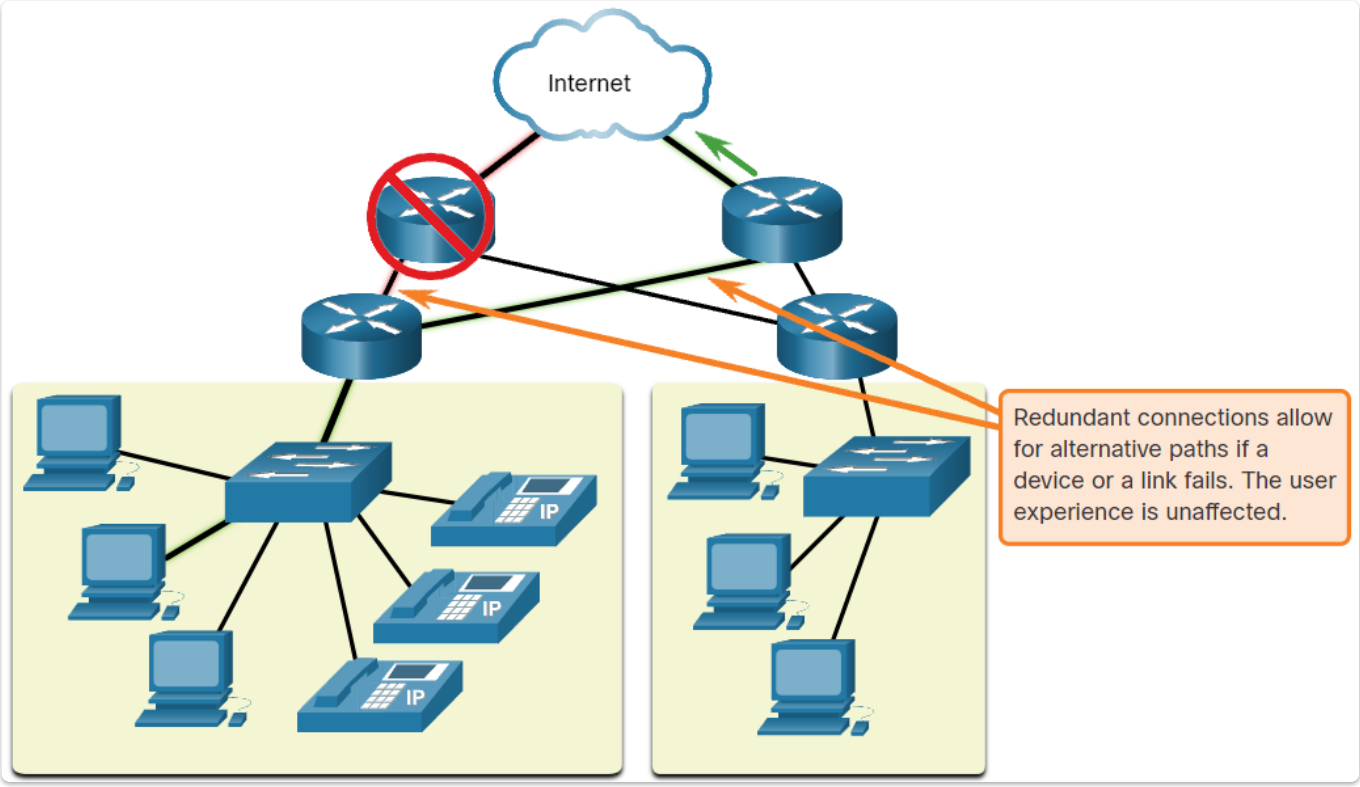
Networking Devices and Initial Configuration

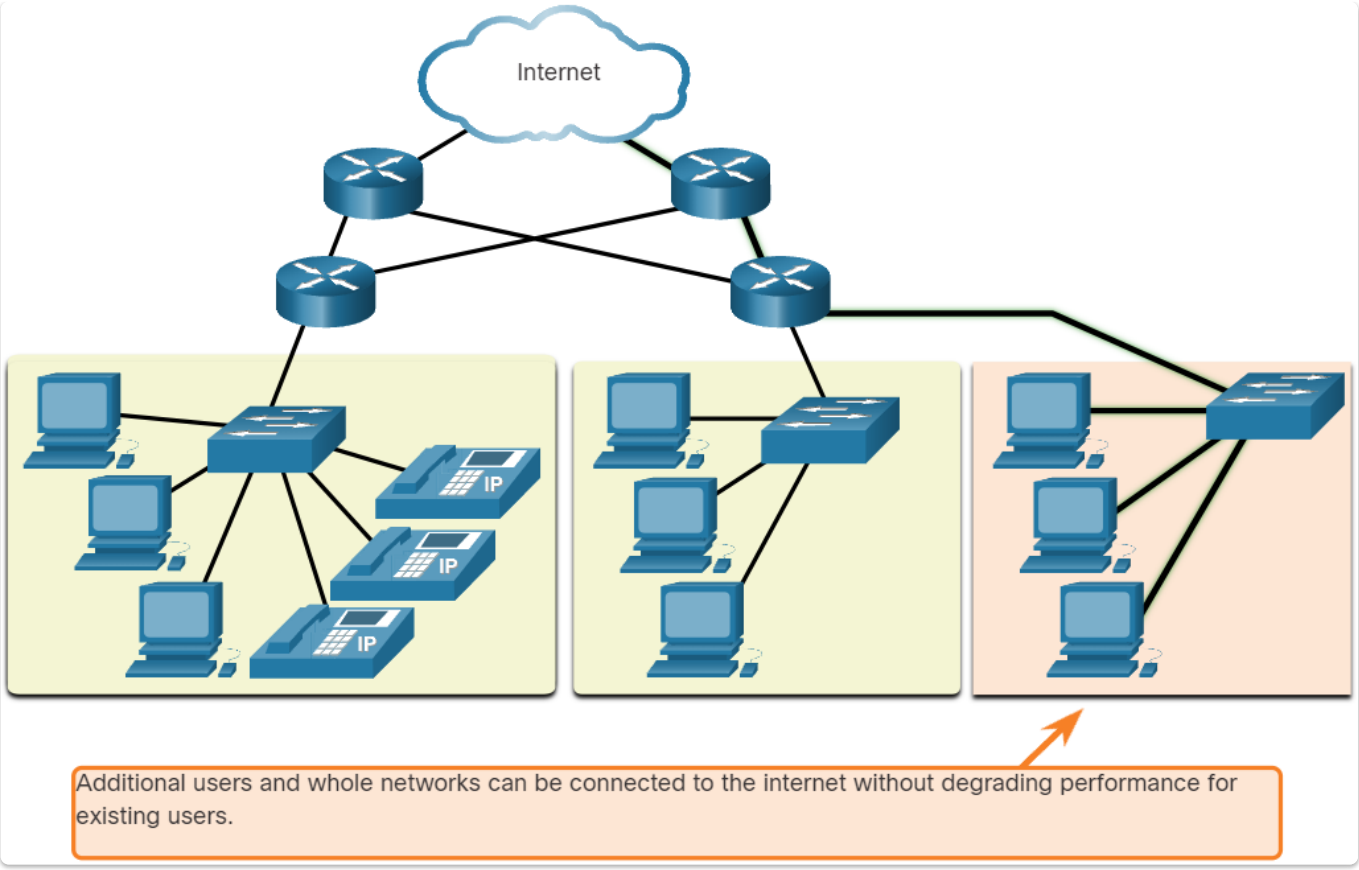
1. Network Design

Reliable Networks

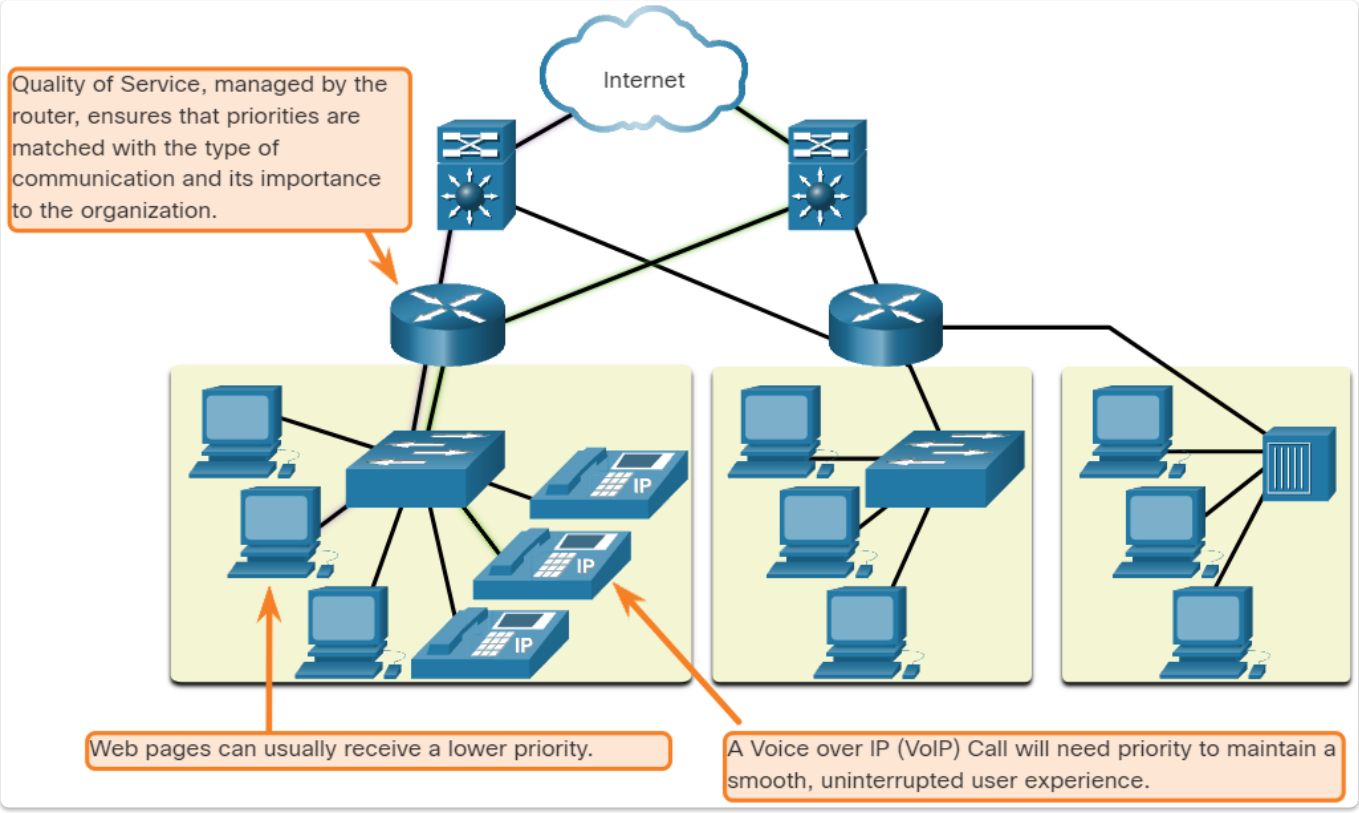
As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations: Fault Tolerance, scalability, QoS, and security.



A fault tolerant network limits the number of affected devices during a failure. It allows quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages are instantly sent over a different link.

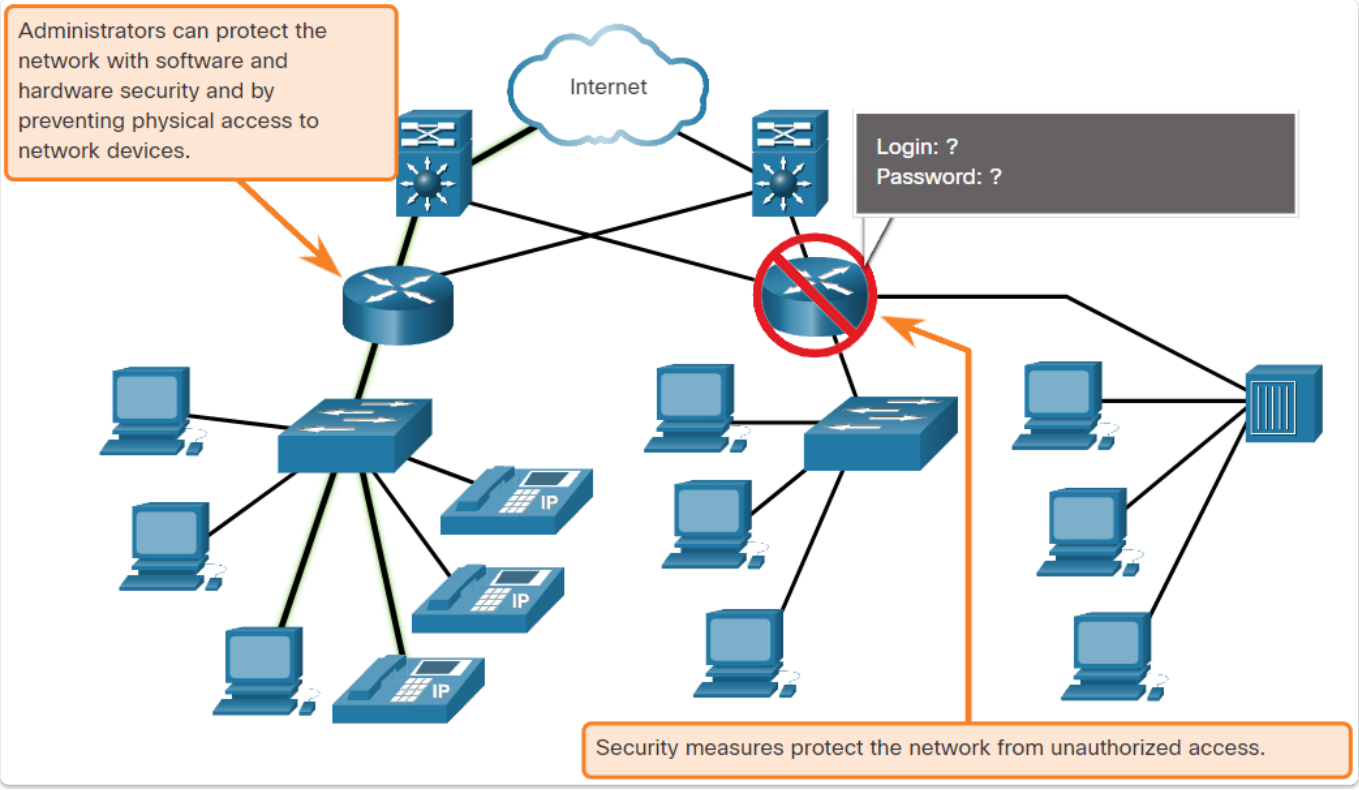


A scalable network expands quickly to support new users and applications. It does this without degrading the performance of services that are being accessed by existing users. Networks can be scalable because the designers follow accepted standards and protocols.



QoS is an increasing requirement of networks today. As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users. Network bandwidth is measured in bps. When

simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The focus of QoS is to prioritize time-sensitive traffic. The type of traffic, not the content of the traffic, is what is important.



Network administrators must address two types of network security concerns: network infrastructure security and information security. Network administrators must also protect the information contained within the packets being transmitted over the network, and the information stored on network attached devices. There are three primary requirements to achieve the goals of network security: Confidentiality, Integrity, and Availability.

Hierarchical Network Design

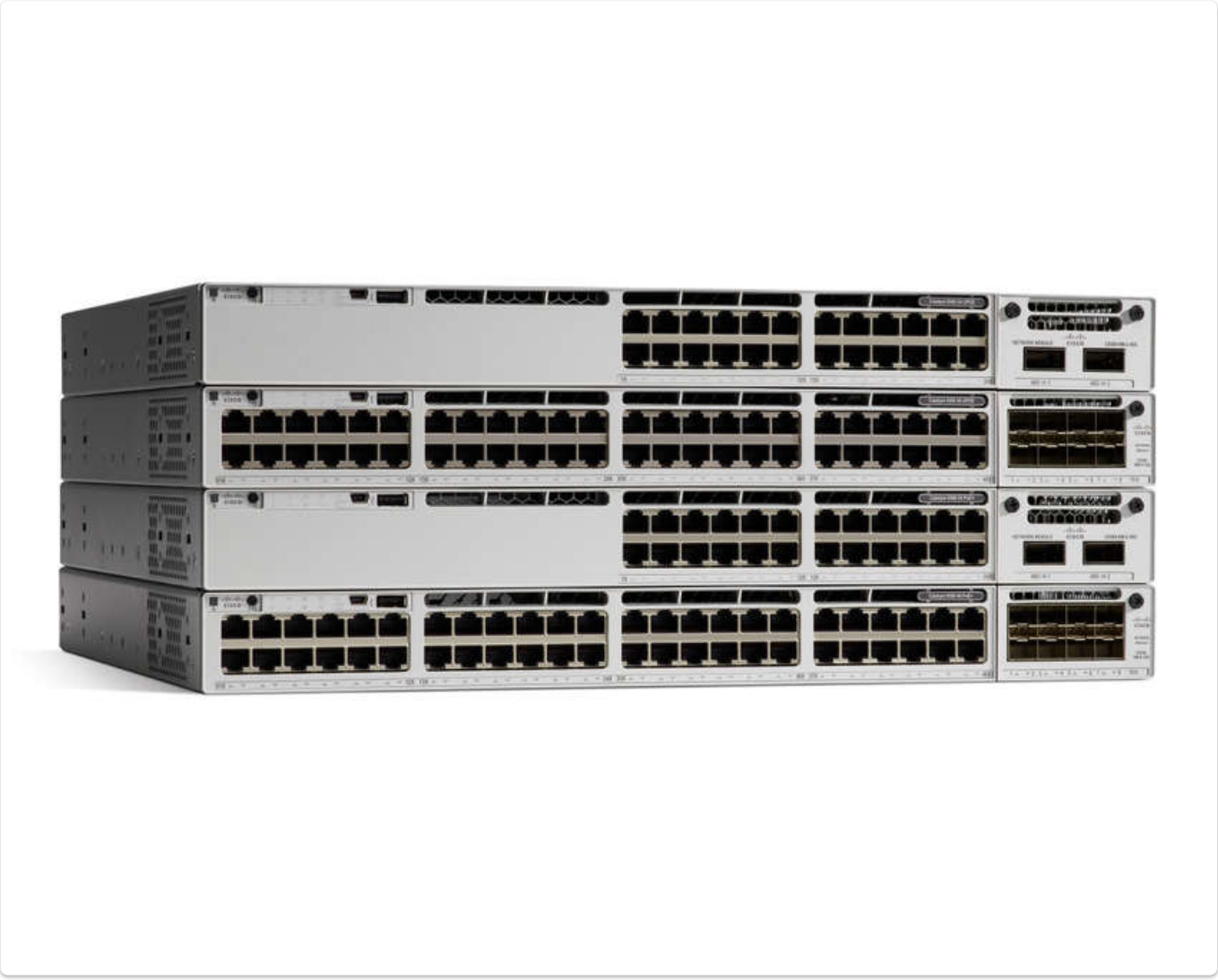
IP addresses contain two parts. One part identifies the network portion. The network portion of the IP address will be the same for all hosts connected to the same local network. The second part of the IP address identifies the individual host on that network. Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchical network.

The Network and Sharing Center on a PC shows your basic network information and set up connections, including your active networks and whether you are connected wired or wirelessly to the internet and within your LAN. You can view the properties of your connections here.

On an Ethernet network, the host MAC address is similar to a person's name. A MAC address indicates the individual identity of a specific host, but it does not indicate where on the network the host is located. If all hosts on the internet (millions and millions of them) were each identified by their unique MAC address only, imagine how difficult it would be to locate a single one. It is better to divide larger networks into smaller, more manageable pieces. One way to divide larger networks is to use a hierarchical design model.

Cisco 2960-XR

Hierarchical networks scale well. The access layer provides a connection point for end user devices to the network and allows multiple hosts to connect to other hosts through a network device, usually a switch or a wireless access point. Typically, all devices within a single access layer will have the same network portion of the IP address.



Cisco C9300 Series

The distribution layer provides a connection point for separate networks and controls the flow of information between the networks. Distribution layer devices control the type and amount of traffic that flows from the access layer to the core layer.

Cisco Catalyst 9600

The core layer is a high-speed backbone layer with redundant connections. It is responsible for transporting large amounts of data between multiple end networks. The main goal of the core layer is to transport data quickly.

2. Cloud and Virtualization

Cloud and Cloud Services

In general, when talking about the cloud, we are talking about data centers, cloud computing, and virtualization. Data centers are usually large facilities which provide massive amounts of power, cooling, and bandwidth. Only very large companies can afford their own data centers. Most smaller organizations lease the services from a cloud provider.
Cloud services include the following:

- SaaS – Software as a service
- PaaS – Platform as a service

- IaaS – Infrastructure as a service
  There are four primary cloud models, as shown in the figure.
- Public clouds - Cloud-based applications and services offered in a public cloud are made available to the general population.
- Private clouds - Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government.
- Hybrid clouds - A hybrid cloud is made up of two or more clouds, where each part remains a separate object, but both are connected using a single architecture.
- Community clouds - A community cloud is created for exclusive use by a specific community. The differences between public clouds and community clouds are the functional needs that have been customized for the community.

Virtualization is the foundation of cloud computing. Without it, cloud computing, as it is most-widely implemented, would not be possible. Virtualization means creating a virtual rather than physical version of something, such as a computer. An example would be running a "Linux computer" on your Windows PC.

Virtualization

One major advantage of virtualization is overall reduced cost:

- Less equipment is required - Virtualization enables server consolidation, which requires fewer physical devices and lowers maintenance costs.
- Less energy is consumed - Consolidating servers lowers the monthly power and cooling costs.
- Less space is required - Server consolidation reduces the amount of required floor space.

These are additional benefits of virtualization:

- Easier prototyping - Self-contained labs, operating on isolated networks, can be rapidly created for testing and prototyping network deployments.
- Faster server provisioning - Creating a virtual server is far faster than provisioning a physical server.
- Increased server uptime - Most server virtualization platforms now offer advanced redundant fault tolerance features.
- Improved disaster recovery - Most enterprise server virtualization platforms have software that can help test and automate failover before a disaster happens.
- Legacy support - Virtualization can extend the life of OSs and applications providing more time for organizations to migrate to newer solutions.

The hypervisor is a program, firmware, or hardware that adds an abstraction layer on top of the physical hardware. The abstraction layer is used to create virtual machines which have access to all the hardware of the physical machine such as CPUs, memory, disk controllers, and NICs. Each of these virtual machines runs a complete and separate operating system.

Type 1 hypervisors are also called the "bare metal" approach because the hypervisor is installed directly on the hardware. Type 1 hypervisors are usually used on enterprise servers and data center networking devices.

A Type 2 hypervisor is software that creates and runs VM instances. The computer, on which a hypervisor is supporting one or more VMs, is a host machine. Type 2 hypervisors are also called hosted hypervisors. This is because the hypervisor is installed on top of the existing OS, such as macOS, Windows, or Linux. Then, one or more additional OS instances are installed on top of the hypervisor. A big advantage of Type 2 hypervisors is that management console software is not required.

3. Number Systems

Binary Number Systems

Binary is a numbering system that consists of the digits 0 and 1 called bits. In contrast, the decimal numbering system consists of 10 digits consisting of the digits 0 – 9. Hosts, servers, and network devices use binary addressing. Specifically, they use binary IPv4 addresses. For ease of use by people, IPv4 addresses are commonly expressed in dotted decimal notation.

This decimal system uses the powers of ten, or base 10. For example, the number 2,146 has a 2 in the thousands place, or two thousand. 2,146 has a 1 in the hundreds place, or one hundred. It has a 4 in the tens place, or forty. It has a 6 in the ones place, or six.

The binary system is a base 2 number system. Each place value can have a 0 or a 1. A useful tool is the binary positional value table. It is common to use a table with eight placeholders. 8 bits equal a byte.

Hexadecimal Number System

The hexadecimal numbering system is used in networking to represent IP Version 6 addresses and Ethernet MAC addresses. This base sixteen number system uses the digits 0 to 9 and the letters A to F. Binary and hexadecimal work well together because it is easier to express a value as a single hexadecimal digit than as four binary bits.

IPv6 addresses are 128 bits in length and every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

4. Ethernet Switching

Ethernet

There is no official local area networking standard protocol, but over time, one technology, Ethernet, has become more common than the others. Ethernet protocols define how data is formatted and how it is transmitted over the wired network. The Ethernet standards specify protocols that operate at Layer

1 and Layer 2 of the OSI model. Ethernet has become a de facto standard, which means that it is the technology used by almost all wired local area networks.

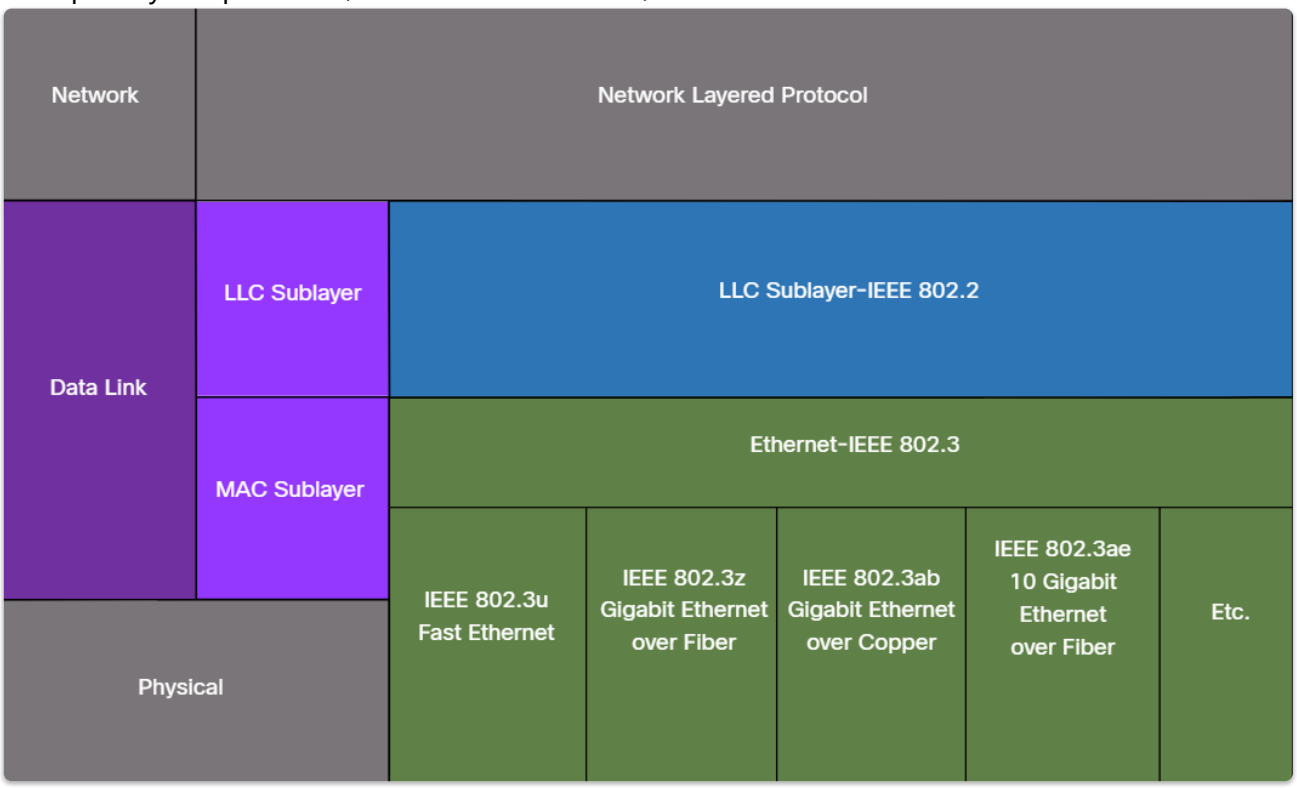
IEEE maintains the networking standards, including Ethernet and wireless standards. Each technology standard is assigned a number that refers to the committee that is responsible for approving and maintaining the standard. The 802.3 Ethernet standard has improved over time.

Ethernet switches can send a frame out all ports (excluding the port it was received from). Each host that receives this frame examines the destination MAC address and compares it to their MAC address. It is the Ethernet NIC card that examines and compares the MAC address. If it does not match the host MAC address, the rest of the frame is ignored. When it is a match, that host receives the rest of the frame and the message it contains.

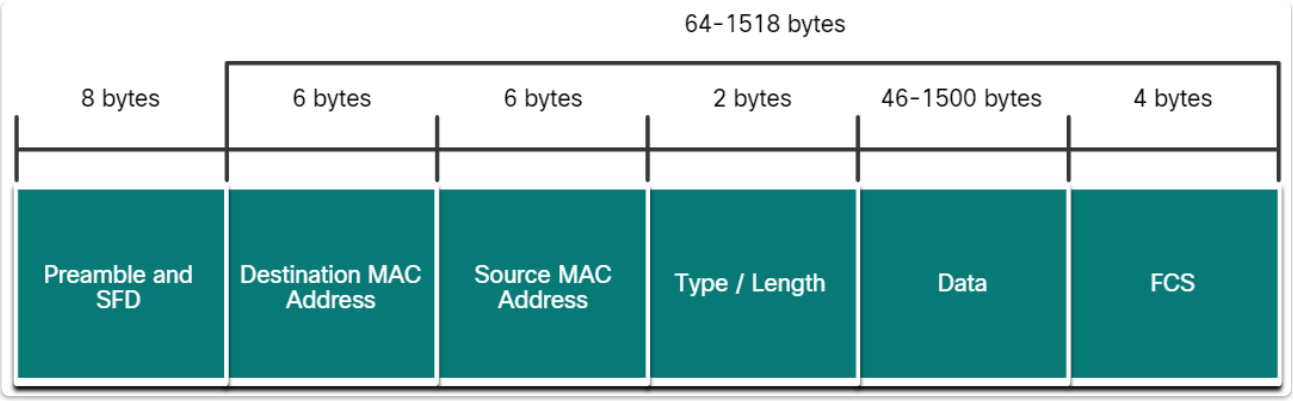
Ethernet Frames

Ethernet is defined by data link layer 802.2 and 802.3 protocols. Ethernet supports data bandwidths from 10 Mbps up to 100 Gps. EEE 802 LAN/MAN protocols, including Ethernet, use two separate sublayers of the data link layer to operate: LLC and MAC.

- LLC Sublayer - This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to use the same network interface and media.



- MAC Sublayer - This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware and is responsible for data encapsulation and media access control. It provides data link layer addressing and is integrated with various physical layer technologies. Data encapsulation includes the Ethernet frame, Ethernet Addressing, and Ethernet error detection.



Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD. The minimum Ethernet frame size is 64 bytes and the expected maximum is 1518 bytes. The fields are Preamble and Start Frame Delimiter, Destination MAC address, Source MAC address, Type / Length, Data, and FCS. This includes all bytes from the destination MAC address field through the FCS field.

Ethernet MAC Address

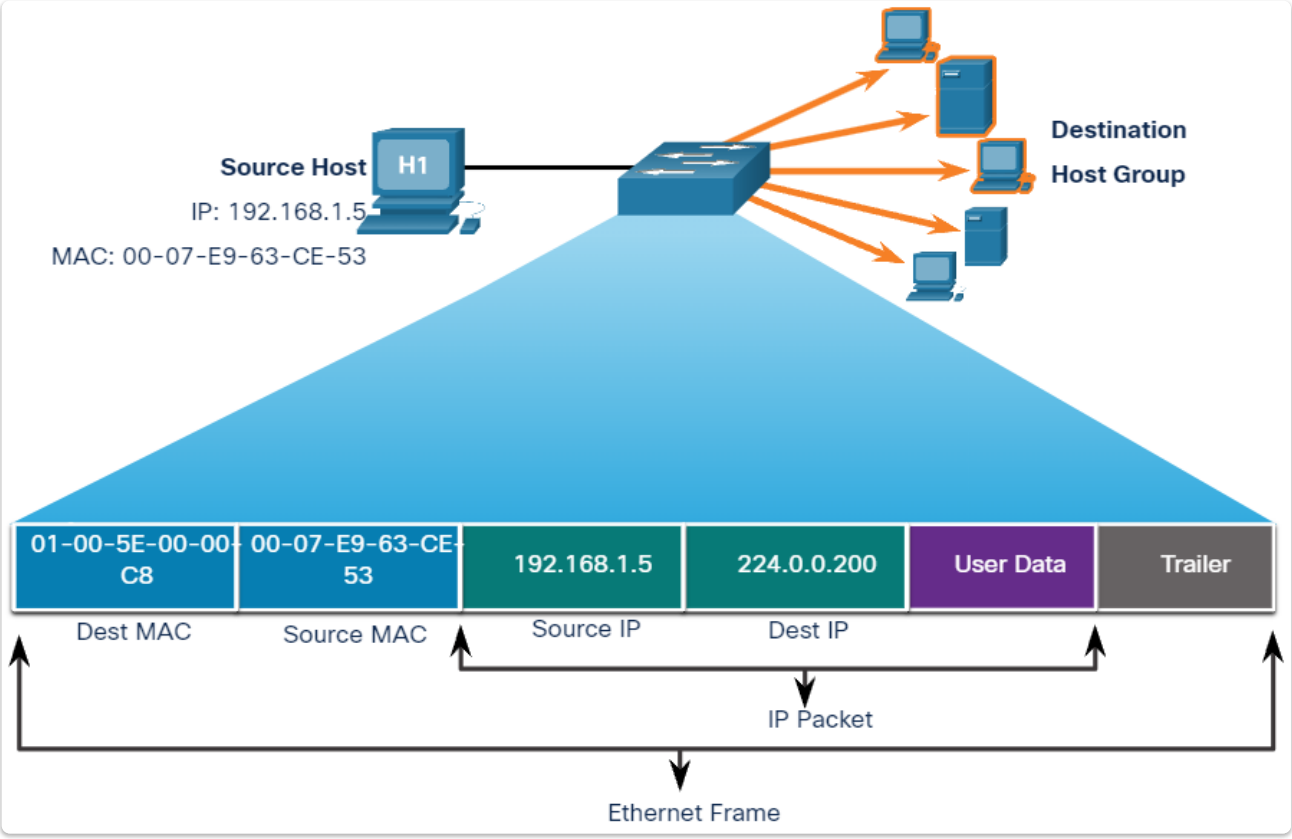
An Ethernet MAC address consists of a 48-bit binary value. Hexadecimal is used to identify an Ethernet address because a single hexadecimal digit represents four binary bits. Therefore, a 48-bit Ethernet MAC address can be expressed using only 12 hexadecimal values.

A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device. The process that a source host uses to determine the destination MAC address associated with an IPv4 address is ARP. The process that a source host uses to determine the destination MAC address associated with an IPv6 address is ND.

The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port.

- It is not forwarded by a router.



The features of an Ethernet multicast are as follows:

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as STP and LLDP.
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping.
- It is not forwarded by a router, unless the router is configured to route multicast packets.

The MAC Address Table

A Layer 2 Ethernet switch uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame. An Ethernet switch examines its MAC address table to make a forwarding decision for each frame. The MAC address table is sometimes referred to as a CAM table.

The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port. The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table. If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry in its MAC address table. If the destination MAC address is in the table, it will forward the frame out the specified port. If the destination MAC address is not in the table, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame. When the MAC address table of the switch contains the destination MAC address, it is able to filter the frame and forward out a single port. A switch can have multiple MAC addresses associated with a single port. This is common when the switch is connected to another switch. The switch will have a separate MAC address table entry for each frame received with a different source MAC address. When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device. Instead, the Ethernet frame is sent to the MAC address of the default gateway, the router.

5. Network Layer

Network Layer Characteristics

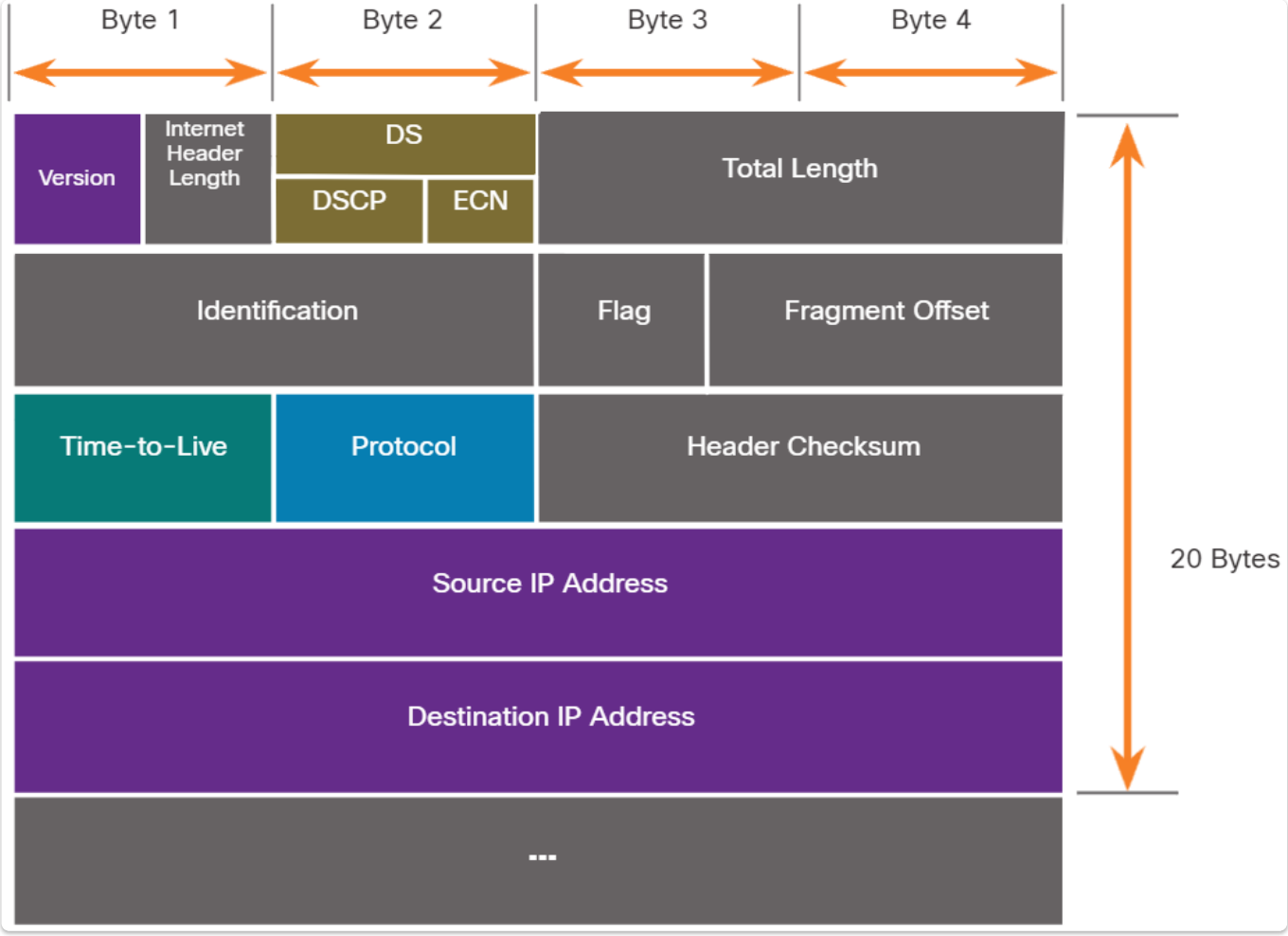
The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principal network layer communication protocols. Other network layer protocols include routing protocols such as OSPF and messaging protocols such as ICMP.

Network layer protocols perform four operations: addressing end devices, encapsulation, routing, and de-encapsulation. IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

IP encapsulates the transport layer segment or other data by adding an IP header. The IP header is used to deliver the packet to the destination host. The IP header is examined by routers and Layer 3 switches as it travels across a network to its destination. IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing NAT for IPv4.

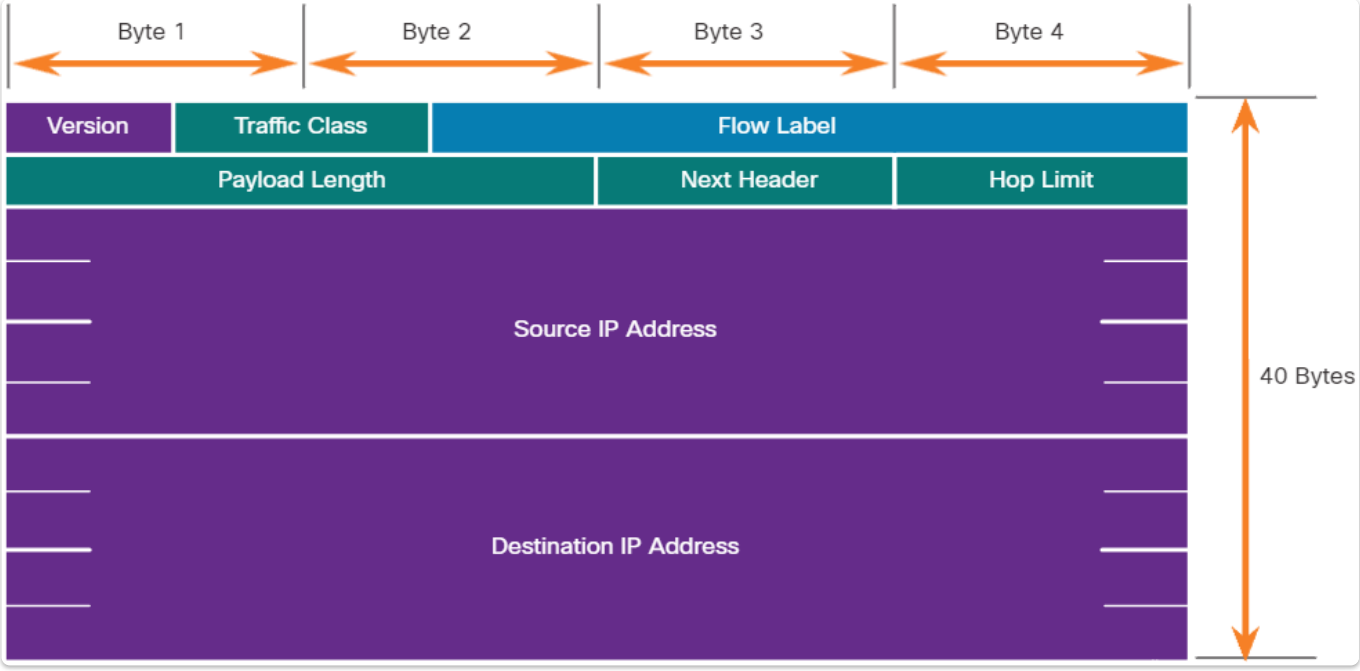
The basic characteristics of IP are that it is: **connectionless, best effort, and media independent.** IP is **connectionless**, meaning that **no dedicated end-to-end connection is created by IP before data is sent.** IP does not require additional fields in the header to maintain an established connection. This reduces the overhead of IP. **Senders are unaware whether destination devices are present and functional when sending packets, nor are they aware if the destination receives the packet, or if the destination device is able to access and read the packet.** IP operates **independently of the media** that carry the data at lower layers of the protocol stack. IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals. One characteristic of the media that the network layer considers is the maximum size of the PDU that each medium can transport, or the MTU.

IPv4



The IPv4 packet header is used to ensure that a packet is delivered to its next stop on the way to its destination end device. An IPv4 packet header consists of fields containing binary numbers which are examined by the Layer 3 process. Significant fields in the IPv4 header include: version, DS, TTL, protocol, header checksum, source IPv4 address, and destination IPv4 address.
The IHL, Total Length, and Header Checksum fields are used to identify and validate the packet. The IPv4 packet uses Identification, Flags, and Fragment Offset fields to keep track of the fragments. A router may have to fragment an IPv4 packet when forwarding it from one medium to another with a smaller MTU.

IPv6



IPv4 has limitations, including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 overcomes the limitations of IPv4. Improvements that IPv6 provides include the following: increased address space, improved packet handling, and it eliminates the need for NAT.

The 32-bit IPv4 address space provides approximately 4,294,967,296 unique addresses. IPv6 address space provides 340,282,366,920,938,463,463,374,607,431,768,211,456, or 340 undecillion addresses. This is roughly equivalent to every grain of sand on Earth.

The IPv6 simplified header fields include: version, traffic class, flow label, payload length, next header, hop limit, source IP address, and destination IP address. An IPv6 packet may also contain EH, which provide optional network layer information. Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility and more. Unlike IPv4, routers do not fragment routed IPv6 packets.

6. IPv4 Address Sructure

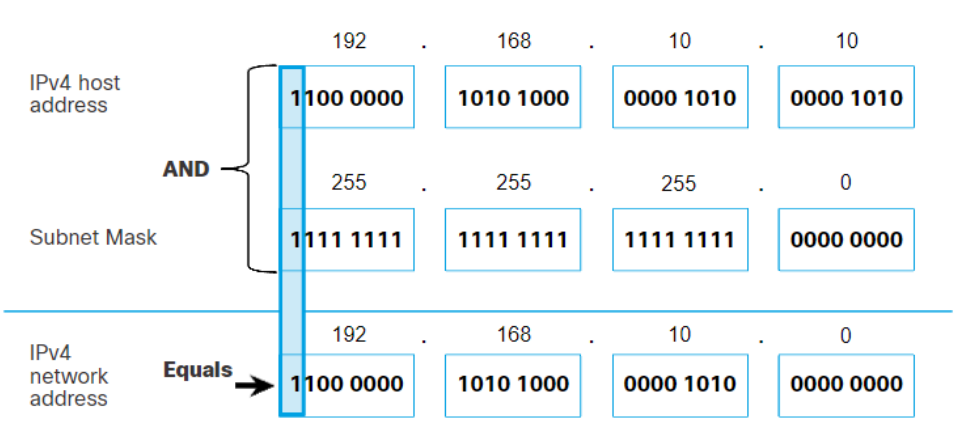
An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. When determining the network portion versus the host portion, you must look at the 32-bit stream. The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network. If two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

The IPv4 subnet mask is used to differentiate the network portion from the host portion of an IPv4 address. When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device. The network address represents all the devices on the same network.

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

An alternative method of identifying a subnet mask, a method called the prefix length. The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits set to 1. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24.

- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



The AND operation is used in determining the network address. Logical AND is the comparison of two bits. Note how only a 1 AND 1 produces a 1. Any other combination results in a 0.

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

- 0 AND 0 = 0
  To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask. ANDing between the address and the subnet mask yields the network address.

7. Address Resolution

ARP
To send a packet to another host on the same local IPv4 network, a host must know the IPv4 address and the MAC address of the destination device. Device destination IPv4 addresses are either known or resolved by device name. However, MAC addresses must be discovered. A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address. ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.

The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

- If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network than the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway.

Each entry, or row, of the ARP table binds an IPv4 address with a MAC address. We call the relationship between the two values a map. ARP messages are encapsulated directly within an Ethernet frame. There is no IPv4 header. The ARP request is encapsulated in an Ethernet frame using the following header information:

- Destination MAC address – This is a broadcast address FF-FF-FF-FF-FF-FF requiring all Ethernet NICs on the LAN to accept and process the ARP request.
- Source MAC address – This is MAC address of the sender of the ARP request.
- Type - ARP messages have a type field of 0x806. This informs the receiving NIC that the data portion of the frame needs to be passed to the ARP process.
  Because ARP requests are broadcasts, they are flooded out all ports by the switch, except the receiving port. Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply. After the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table.

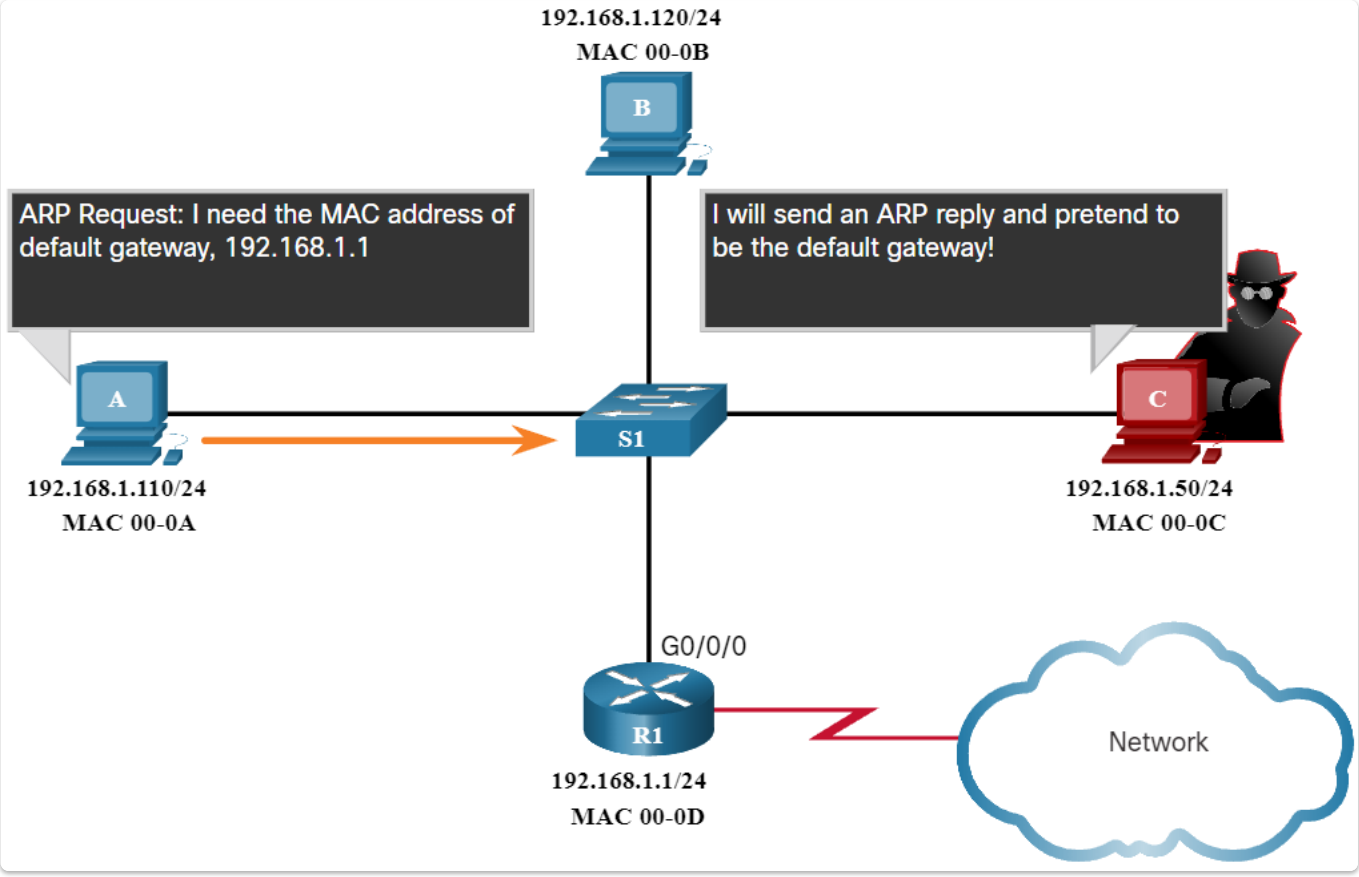
When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway. This is the interface of the local router. Whenever a source device has a packet with an IPv4 address on another network, it will encapsulate that packet in a frame using the destination MAC address of the router. The IPv4 address of the default gateway is stored in the IPv4 configuration of the hosts. If the destination host is not on its same network, the source checks its ARP table for an entry with the IPv4 address of the default

gateway. If there is not an entry, it uses the ARP process to determine a MAC address of the default gateway.

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. The times differ depending on the operating system of the device. Commands may be used to manually remove some or all of the entries in the ARP table.

On a Cisco router, the show ip arp command is used to display the ARP table. On a Windows 10 PC, the arp –a command is used to display the ARP table.

As a broadcast frame, an ARP request is received and processed by every device on the local network. If a large number of devices were to be powered up and all start accessing network services at the same time, there could be some reduction in performance for a short period of time. In some cases, the use of ARP can lead to a potential security risk.



A threat actor can use ARP spoofing to perform an ARP poisoning attack. This is a technique used by a threat actor to reply to an ARP request for an IPv4 address that belongs to another device, such as the default gateway. The threat actor sends an ARP reply with its own MAC address. The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor.

8. IP addressing Services

IP Addressing Services

In data networks, devices are labeled with numeric IP addresses to send and receive data over

networks. Domain names were created to convert the numeric address into a simple, recognizable name. The DNS protocol defines an automated service that matches resource names with the required numeric network address. The DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.

The DNS server stores different types of resource records that are used to resolve names. These records contain the name, address, and type of record. DNS uses the same message format between servers, consisting of a question, answer, authority, and additional information for all types of client queries and server responses, error messages, and transfer of resource record information.

DNS uses domain names to form the hierarchy. The naming structure is broken down into zones. Each DNS server maintains a specific database file and is only responsible for managing name-to-IP mappings for that small portion of the entire DNS structure. When a DNS server receives a request for a name translation that is not within its DNS zone, the DNS server forwards the request to another DNS server within the proper zone for translation. DNS is scalable because hostname resolution is spread across multiple servers.

Computer operating systems have a utility called Nslookup that allows the user to manually query the name servers to resolve a given host name. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers. When the nslookup command is issued, the default DNS server configured for your host is displayed. The name of a host or domain can be entered at the nslookup prompt.

On larger networks, DHCP is preferred for address assignment. Rather than use static addressing for each connection, it is more efficient to have IPv4 addresses assigned automatically using DHCP. DHCP can allocate IP addresses for a configurable period of time, called a lease period. When the lease period expires or the DHCP server gets a DHCPRELEASE message, the address is returned to the DHCP pool for reuse. Users can freely move from location to location and easily re-establish network connections through DHCP.

DHCPv6 provides similar services for IPv6 clients. One important difference is that DHCPv6 does not provide a default gateway address. This can only be obtained dynamically from the Router Advertisement message of the router.
When an IPv4, DHCP-configured device boots up or connects to the network, the client broadcasts a DHCPDISCOVER message to identify any available DHCP servers on the network.

A DHCP server replies with a DHCPOFFER message, which offers a lease to the client. The client sends a DHCPREQUEST message that identifies the explicit server and lease offer that the client is accepting.

Assuming that the IPv4 address requested by the client, or offered by the server, is still available, the server returns a DHCPACK message that acknowledges to the client that the lease has been finalized. If the offer is no longer valid, then the selected server responds with a DHCPNAK message. If a DHCPNAK message is returned, then the selection process must begin again with a new DHCPDISCOVER message being transmitted.

DHCPv6 has a set of messages that is similar to those for DHCPv4. The DHCPv6 messages are SOLICIT, ADVERTISE, INFORMATION REQUEST, and REPLY.

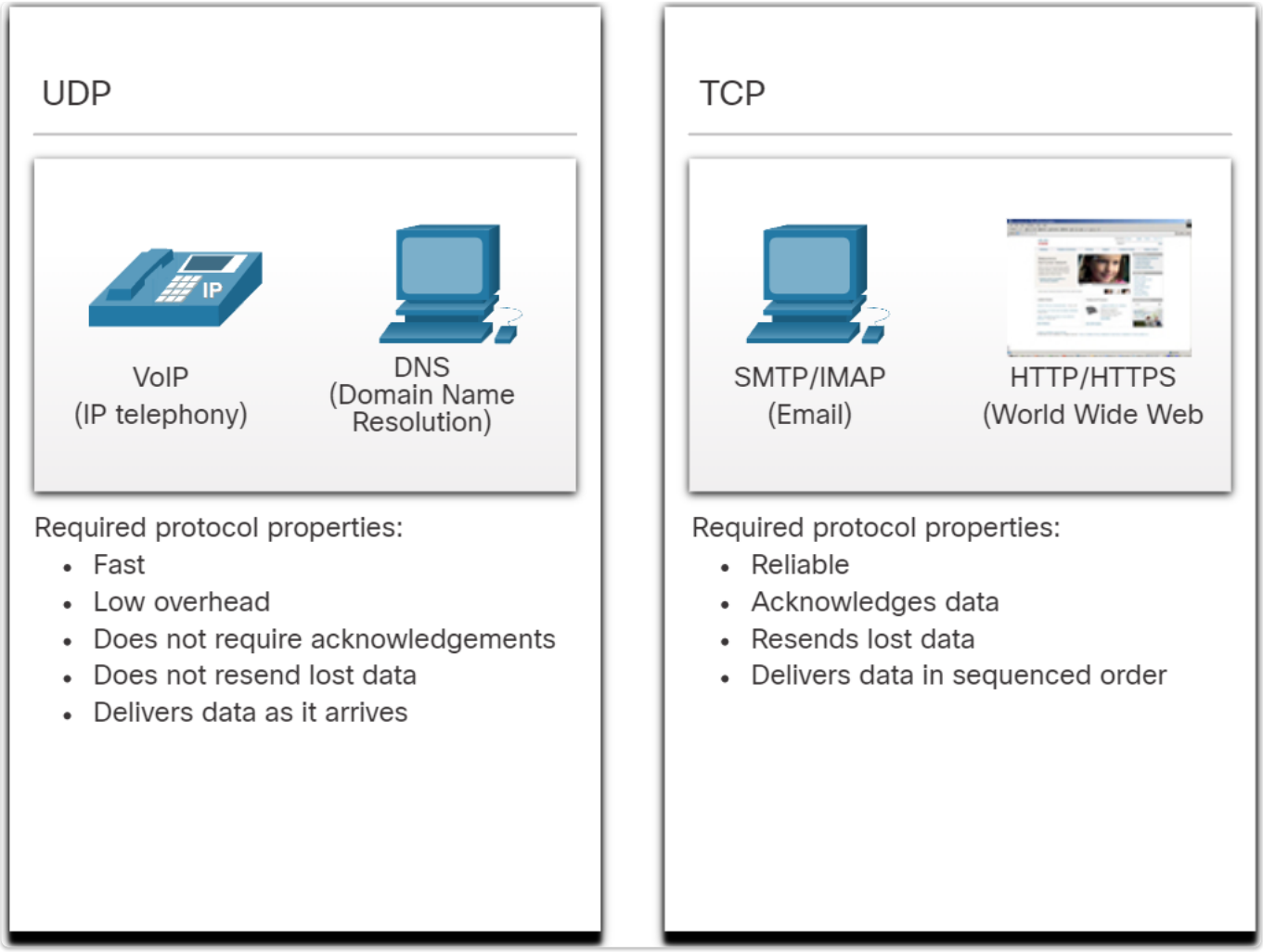
9. Transport Layer

Transport Layer

Application layer programs generate data that must be exchanged between source and destination hosts. The transport layer is responsible for logical communications between applications running on different hosts. The transport layer includes two protocols: Transmission Control Protocol TCP and User Datagram Protocol UDP.

- Tracking Individual Conversations - At the transport layer, each set of data flowing between a source application and a destination application is known as a conversation and is tracked separately. It is the responsibility of the transport layer to maintain and track these multiple conversations.
- Segmenting Data and Reassembling Segments - It is the transport layer responsibility to divide the application data into appropriately sized blocks. Depending on the transport layer protocol used, the transport layer blocks are called either segments or datagrams.
- Add Header Information - The transport layer protocol also adds header information containing binary data organized into several fields to each block of data.
- Identifying the Applications - The transport layer must be able to separate and manage multiple communications with different transport requirement needs.
- Conversation Multiplexing - Sending some types of data (e.g., a streaming video) across a network, as one complete communication stream, can consume all the available bandwidth. The transport layer uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network.

Transport layer protocols specify how to transfer messages between hosts, and are responsible for managing reliability requirements of a conversation. The transport layer includes the TCP and UDP protocols.



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
- 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
  In order to maintain the state of a conversation and track the information, TCP must first establish a connection between the sender and the receiver. This is why TCP is known as a connection-oriented protocol.
  UDP is a connectionless protocol. Because UDP does not provide reliability or flow control, it does not require an established connection. Because UDP does not track information sent or received between the client and server, UDP is also known as a stateless protocol. UDP is also known as a best-effort delivery protocol because there is no acknowledgment that the data is received at the destination. With UDP, there are no transport layer processes that inform the sender of a successful delivery. UDP is preferable for applications such as 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.

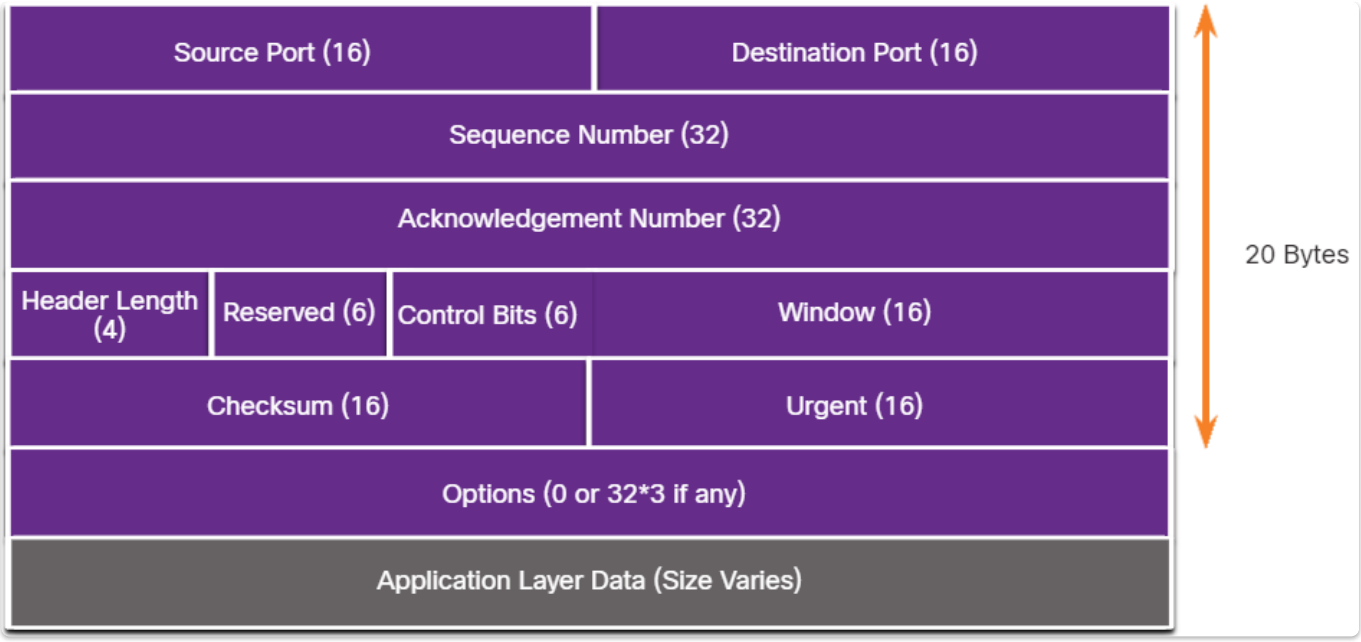
For other applications it is important that all the data arrives and that it can be processed in its proper sequence. For these types of applications, TCP is used as the transport protocol. For example, applications such as databases, web browsers, and email clients, require that all data that is sent arrives at the destination in its original condition. Any missing data could corrupt a communication, making it either incomplete or unreadable.

TCP Overview

In addition to supporting the basic functions of data segmentation and reassembly, TCP also provides the following services:

- Establishes a Session - TCP is a connection-oriented protocol that negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic. Through session establishment, the devices negotiate the amount of traffic that can be forwarded at a given time, and the communication data between the two can be closely managed.
- Ensures Reliable Delivery - For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network. TCP ensures that each segment that is sent by the source arrives at the destination.
- Provides Same-Order Delivery - Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order. By numbering and sequencing the segments, TCP ensures segments are reassembled into the proper order.
- Supports Flow Control - Network hosts have limited resources (i.e., memory and processing power). When TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow. This is done by TCP regulating the amount of data the source transmits. Flow control can prevent the need for retransmission of the data when the resources of the receiving host are overwhelmed.

TCP is a stateful protocol which means it keeps track of the state of the communication session. To track the state of a session, TCP records which information it has sent and which information has been acknowledged. The stateful session begins with the session establishment and ends with the session termination.



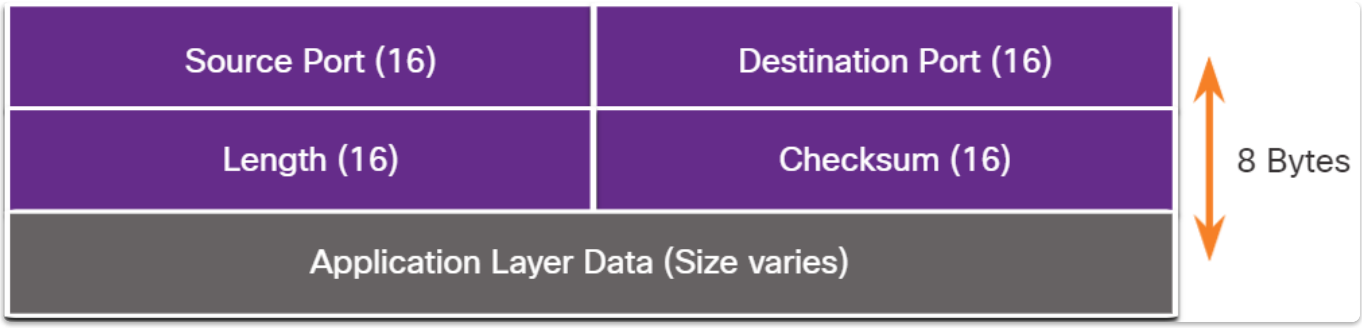
The ten fields in the TCP header are as follows:

- Source Port - A 16-bit field used to identify the source application by port number.
- Destination Port - A 16-bit field used to identify the destination application by port number.
- Sequence Number - A 32-bit field used for data reassembly purposes.
- Acknowledgment Number - A 32-bit field used to indicate that data has been received and the next byte expected from the source.
- Header Length - A 4-bit field known as "data offset" that indicates the length of the TCP segment header.
- Reserved - A 6-bit field that is reserved for future use.
- Control bits - A 6-bit field that includes bit codes, or flags, which indicate the purpose and function of the TCP segment.
- Window size - A 16-bit field used to indicate the number of bytes that can be accepted at one time.
- Checksum - A 16-bit field used for error checking of the segment header and data.
- Urgent -A 16-bit field used to indicate if the contained data is urgent.

TCP is a good example of how the different layers of the TCP/IP protocol suite have specific roles. TCP handles all tasks associated with dividing the data stream into segments, providing reliability, controlling data flow, and reordering segments. TCP frees the application from having to manage any of these tasks. HTTP, FTP, SMTP, and SSH, can simply send the data stream to the transport layer and use the services of TCP.

UDP Overview

UDP is a lightweight transport protocol that offers the same data segmentation and reassembly as TCP, but without TCP reliability and flow control.



UDP features include the following:

- Data is reconstructed in the order that it is received.
- Any segments that are lost are not resent.
- There is no session establishment.
- The sending is not informed about resource availability.

UDP is a stateless protocol, meaning neither the client, nor the server, tracks the state of the communication session. If reliability is required when using UDP as the transport protocol, it must be handled by the application.

The blocks of communication in UDP are called datagrams, or segments. These datagrams are sent as best effort by the transport layer protocol. The UDP header is far simpler than the TCP header because it only has four fields and requires 8 bytes (i.e., 64 bits).

The four fields in the UDP header are as follows:

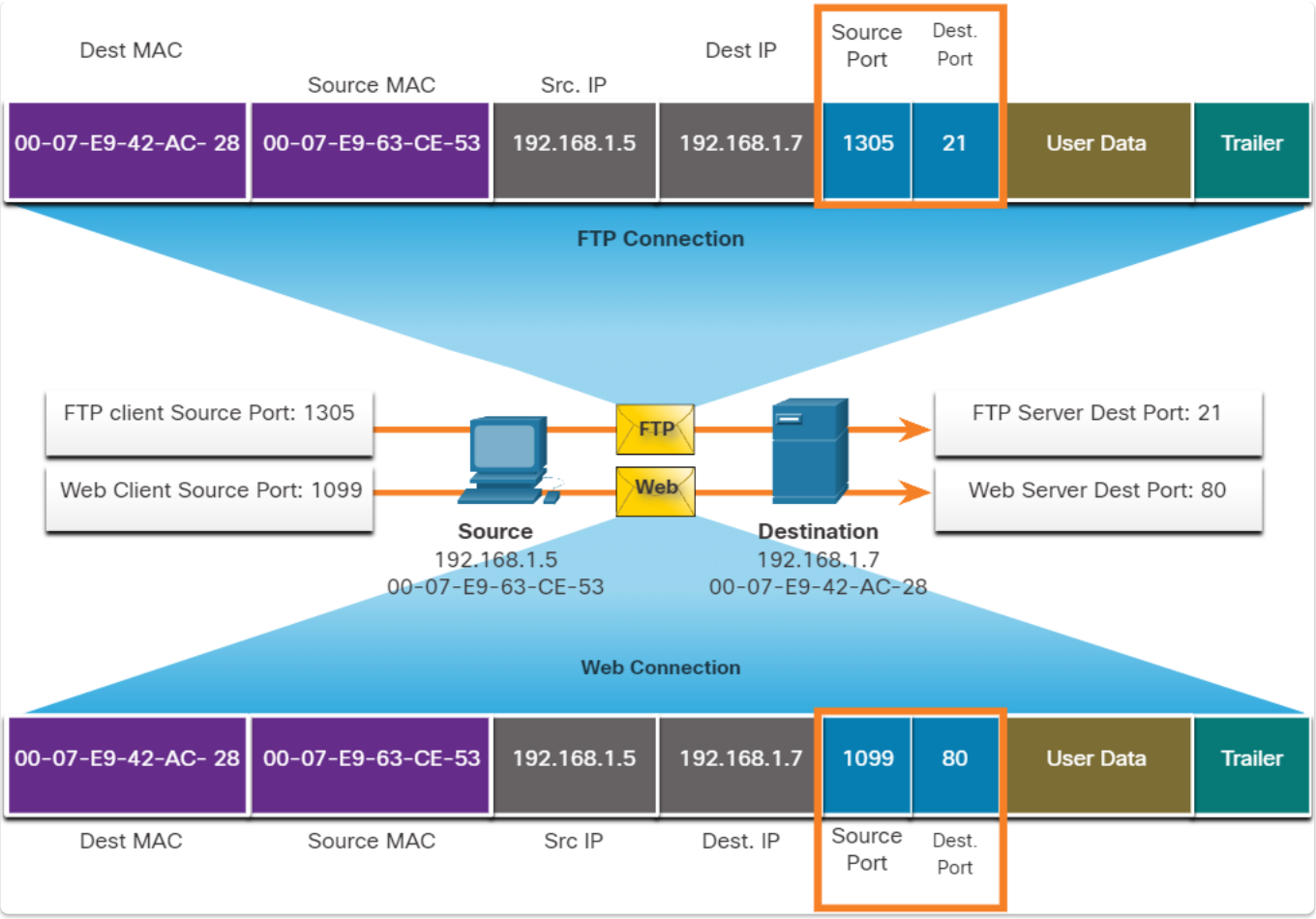
- Source Port - A 16-bit field used to identify the source application by port number.
- Destination Port - A 16-bit field used to identify the destination application by port number.
- Length - A 16-bit field that indicates the length of the UDP datagram header.
- Checksum - A 16-bit field used for error checking of the datagram header and data.

There are three types of applications that are best suited for UDP are live video and multimedia applications, simple request and reply applications, applications that handle reliability themselves.

Port Numbers

The TCP and UDP transport layer protocols use port numbers to manage multiple, simultaneous conversations. The TCP and UDP header fields identify a source and destination application port number. The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet. The IP packet contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket.



The socket is used to identify the server and service being requested by the client. A client socket might look like this, with 1099 representing the source port number: 192.168.1.5:1099. The socket on a web server might be 192.168.1.7:80. Together, these two sockets combine to form a socket pair: 192.168.1.5:1099, 192.168.1.7:80. Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.

The IANA is the standards organization responsible for assigning various addressing standards, including the 16-bit port numbers. The 16 bits used to identify the source and destination port numbers provides a range of ports from 0 through 65535.

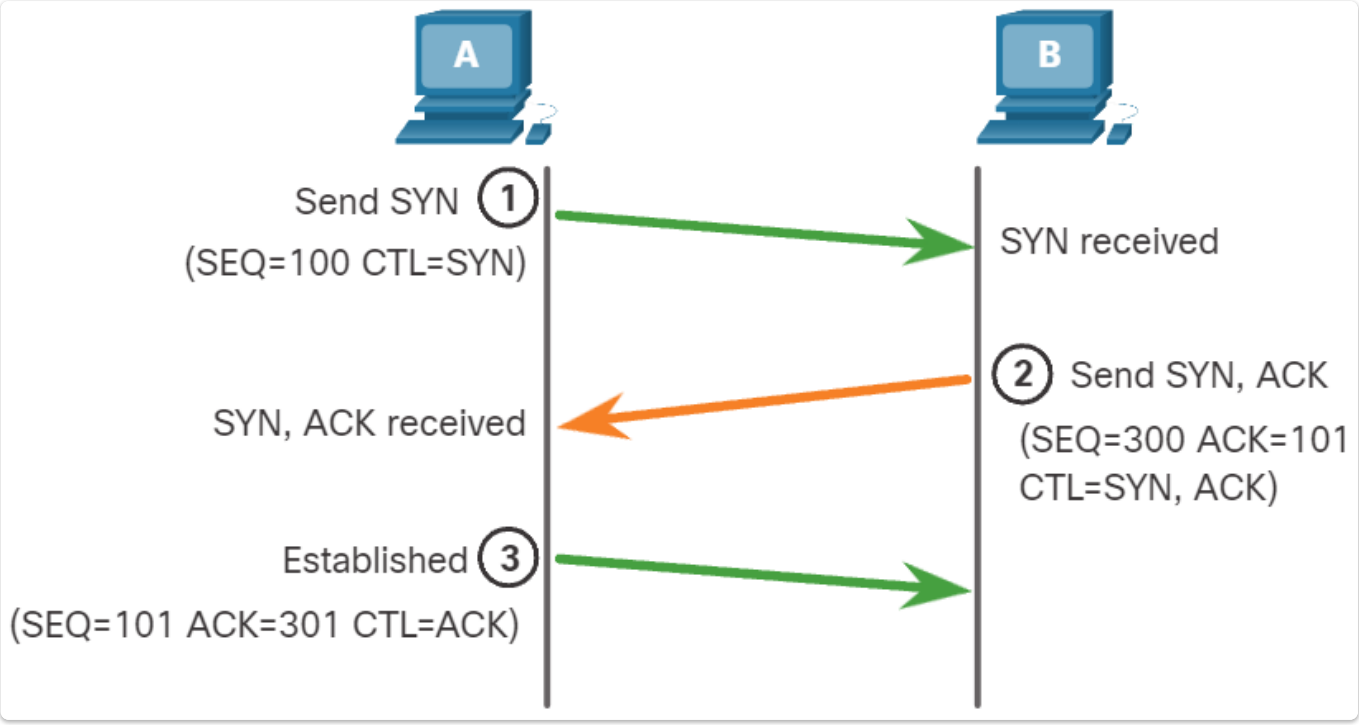
The IANA has divided the range of numbers into the following three port groups:

- Well-known Ports (0 to 1,023)
- Registered Ports (1,024 to 49,151)
- Private and/or Dynamic Ports (49,152 to 65,535)

Unexplained TCP connections can pose a major security threat. They can indicate that something or someone is connected to the local host. Netstat is an important network utility that can be used to verify those connections. Enter the command netstat to list the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state. By default, the netstat command will attempt to resolve IP addresses to domain names and port numbers to well-known applications.

TCP Communication Process

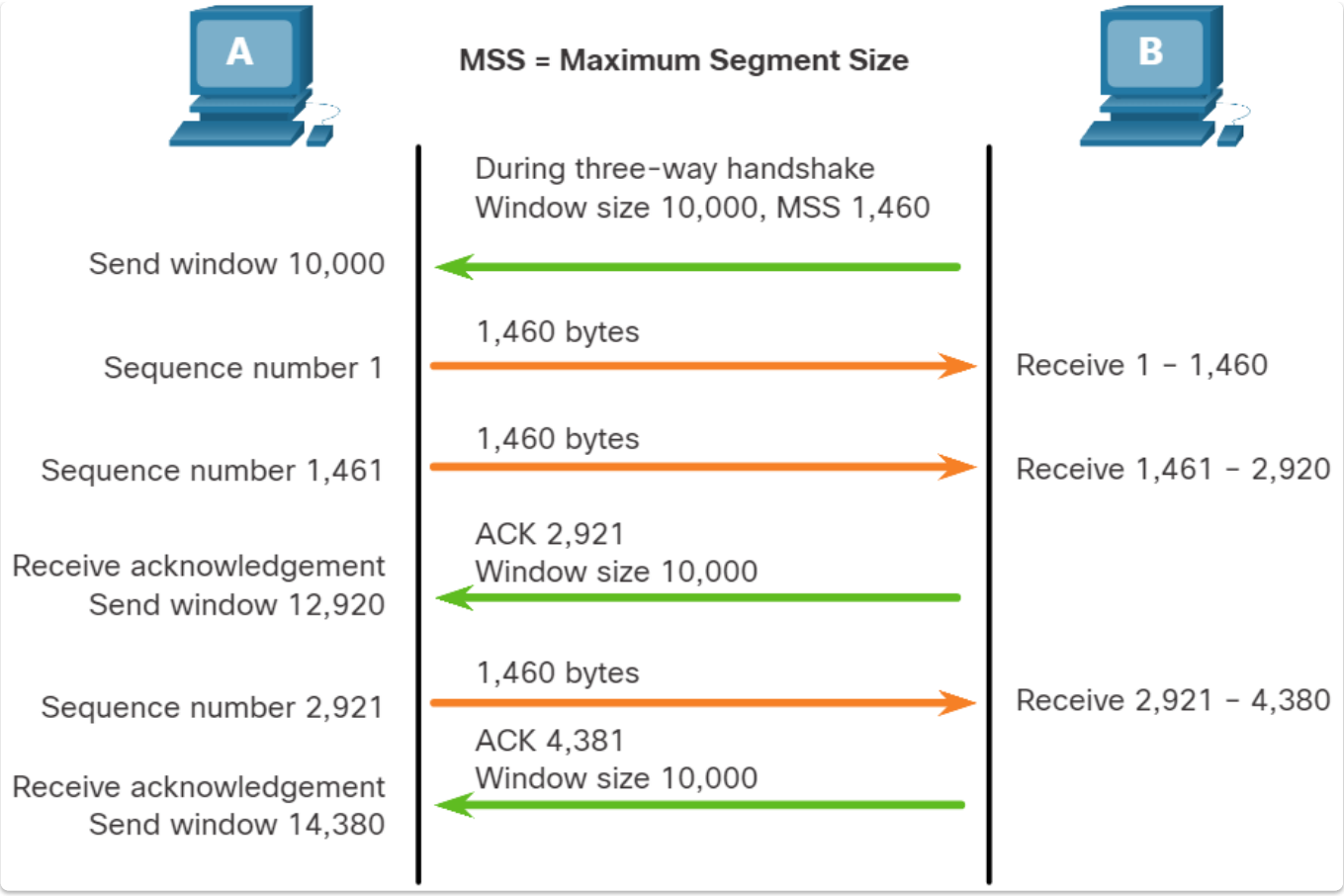
The reason that TCP is the better protocol for some applications is because, unlike UDP, it resends dropped packets and number of packets to indicate their proper order before delivery. TCP can also help maintain the flow of packets so that devices do not become overloaded.
Sequence numbers are assigned in the header of each packet to ensure all of the segments arrive in proper order to the destination. The sequence number represents the first data byte of the TCP segment. During session setup, an ISN is set. This ISN represents the starting value of the bytes that are transmitted to the receiving application. As data is transmitted during the session, the sequence number is incremented by the number of bytes that have been transmitted. This data byte tracking enables each segment to be uniquely identified and acknowledged. Missing segments can then be identified.



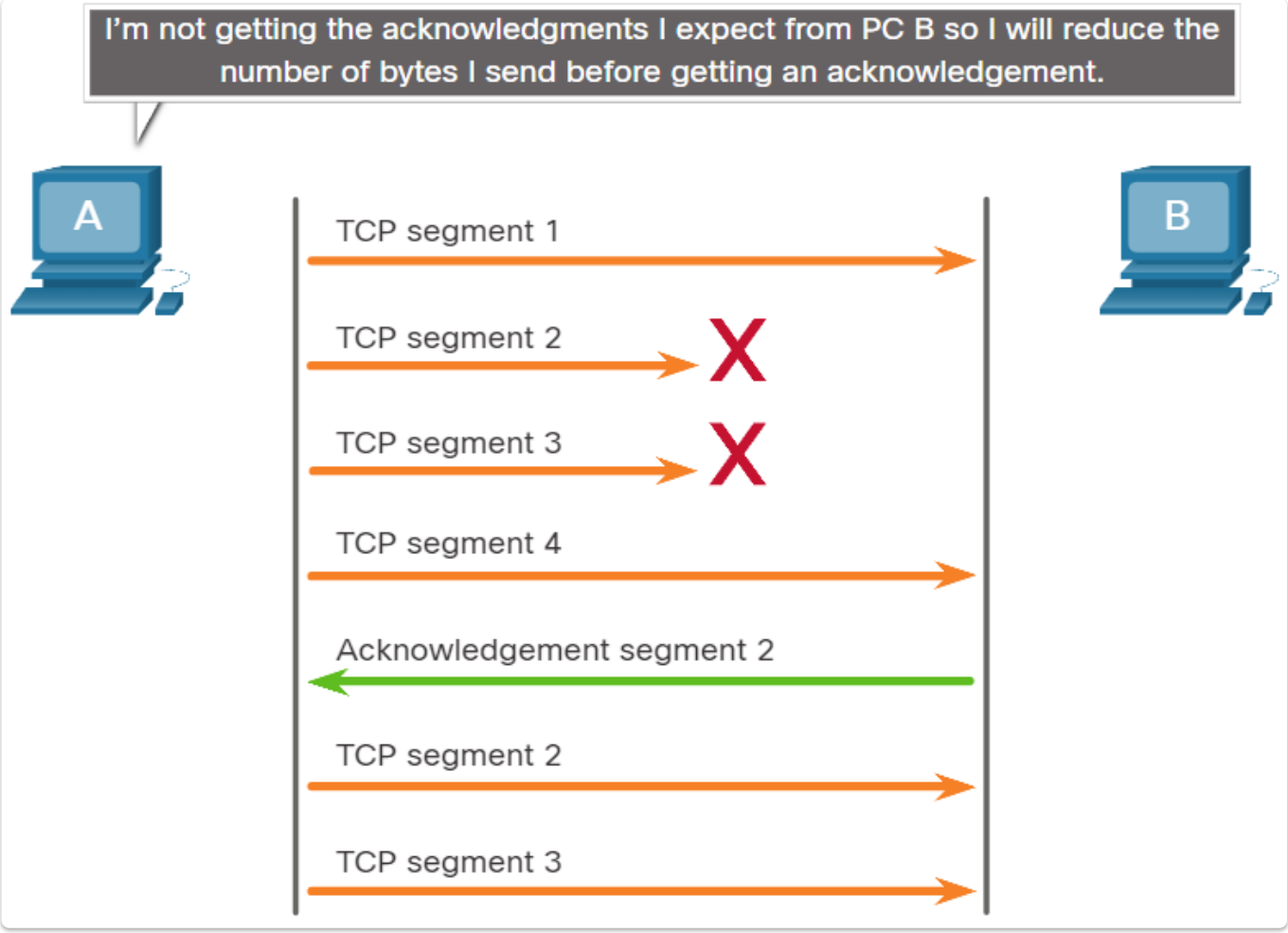
The SEQ number and ACK number are used together to confirm receipt of the bytes of data contained in the transmitted segments. The SEQ number identifies the first byte of data in the segment being transmitted. TCP uses the ACK number sent back to the source to indicate the next byte that the receiver expects to receive. This is called expectational acknowledgement.

TCP also provides mechanisms for flow control. Flow control is the amount of data that the destination can receive and process reliably. Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session. To accomplish this, the TCP header includes a 16-bit field called the window size.

The window size determines the number of bytes that can be sent before expecting an acknowledgment. The acknowledgment number is the number of the next expected byte. The initial window size is agreed upon when the TCP session is established during the three-way handshake. The source device must limit the number of bytes sent to the destination device based on the window size of the destination. Only after the source device receives an acknowledgment that the bytes have been received, can it continue sending more data for the session.



The MSS is part of the options field in the TCP header that specifies the largest amount of data, in bytes, that a device can receive in a single TCP segment. The MSS size does not include the TCP header. The MSS is typically included during the three-way handshake.



Whenever there is congestion, retransmission of lost TCP segments from the source will occur. If the retransmission is not properly controlled, the additional retransmission of the TCP segments can make the congestion even worse. To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.

UDP Communications

UDP does not establish a connection. UDP provides low overhead data transport because it has a small datagram header and no network management traffic.

Like segments with TCP, when UDP datagrams are sent to a destination, they often take different paths and arrive in the wrong order. UDP does not track sequence numbers the way TCP does. Therefore, UDP simply reassembles the data in the order that it was received and forwards it to the application.

Like TCP-based applications, UDP-based server applications are assigned well-known or registered port numbers. When these applications or processes are running on a server, they accept the data matched with the assigned port number. When UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number.

After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction. For the data returning to the client from the server, the

source and destination port numbers in the datagram header are reversed.

10. The Cisco IOS Command Line

Navigate the IOS

The Cisco IOS CLI is a text-based program that enables entering and executing Cisco IOS commands to configure, monitor, and maintain Cisco devices. The Cisco CLI can be used with either in-band or out-of-band management tasks.

CLI commands are used to alter the configuration of the device and to display the current status of processes on the router. When the router has completed the power-up sequence and the Router> prompt appears, the CLI can be used to enter Cisco IOS commands.

As a security feature, the Cisco IOS software separates management access into the following two command modes:

```
Router con0 is now available


Press RETURN to get started!



Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)#
```

- User EXEC Mode - This mode is useful for basic operations. It allows a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the > symbol.
- Privileged EXEC Mode - To execute configuration commands, a network administrator must access privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. Global configuration mode is identified by the CLI prompt that ends with (config)#.

The commands used to navigate between the different IOS command modes are:

- enable

- disable
- configure terminal
- exit
- end
- Ctrl+Z
- line console 0
- line vty 0 15
- interface vlan 1

Hotkeys and Shortcuts

CLI console	
Ctrl+T	Swap the current character with the one before it
Ctrl+K	Erase all characters from the current cursor position to the end of the line
Ctrl+X	Erase all characters from the current cursor position to the beginning of the line
Ctrl+L	Reprint the line
Ctrl+C	Exit configuration mode
Ctrl+A	Moves the cursor to the beginning of the current line
Ctrl+E	Moves the cursor to the end of the current line
Ctrl+F	Moves forward one character
Ctrl+B	Moves backwards one character
Ctrl+R	Redisplays a line (starts a new line, with the same command shown)
Ctrl+U	Erases a line
Ctrl+W	Erases a word
Ctrl+Z	Exits configuration mode, returning you to privileged EXEC mode
Ctrl+P (or up arrow)	Displays the last command entered
Ctrl+N (or down arrow)	Displays previous commands entered
Tab	Completes a partial command
Esc, F	Moves forward one word
Esc, B	Moves backwards one word
Ctrl+D	Erase one character in current position
Control keys: While pressing <Ctrl> key then press needed button. Escape sequences: Press and release <Esc> key then press needed button.	

-----More----- block	
Enter	Shows next string
Space	Shows next page
Any another key	Jump to EXEC screen

Break operation combinations	
Ctrl+C	In configuration mode closing it and jumps to privilege EXEC mode. In setup mode stops it and jump to command line hint.
Ctrl+Z	In configuration mode closing it and jumping to privilege EXEC mode.
Ctrl+Shift+6, x	Break current command / suspend telnet connections

Show Commands

Command	Used to
show running-config	Verify the current configuration and settings.
show interfaces	Verify the interface status and see if there are any error messages.
show ip interface	Verify the Layer 3 information of an interface.
show arp	Verify the list of known hosts on the local Ethernet LANs.
show ip route	Verify the Layer 3 routing information.
show protocols	Verify which protocols are operational.
show version	Verify the memory, interfaces, and licenses of the device.

11. Build a Small Cisco Network

Basic Switch Configuration

Elements to configure on a LAN switch include host name, management IP address information, passwords, and descriptive information. A management address enables you to reach the device through Telnet, SSH, or HTTP clients. The IP address information that must be configured on a switch includes the IP address, subnet mask, and default gateway. To secure a Cisco LAN switch, configure passwords on each of the various methods of access to the command line. Assign passwords to remote access methods, such as Telnet, SSH and the console connection. Also assign a password to the privileged mode in which configuration changes can be made.

To access the switch remotely, configure an IP address and a subnet mask on the SVI. Use the interface vlan 1 global configuration command. Assign an IPv4 address using the ip address *ip-address subnet-mask* interface configuration command. Finally, enable the virtual interface using the no shutdown interface configuration command. After the switch is configured with these commands, the switch has all the IPv4 elements ready for communication over the network.

Configuration Tasks

Before configuring a switch, review the following initial switch configuration tasks:
Configure the device name.

- hostname *name*
  Secure user EXEC mode.

- **line console 0**
- **password** *password*
- **login**
  Secure remote Telnet / SSH access.
- **line vty 0 15**
- **password** *password*
- **login**
  Secure privileged EXEC mode.
- **enable secret** *password*
  Secure all passwords in the config file.
- **service password-encryption**
  Provide legal notification.
- **banner motd** *delimiter message delimiter*
  Configure the management SVI.
- **interface vlan 1**
- **ip address** *ip-address subnet-mask*
- **no shutdown**
  Save the configuration.

- copy running-config startup-config

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.20 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Switch Virtual Interface Configuration

To access the switch remotely, an IP address and a subnet mask must be configured on the switch virtual interface (SVI). To configure an SVI on a switch, use the **interface vlan 1** global configuration command. Vlan 1 is not an actual physical interface but a virtual one. Next, assign an IPv4 address using the **ip address** *ip-address subnet-mask* interface configuration command. Finally, enable the virtual interface using the **no shutdown** interface configuration command.

After the switch is configured with these commands, the switch has all the IPv4 elements ready for communication over the local network.

Note: Similar to Windows hosts, switches configured with an IPv4 address will typically also need to have a default gateway assigned. This can be done using the **ip default-gateway** *ip-address* global configuration command. The *ip-address* parameter would be the IPv4 address of the local router on the network, as shown in the example. However, in this topic you will only be configuring a network

with switches and hosts. Routers will be configured later.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

Basic Router Configuration

The following tasks should be completed when configuring initial settings on a router.

Step 1. Configure the device name.

```
Router(config)# hostname hostname
```

Step 2. Secure privileged EXEC mode.

```
Router(config)# enable secret password
```

Step 3. Secure user EXEC mode.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

Step 4. Secure remote Telnet / SSH access.

```
Router(config-line)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet | none | all}
```

Step 5. Secure all passwords in the config file.

```
Router(config-line)# exit
Router(config)# service password-encryption
```

Step 6. Provide legal notification.

```
Router(config)# banner motd delimiter message delimiter
```

Step 7. Save the configuration.

```
Router(config)# copy running-config startup-config
```

Basic Router Configuration Example

In this example, router R1 will be configured with initial settings. To configure the device name for R1, use the following commands.

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

Note: Notice how the router prompt now displays the router host name.

All router access should be secured. Privileged EXEC mode provides the user with complete access to the device and its configuration, so you must secure it.

The following commands secure privileged EXEC mode and user EXEC mode, enable Telnet and SSH remote access, and encrypt all plaintext (i.e., user EXEC and vty line) passwords. It is very important to use a strong password when securing privileged EXEC mode because this mode allows access to the configuration of the device.

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

The legal notification warns users that the device should only be accessed by permitted users. Legal notification is configured as follows:

```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)#
```

If the router were to be configured with the previous commands and it accidently lost power, the router configuration would be lost. For this reason, it is important to save the configuration when changes are implemented. The following command saves the configuration to NVRAM:

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Secure the Devices

Secure Remote Access

There are multiple ways to access a device to perform configuration tasks. One of these ways is to use a PC attached to the console port on the device. This type of connection is frequently used for initial device configuration.

Setting a password for console connection access is done in global configuration mode. These commands prevent unauthorized users from accessing user mode from the console port.

```
Switch(config)# line console 0
Switch(config-line)# password password
Switch(config-line)# login
```

When the device is connected to the network, it can be accessed over the network connection using SSH or Telnet. SSH is the preferred method because it is more secure. When the device is accessed through the network, it is considered a vty connection. The password must be assigned to the vty port. The following configuration is used to enable SSH access to the switch.

```
Switch(config)# line vty 0 15
Switch(config-line)# password password
Switch(config-line)# transport input ssh
Switch(config-line)# login
```

An example configuration is shown in the command window.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)#
```

By default, many Cisco switches support up to 16 vty lines that are numbered 0 to 15. The number of vty lines supported on a Cisco router varies with the type of router and the IOS version. However, five is the most common number of vty lines configured on a router. These lines are numbered 0 to 4 by default, though additional lines can be configured. A password needs to be set for all available vty lines. The same password can be set for all connections.

To verify that the passwords are set correctly, use the show running-config command. These passwords are stored in the running-configuration in plaintext. It is possible to set encryption on all passwords stored within the router so that they are not easily read by unauthorized individuals. The global configuration command service password-encryption ensures that all passwords are encrypted.

With remote access secured on the switch, you can now configure SSH.

Enable SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

Step 1. Verify SSH support.

Use the **show ip ssh** command to verify that the switch supports SSH. If the switch is not running an IOS that supports cryptographic features, this command is unrecognized.

Step 2. Configure the IP domain.

Configure the IP domain name of the network using the **ip domain-name** *domain-name* global configuration mode command. In the example configuration below, the *domain-name* value is **cisco.com**.

Step 3. Generate RSA key pairs.

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the **ip ssh version 2** global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in the figure uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes more time to generate and to use.

Note: To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Step 4. Configure user authentication.

The SSH server can authenticate users locally or use an authentication server. To use the local authentication method, create a username and password pair with the **username** *username* **secret** *password* global configuration mode command. In the example, the user **admin** is assigned the password **ccna**.

Step 5. Configure the vty lines.

Enable the SSH protocol on the vty lines using the **transport input ssh** line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the **line vty** global configuration mode command and then the **login local** line configuration mode command to require local authentication for SSH connections from the local username database.

Step 6. Enable SSH version 2.

By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the **show ip ssh** output as supporting version 1.99. Version 1 has known vulnerabilities. For this reason, it is recommended to enable only version 2. Enable SSH version using the **ip ssh version 2** global

configuration command.

```
S1# show ip ssh
SSH Disabled - version 1.99
%Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Authentication timeout: 120 secs; Authentication retries: 3
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)# exit
S1#
```

Configure Default Gateway

If your local network has only one router, it will be the gateway router and all hosts and switches on your network must be configured with this information. If your local network has multiple routers, you must select one of them to be the default gateway router. The default gateway is only used when the host wants to send a packet to a device on another network. The default gateway address is generally the router interface address attached to the local network of the host. The IP address of the host device and the router interface address must be in the same network.

To connect to and manage a switch over a local IP network, it must have an SVI configured. The SVI is configured with an IPv4 address and subnet mask on the local LAN. The switch must also have a default gateway address configured to remotely manage the switch from another network. To configure an IPv4 default gateway on a switch, use the **ip default-gateway** *ip-address* global configuration command. The *ip-address* that is configured is the IPv4 address of the local router interface connected to the switch.

12. ICMP

ICMP Messages

Although IP is only a best-effort protocol, the TCP/IP suite does provide for error messages and informational messages when communicating with another IP device. These messages are sent using the services of ICMP. The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions, not to make IP reliable. ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides these same services for IPv6 but includes additional functionality.

An ICMP Echo Message can be used to test the reachability of a host on an IP network. The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply.

When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered.

An ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the TTL field of the packet was decremented to 0. If a router receives a packet and decrements the TTL field in the IPv4 packet to zero, it discards the packet and sends a Time Exceeded message to the source host.

ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired. The informational and error messages found in ICMPv6 are very similar to the control and error messages implemented by ICMPv4. However, ICMPv6 includes four new protocols as part of the ND or NDP, as follows:

- RS message
- RA message
- NS message
- NA message

Destination or Service Unreachable

When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered.

Some of the Destination Unreachable codes for ICMPv4 are as follows:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

Some of the Destination Unreachable codes for ICMPv6 are as follows:

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

Note: ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

Ping and Traceroute Tests

To test connectivity to another host on a network, an echo request is sent to the host address using the ping command. If the host at the specified address receives the echo request, it responds with an echo reply. As each echo reply is received, ping provides feedback on the time between when the request was sent and when the reply was received. This can be a measure of network performance. Ping has a timeout value for the reply. If a reply is not received within the timeout, ping provides a message indicating that a response was not received.

Type of connectivity tests performed with ping include the following:

- **Pinging the local loopback** - Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To perform this test, ping the local loopback address.
- **Pinging the default gateway** - This is generally done by pinging the IP address of the default gateway of the host. A successful ping to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- **Pinging the remote host** - A successful ping across the internetwork confirms communication on the local network, the operation of the router serving as the default gateway, and the operation of all other routers that might be in the path between the local network and the network of the remote host.

tracert is a utility that generates a list of hops that were successfully reached along the path. This list can provide important verification and troubleshooting information. If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts. If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.

The round-trip time is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost or unreplied packet. Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.