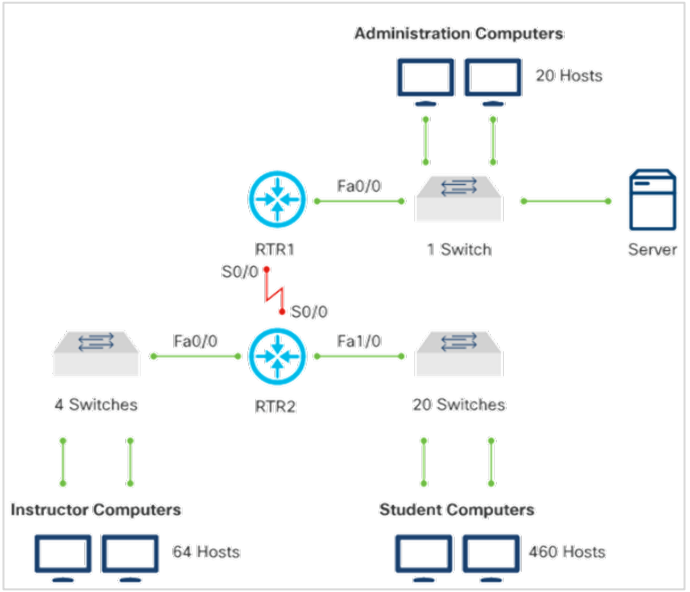
High services availability	Scalability	Services-level security
This allows distribution of client requests among physical servers and server farms.	Virtualization allows the use of advanced load-balancing algorithms to distribute client requests among the virtual devices.	This allows establishment and maintenance of a Secure Sockets Layer (SSL) session between the load balancer and its peer.

Network Diagrams

- Network diagrams are part of the documentation that goes with a network deployment and also play an important role when the documentation steps in programming code.
- They display a visual and intuitive representation of the network, depicting how are all the devices connected and what interface connects to each device and so on.
- There are generally two types of network diagrams:
  - **Layer 2 physical connectivity diagrams**: These are the network diagrams that represent the port connectivity between the devices in the network.
  - **Layer 3 logical connectivity diagrams**: These are the network diagrams which display the IP connectivity between devices on the network.

Network Diagrams

- A simplified Layer 2 network diagram is shown here.
- This diagram gives a general idea of how the clients connect to the network and how the network devices connect to each other so that end to end connectivity between all clients is accomplished.



5.5 Networking Protocols

Networking Protocols

- It is essential to understand the standard network protocols for effective communication and troubleshooting.

Telnet and Secure Shell (SSH)

- These protocols are used to connect and log into a remote computer.
- SSH uses encryption to protect data over a network connection and hence is most frequently used.
- Telnet should only be used in non-prod environments.
- SSH uses port 22
- Telnet uses port 23

HTTP and HTTPS

- HTTP stands for Hyper Text Transfer Protocol and HTTPS is the secure version of HTTP.
- HTTP uses port 80
- HTTPS uses port 443
- These protocols are recognized by web browsers and are used to connect to web sites.
- HTTPS uses TLS or SSL to make a secure connection.

NETCONF and RESTCONF

- NETCONF uses port 830.
- RESTCONF does not have a reserved port value.
- To have multiple network operations, make sure each protocol has a default port and use standards to try to avoid conflicts.

DHCP

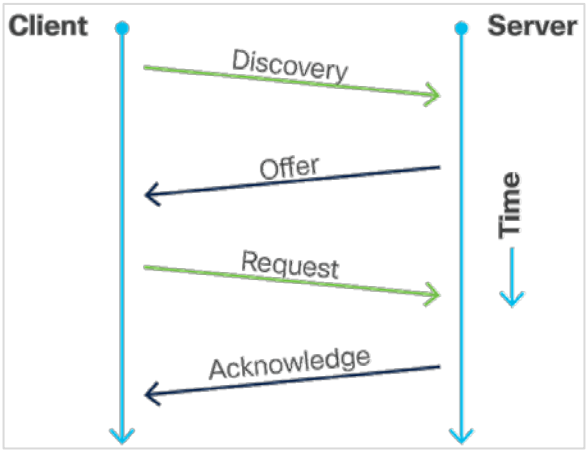
- DHCP works within a client/server model, where DHCP servers allocate IP addresses and deliver configuration information to devices that are configured to dynamically request addressing information.
- In addition to the IP address for the device itself, a DHCP server can also provide additional information, like the IP address of the DNS server, default router, and other configuration parameters.
- Some of the benefits of using DHCP instead of manual configurations are reduced client configuration tasks and costs and centralized management
- DHCP allocates IP addresses in three ways: Automatic allocation, Dynamic allocation, Manual allocation.

DHCP

- **DHCP Relay**
  - In cases in which the DHCP client and server are located in different subnets, a DHCP relay agent can be used. A relay agent is any host that forwards DHCP packets between clients and servers.
  - Relay agents receive DHCP messages and then generate new DHCP messages on another interface.

DHCP

- **DHCP Operations**
  - DHCP operations includes four messages between the client and the server:
    - **DHCPDISCOVER** - Server discovery
    - **DHCPPOFFER** - IP lease offer
    - **DHCPREQUEST** - IP lease request
    - **DHCPACK** - IP lease acknowledgment
  - The client broadcasts a DHCPDISCOVER message looking for a DHCP server..
  - The server responds with a unicast DHCPOFFER.
  - In case of multiple DHCP servers, it identifies the explicit server and broadcast a DHCPREQUEST message and lease offer.
  - The server sends a unicast DHCP acknowledgment message acknowledging to the client that the lease has been finalized.



DNS

- In data networks, devices are labeled with numeric IP addresses to send and receive data over networks. Domain names (DNS) were created to convert the numeric address into a simple, recognizable name.
- The DNS protocol defines an automated service that matches domain names to IP addresses.
- DNS uses port 53
- It includes the format for queries, responses, and data. DNS uses a single format called a DNS message.
- **DNS Message Format**
  - The DNS server stores different types of resource records that are used to resolve names. Some of these record types are as follows:
    - **A** – An end device IPv4 address
    - **NS** – An authoritative name server
    - **AAAA** – An end device IPv6 address (pronounced quad-A)
    - **MX** – A mail exchange record

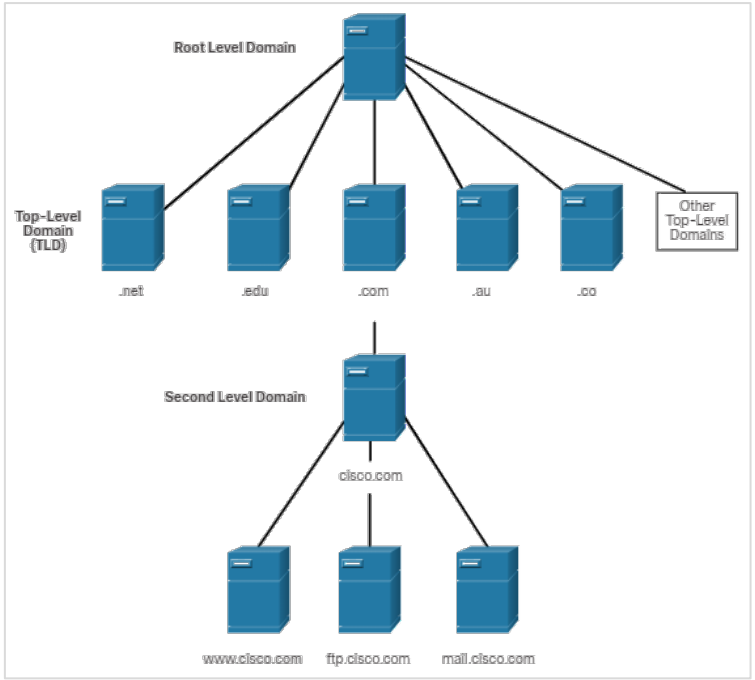
DNS

- When a client makes a query to its configured DNS server, the DNS server first looks at its own records to resolve the name. If it is unable to resolve the name by using its stored records, it contacts other servers to resolve the name.
- After a match is found and returned to the requesting server, the server temporarily stores the address in the event that the same name is requested again.
- As shown in the following table, DNS uses the same message format between servers

DNS Message Section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

DNS

- **DNS Hierarchy**
  - DNS uses a hierarchical system based on domain names to create a database to provide name resolution.
  - The naming structure is broken down into small, manageable zones.
  - When a DNS server receives a request for a name translation that is not within its DNS zone, then it forwards the request to another DNS server within the proper zone for translation.

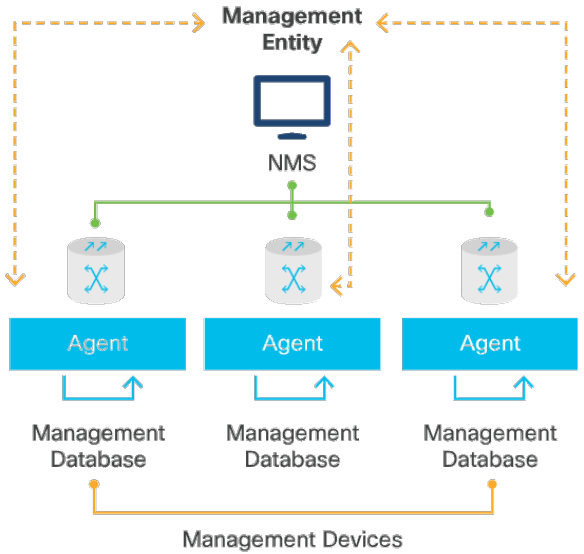


SNMP

- SNMP was developed to allow administrators to manage devices such as servers, workstations, routers, switches, and security appliances, on an IP network.
- SNMP is an application layer protocol that provides a message format for communication between managers and agents.
- The SNMP system consists of three elements:
  - SNMP manager: network management system (NMS)
  - SNMP agents (managed node)
  - Management Information Base (MIB)

SNMP

- **SNMP Components**
  - To configure SNMP on a networking device, it is first necessary to define the relationship between the manager and the agent.
  - The SNMP manager is part of a network management system (NMS).
  - It can collect information from an SNMP agent by using the get action and can change configurations on an agent by using the set action.
  - Also, SNMP agents can forward information directly to the SNMP manager by using traps.



SNMP

- **SNMP Operation**
  - A SNMP agents running on a device collects and stores information about the device and its operation. The SNMP manager then uses the SNMP agent to access information within the MIB and make changes to the device configuration.
  - There are two primary SNMP manager requests, get and set. A get request is used by the SNMP manager to query the device for data. A set request is used by the SNMP manager to change configuration variables in the agent device.

SNMP

- **SNMP Polling**
  - The NMS can be configured to periodically have the SNMP managers poll the SNMP agents.
  - Using this process, the information is collected to monitor traffic loads and to verify the device configurations of managed devices.
  - The data can be graphed, or thresholds can be established to trigger a notification process when the thresholds are exceeded.

SNMP

- **SNMP Traps**
  - Traps are a term given to SNMP log messages that are generated by network devices and sent to the SNMP server.
  - Periodic SNMP polling have some drawbacks:
    - Delay between the time that an event occurs and the time that it is noticed (via polling) by the NMS.
    - Trade-off between polling frequency and bandwidth usage.
  - To mitigate the disadvantages, SNMP agents generate and send traps to inform the NMS immediately of certain events.
- **SNMP Community Strings**
  - For SNMP to operate, the NMS must have access to the MIB.
  - SNMPv1 and SNMPv2c use community strings (plaintext passwords) that control access to the MIB.
  - SNMP community strings authenticate access to MIB objects.
  - There are two types of community strings: Read-only (ro) and Read-write (rw)

SNMP

- **Management Information Base (MIB)**
  - MIBs are data structures that describe SNMP network elements as a list of data objects.
  - The MIB is organized in a tree-like structure with unique variables represented as terminal leaves.
  - An Object IDentifier (OID) is a long numeric tag. It is used to distinguish each variable uniquely in the MIB and in the SNMP messages.
  - Variables that measure things such as CPU temperature, inbound packets on an interface, fan speed, and other metrics, all have associated OID values.
  - SNMP traps are used to generate alarms and events that are happening on the device. Traps contain:
    - OIDs that identify each event and match it with the entity that generated the event
    - Severity of the alarm (critical, major, minor, informational or event)
    - A date and time stamp

SNMP

- **SNMP Communities**
  - SNMP community names are used to group SNMP trap destinations.
  - When community names are assigned to SNMP traps, the request from the SNMP manager is considered valid if the community name matches the one configured on the managed device otherwise, SNMP drops the request.
- **SNMP Messages**
  - SNMP uses the following messages to communicate between the manager and the agent:
    - **Get and GetNext** - The Get and GetNext messages are used when the manager requests information for a specific variable.
    - **GetResponse** - When the agent receives a Get or GetNext message it will issue a GetResponse message back to the manager.
    - **Set** - A Set message is used by the manager to request that a change should be made to the value of a specific variable.
    - **Trap** - The Trap message is used by the agent to inform the manager when important events take place.

NTP

- The main role of Network Time Protocol (NTP) is to synchronize the time of the devices on the network.
- NTP enables a device to update its clock from a trusted network time source. A device receiving authoritative time can be configured to serve time to other machines, enabling groups of devices to be closely synchronized.
- NTP runs over UDP using port 123 as source and destination.
- An authoritative time source is usually a radio clock, or an atomic clock attached to a time server. Authoritative server in NTP is a very accurate time source. It is the role of NTP to distribute the time across the network.
- NTP uses the concept of strata (layers) to describe how far away a host is from an authoritative time source. The most authoritative sources are in stratum 1.

NTP

- NTP avoids synchronizing with upstream servers whose time is not accurate by using these two ways:
  - NTP never synchronizes with a NTP server that is not itself synchronized.
  - NTP compares time reported by several NTP servers and will not synchronize to a server whose time is an outlier.
- Clients usually synchronize with the lowest stratum server they can access. But NTP incorporates safeguards as well: it prefers to have access to at least three lower-stratum time sources because this helps it determine if any single source is incorrect.
- **NTP Association Modes** - NTP servers can associate in several modes, including:
  - Client/Server
  - Symmetric Active/Passive
  - Broadcast

NTP

- **Client/Server Mode**
  - This is the most common mode in which a client or dependent server can sync with a group member, but not the reverse, protecting against protocol attacks or malfunctions.
  - Client-to-server requests are made via asynchronous remote procedure calls.
  - In this mode, a client requests time from one or more servers and processes replies as received. The server changes addresses and ports, overwrites message fields, recalculates the checksum, and returns the message immediately.
  - Information included in the NTP message lets the client determine the skew between server and local time, enabling clock adjustment.
  - The message also includes information to calculate the expected timekeeping accuracy and reliability, as well as help the client select the best server.

NTP

- **Symmetric Active/Passive Mode**
  - In this mode, a group of low stratum peers work as backups for one another. Each peer derives time from one or more primary reference sources or from reliable secondary servers.
  - Symmetric/active mode is usually configured by declaring a peer in the configuration file, telling the peer that one wishes to obtain time from it, and provide time back if necessary.
  - Symmetric modes are most often used to interconnect two or more servers that work as a mutually redundant group.

NTP

- **Broadcast and/or Multicast Mode**
  - When only modest requirements for accuracy exist, clients can use NTP broadcast and/or multicast modes, where many clients are configured the same way, and one broadcast server (on the same subnet) provides time for them all.
  - Configuring a broadcast server is done using the broadcast command, and then providing a local subnet address. The broadcast client command lets the broadcast client respond to broadcast messages received on any interface.
  - This mode cannot be used beyond a single subnet. This mode should always be authenticated because an intruder can impersonate a broadcast server and propagate false time values.

NAT

- **Network Address Translation (NAT)** helps with the problem of IPv4 address depletion. NAT works by mapping thousands of private internal IPv4 addresses to a range of public addresses.
- NAT identifies traffic to and from a specific device, translating between external/public and internal/private IPv4 addresses.
- It enables an organization to easily change service providers or voluntarily renumber network resources without affecting their public IPv4 address space.
- NAT also hides clients on the internal network behind a range of public addresses, providing a sense of security against the devices being directly attacked from outside.
- **Types of NAT**
  - Static address translation (static NAT)
  - Dynamic address translation (dynamic NAT)
  - Overloading (also called Port Address Translation or PAT)

NAT

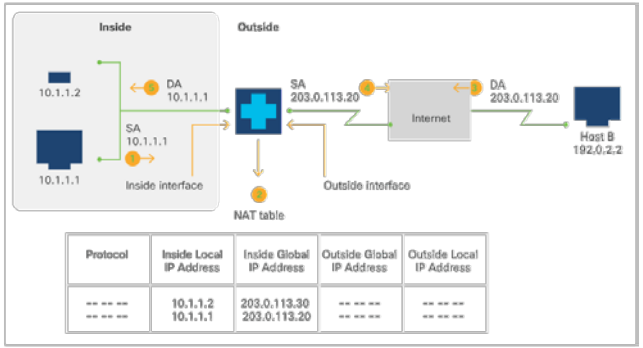
- IPv6 was developed with the intention of making NAT unnecessary.
- IPv6 provides protocol translation between IPv4 and IPv6. This is known as NAT64. NAT for IPv6 is used in a much different context than NAT for IPv4.
- The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks.
- NAT includes four types of addresses:
  - **Inside address** - This is the address of the device which is being translated by NAT.
  - **Outside address** - This is the address of the destination device.
  - **Local address** - This is any address that appears on the inside portion of the network.
  - **Global address** - This is any address that appears on the outside portion of the network.

NAT

- **Inside Local address** - Consider the term "Inside" as inside our network. Inside local address is an IP address assigned to a workstation inside our network. Inside Local addresses are typically private IP addresses, which stay inside our network.
- **Inside Global address** - Inside Global address are typically public IP addresses which are assigned to our end internet facing router to be used as the IP address for communicating with other devices in the internet. The Inside Local IP addresses are removed at the NAT router and translated with Inside Global address.
- **Outside Global address** - Outside Global address is the public IP address assigned to the end device on the other network to communicate other devices in the internet. Outside Global addresses are public IP addresses which are routable.
- **Outside local address** - Outside local address is the real IP address of the end device at other network. Outside local addresses are typically private IP addresses assigned to the computers in the other private network. We cannot know the Outside local addresses because in a NAT enabled network we use the destination IP address as Outside Global address.

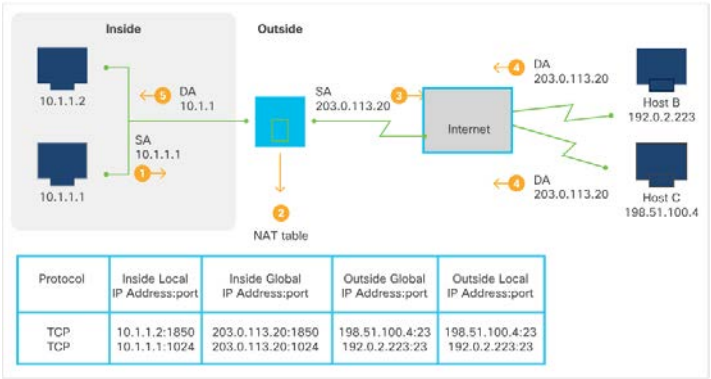
NAT

- **Inside Source Address Translation**
  - IPv4 addresses can be translated into globally-unique IPv4 addresses when communicating outside the internal network. There are two options to accomplish this:
    - **Static translation** - This method sets up a one-to-one mapping between an inside local address and an inside global address; useful when a host on the inside must be accessed from a fixed outside address.
    - **Dynamic translation** - This method maps between inside local addresses and a global address pool.
  - The figure shows a device translating a source address inside a network to a source address outside the network.



NAT

- **Overloading of Inside Global Addresses**
  - Using a single global address for multiple local addresses is known as overloading.
  - When overloading is configured, the NAT device gathers information from higher-level protocols (for example, TCP or UDP port numbers) to translate global addresses back to correct local addresses.
  - To map multiple local addresses to one global address, TCP or UDP port numbers are used to distinguish local addresses. This NAT process is called **Port Address Translation (PAT)**.



Protocol	Inside Local IP Address:port	Inside Global IP Address:port	Outside Global IP Address:port	Outside Local IP Address:port
TCP TCP	10.1.1.2:1850 10.1.1.1:1024	203.0.113.20:1850 203.0.113.20:1024	198.51.100.4:23 192.0.2.223:23	198.51.100.4:23 192.0.2.223:23

5.6 Troubleshooting Application Connectivity Issues

Troubleshooting Common Network Connectivity Issues

- Network troubleshooting usually follows the OSI layers.
- You can start either top to bottom beginning at the application layer and making your way down to the physical layer. Or you can go from the bottom to the top.
- Solutions like Cisco AppDynamics can offer a deeper view into application performance and root cause analysis of application issues.

Troubleshooting Common Network Connectivity Issues

- A typical troubleshooting session starting from physical layer and making our way up the stack of layers towards the application layer:
  - Determine how the client connects to the network - is it a wired or wireless connection?
  - If the client connects via an Ethernet cable, make sure the NIC comes online and there are electrical signals being exchanged with the switch port to which the cable is connected.
  - If the NIC is connected, the physical layer is working as expected.
  - If the NIC is not connected or enabled, check the configuration on the switch. The port to which the client is connecting might be shut down, or maybe the cable connecting the client to the network port in the wall is defective, or the cable connecting the network port from the wall all the way to the switch might be defective.

Troubleshooting Common Network Connectivity Issues

- Troubleshooting at the physical layer is to ensure that there are four uninterrupted pairs of twisted copper cables between the network client and the switch port.
- If the client uses a wireless connection, check if the wireless network interface is turned on and make sure you stay in the range of the wireless access point.
- Moving up to the data link layer, or Layer 2, ensure the client is able to learn destination MAC ensure that the addresses (using ARP) and also that the switch to which the client is connecting is able to learn the MAC addresses received in its ports.
- If you can verify that the both these tables are accurate, then you can move to the next layer.

Troubleshooting Common Network Connectivity Issues

- If the client cannot see any MAC addresses in its local ARP table, check for any Layer 2 access control lists on the switch port that might block this traffic. Also ensure that the switch port is configured for the correct client VLAN.
- At the network layer, or Layer 3, ensure the client obtains the correct IP address from the DHCP server, or is manually configured with the correct IP address and the correct default gateway.
- If Layer 3 connectivity cannot be established, check IP access lists on the router interfaces, check the routing table on both the client and the default gateway router and make sure the traffic is routed correctly.
- If Layer 3 connectivity can be established all the way from the client to the destination, move on with troubleshooting to the transport layer, or Layer 4.
- If Layer 3 connectivity cannot be established, check IP access lists on the router interfaces, check the routing table on both the client and the default gateway router and make sure the traffic is routed correctly.

Troubleshooting Common Network Connectivity Issues

- If a transport connection cannot be established, verify firewalls and security appliances that are placed on the path of traffic for rules that are blocking the traffic based on TCP and UDP ports.
- Verify if any load balancing is enabled and if the load balancer is working as expected, or if any proxy servers intercepting the traffic are filtering and denying the connection.
- Traffic load and network delay are the most difficult to troubleshoot. Implementing QoS throughout the network can help with these issues.
- If despite the network troubleshooting, you have not been able to identify any issue, there is a good chance that the problem is not with the network.

Networking Tools – Using ifconfig

- **`ifconfig`** is a software utility for UNIX-based operating systems. There is also a similar utility for Microsoft Windows-based operating systems called ipconfig.
- The main purpose of this utility is to manage, configure, and monitor network interfaces and their parameters.
- ifconfig runs as a command-line interface tool and comes by default installed with most operating systems.
- The ifconfig command has been used within Linux for many years. However, some Linux distributions have deprecated the ifconfig command. The **`ip address`** command is becoming the new alternative. You will see the ip address command used in some of the labs in this course.
- The common uses for ifconfig are:
  - Configure IP address and subnet mask for network interfaces.
  - Query the status of network interfaces.
  - Enable/disable network interfaces.
  - Change the MAC address on an Ethernet network interface.

Networking Tools – Using ifconfig

- Issuing the **`ifconfig --help`** command in the command line interface will display all the options available with this version of ifconfig.
- ifconfig gives us the option to **`add`** (add) or **`del`** (delete) IP addresses and their subnet mask (prefix length) to a specific network interface.
- The **`hw ether`** gives us the option to change the Ethernet MAC address.

```
devasc@labvm:~$ ifconfig --help
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast [<address>]]  [[-]pointopoint [<address>]]
  [netmask <address>]  [dstaddr <address>]  [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>]  [mtu <NN>]
  [[-]trailers]  [[-]arp]  [[-]allmulti]
  [multicast]  [[-]promisc]
  [mem_start <NN>]  [io_addr <NN>]  [irq <NN>]  [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...
<output omitted>
```

Networking Tools – Using ifconfig

- If **`ifconfig`** is issued without any parameters, it just returns the status of all the network interfaces on that host.
- The **Maximum Transmission Unit (MTU)** specifies the maximum number of bytes that the frame can be transmitted on this medium before being fragmented.
- The **RX packets** and **RX bytes** contain the values of the received packets and bytes respectively on that interface.
- The **TX packets** and **TX bytes** contain the values of transmit packets and bytes on that specific interface.

```
devasc@labvm:~$ ifconfig
dummy0: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet 192.0.2.1  netmask 255.255.255.255  broadcast 0.0.0.0
        inet6 fe80::48db:6aff:fe27:4849  prefixlen 64  scopeid 0x20<link>
        ether 4a:db:6a:27:48:49  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12293  bytes 2544763 (2.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee9:3de6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e9:3d:e6  txqueuelen 1000  (Ethernet)
        RX packets 280055  bytes 281957761 (281.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 112889  bytes 10175993 (10.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 46014  bytes 14094803 (14.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46014  bytes 14094803 (14.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

devasc@labvm:~$
```

Using ping

- **`ping`** is a software utility used to test IP network reachability for hosts and devices connected to a specific network.
- It is available virtually on all operating systems and is extremely useful for troubleshooting connectivity issues.
- The ping utility uses **Internet Control Message Protocol (ICMP)** to send packets to the target host and then waits for ICMP echo replies.
- Based on this exchange of ICMP packets, ping reports errors, packet loss, roundtrip time, Time To Live (TTL) for received packets, and so on.

Using ping

- On Windows 10, enter the **`ping`** command to view its usage information.
- The output should look similar to the figure:

```
C:\> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\>
```

Using ping

- On MacOS Catalina, enter the **`ping`** command to view its usage information.
- The output should look similar to the figure:

```
$ ping
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize]
            [-g sweepminsize] [-h sweepincrsize] [-i wait]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern]
            [-S src_addr] [-s packetsize] [-t timeout][-W waittime]
            [-z tos] host
       ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern] [-S src_addr]
            [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
            [-z tos] mcast-group
Apple specific options (to be specified before mcast-group or host like all options)
            -b boundif           # bind the socket to the interface
            -k traffic_class     # set traffic class socket option
            -K net_service_type  # set traffic class socket options
            -apple-connect       # call connect(2) in the socket
            -apple-time          # display current time
```

Using ping

- On Linux, use the **`ping -help`** option to view its usage information.
- The output should look similar to the figure:

```
devasc@labvm:~$ ping -help

Usage
  ping [options] <destination>

Options:
  <destination>      dns name or ip address
  -a                 use audible ping
  -A                 use adaptive ping
  -B                 sticky source address
  -c <count>         stop after <count> replies
  -D                 print timestamps
  -d                 use SO_DEBUG socket option
  -f                 flood ping
  -h                 print help and exit
<output omitted>

IPv4 options:
  -4                 use IPv4
  -b                 allow pinging broadcast
  -R                 record route
  -T <timestamp>     define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6                 use IPv6
  -F <flowlabel>     define flow label, default is random
  -N <nodeinfo opt>  use icmp6 node info query, try <help> as argument

For more details see ping(8).
devasc@labvm:~$
```

Using ping

- By default, ping (or ping -help in Linux) will display all the available options. Some of the options you can specify include:
  - Count of how many ICMP echo requests you want to send.
  - Source IP address in case there are multiple network interfaces on the host
  - Timeout to wait for an echo reply packet
  - Packet size, if you want to send larger packet sizes than the default 64 bytes. This option is very important when determining what is the MTU on an interface.
- If you do not receive any reply from the destination you are trying to reach with ping, it does not mean that the host is offline or not reachable. It could simply mean that ICMP echo-request packets are filtered by a firewall and are not allowed to reach the host destination.

Using traceroute

- **`traceroute`** displays the route that the packets take to display the host reachability on the network.
- traceroute uses ICMP packets to determine the path to the destination.
- On Windows 10, use tracert to see the available options as shown in the output:

```
C:\> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\>
```

- Instead of ICMP, by default, Linux uses UDP and a high port range (33434 - 33534). Destinations along the path respond with ICMP port unreachable messages instead of the echo replies sent in ICMP-based traceroutes.

Using traceroute

- On MacOS, use **`traceroute`** to see the available options as shown in the figure:

```
$ traceroute
Version 1.4a12+Darwin
Usage: traceroute [-adDeFInrSvx] [-A as_server] [-f first_ttl] [-g gateway] [-i iface]
    [-M first_ttl] [-m max_ttl] [-p port] [-P proto] [-q nqueries] [-s src_addr]
    [-t tos] [-w waittime] [-z pausemsecs] host [packetlen]
```

Using traceroute

- On Linux, use **`traceroute --help`** to see the available options as shown in the figure:

```
devasc@labvm:~$ traceroute --help
Usage: traceroute [OPTION...] HOST
Print the route packets trace to network host.

  -f, --first-hop=NUM        set initial hop distance, i.e., time-to-live
  -g, --gateways=GATES       list of gateways for loose source routing
  -I, --icmp                 use ICMP ECHO as probe
  -m, --max-hop=NUM          set maximal hop count (default: 64)
  -M, --type=METHOD          use METHOD (`icmp' or `udp') for traceroute
                             operations, defaulting to `udp'
  -p, --port=PORT            use destination PORT port (default: 33434)
  -q, --tries=NUM            send NUM probe packets per hop (default: 3)
      --resolve-hostnames    resolve hostnames
  -t, --tos=NUM              set type of service (TOS) to NUM
  -w, --wait=NUM             wait NUM seconds for response (default: 3)
  -?, --help                 give this help list
      --usage                give a short usage message
  -V, --version              print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Report bugs to <bug-inetutils@gnu.org>.
devasc@labvm:~$]
```

Using traceroute

- Several options are available with traceroute including:
  - Specifying the TTL value of the first packet sent. By default this is 1.
  - Specifying the maximum TTL value. By default, it will increase the TTL value up to 64 or until the destination is reached.
  - Specifying the source address in case there are multiple interfaces on the host.
  - Specifying QoS value in the IP header.
  - Specifying the packet length.

Using traceroute

- You can **`tracert`** from your Windows device or **`traceroute`** from your MacOS device.
- The output is from a MacOS device inside the corporate Cisco network tracing the route to one of Yahoo's web servers.

```
$ traceroute www.yahoo.com
traceroute: Warning: www.yahoo.com has multiple addresses; using 98.138.219.232
traceroute to atsv2-fp-shed.wg1.b.yahoo.com (98.138.219.232), 64 hops max, 52 byte packets
 1  sjc2x-dtbb.cisco.com (10.1x.y.z)  2.422 ms  1.916 ms  1.773 ms
 2  sjc2x-dt5.cisco.com (12x.1y.1z.1ww)  2.045 ms
    sjc2x-dt5-01.cisco.com (12x.1y.1z.15w)  2.099 ms  1.968 ms
 3  sjc2x-sbb5.cisco.com (1xx.1x.1xx.4y)  1.713 ms  1.984 ms
    sjc2x-sbb5-10.cisco.com (1xx.1x.1y.4w)  1.665 ms
 4  sjc2x-rbb.cisco.com (1xx.1y.zz.yyy)  1.836 ms  1.804 ms  1.696 ms
 5  sjc1x-rbb-7.cisco.com (1xx.zz.y.ww)  68.448 ms  1.880 ms  1.939 ms
 6  sjc1x-corp-0.cisco.com (1xx.yy.z.w)  1.890 ms  2.660 ms  2.793 ms
 7  * * *
 8  * * *
 9  * * *
```

- Note: The output above has been altered for security reasons, but your output should actually have both valid hostnames and IP addresses.

Using nslookup

- **`nslookup`** is another command-line utility used for querying DNS to obtain domain name to IP address mapping. This tool is useful to determine if the DNS server configured on a specific host is working as expected and actually resolving hostnames to IP addresses.
- Execute the command **`nslookup www.cisco.com 8.8.8.8`** to resolve the IP address or addresses for Cisco's web server and specify that you want to use Google's DNS server at 8.8.8.8 to do the resolution.

```
devasc@labvm:~$ nslookup www.cisco.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.cisco.com   canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net        canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net     canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net      canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 23.204.11.200
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1404:5800:392::b33
Name:   e2867.dsca.akamaiedge.net
Address: 2600:1404:5800:39a::b33

devasc@labvm:~$
```

5.7 Networking Fundamentals Summary

What Did I Learn in this Module?

- A network consists of end devices such as computers, mobile devices, and printers that are connected by networking devices such as switches and routers.
- Both the OSI and the TCP/IP reference models use layers to describe the functions and services that can occur at that layer.
- All network devices on the same network must have a unique MAC address.
- Every device on a network has a unique IP address. An IP address and a MAC address are used for access and communication across all network devices.
- While switches are used to connect devices on LAN, routers are used to route traffic between different networks.
- A firewall is a hardware or software system that prevents unauthorized access into or out of a network.

What Did I Learn in this Module?

- Load balancing improves the distribution of workloads across multiple computing resources, such as servers, cluster of servers, network links, and so on.
- Server load balancing helps ensure the availability, scalability, and security of applications and services by distributing the work of a single server across multiple servers.
- Network diagrams display a visual and intuitive representation of the network.
- There are multiple network operations that use different protocols such as SSH, Telnet, DNS, http, NETCONF and RESTCONF. Each protocol has a default port.
- ping is a software utility used to test IP network reachability for hosts and devices connected to a specific network.
- traceroute uses ICMP packets to determine the path to the destination.
- nslookup is another command-line utility used for querying DNS to obtain domain name to IP address mapping.


CISCO


Elk Technologies
https://elktech.org
SCOTT STEPHENSON