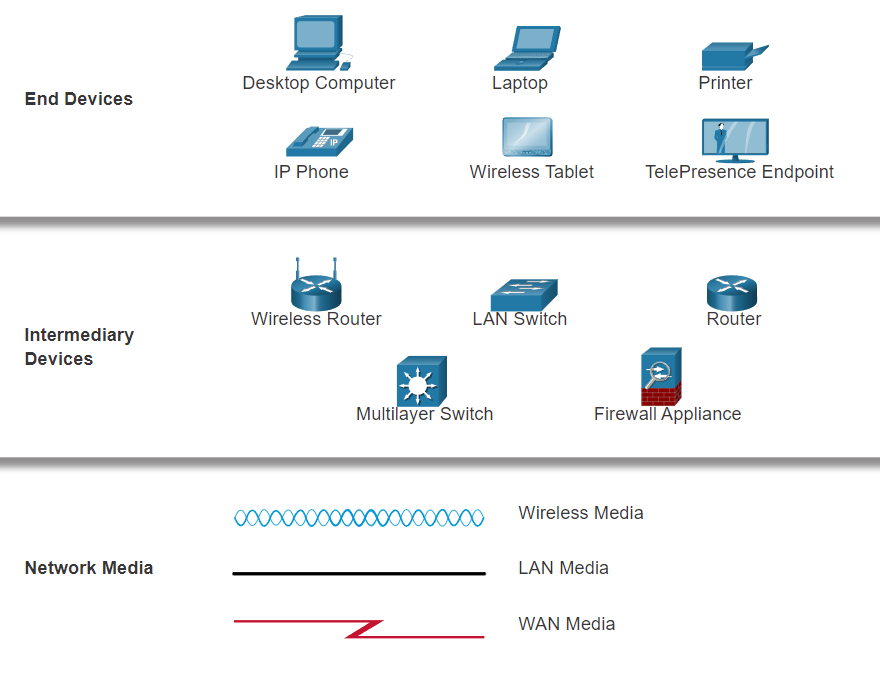
Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание



* **Network Interface Card (NIC)** - A NIC physically connects the end device to the network.
* **Physical Port** - A connector or outlet on a networking device where the media connects to an end device or another networking device.
* **Interface** - Specialized ports on a networking device that connect to individual networks. Because routers connect networks, the ports on a router are referred to as network interfaces.

Изображение выглядит как текст

Автоматически созданное описание

The two most common types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs). A LAN is a network infrastructure that provides access to users and end devices in a small geographical area. A LAN is typically used in a department within an enterprise, a home, or a small business network. A WAN is a network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a larger corporation or a telecommunications service provider. The figure shows LANs connected to a WAN.

A LAN is a network infrastructure that spans a small geographical area. LANs have specific characteristics:

* LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
* A LAN is usually administered by a single organization or individual. Administrative control is enforced at the network level and governs the security and access control policies.
* LANs provide high-speed bandwidth to internal end devices and intermediary devices, as shown in the figure.
* **WANs**
* The figure shows a WAN which interconnects two LANs. A WAN is a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet Service Providers (ISPs).

WANs have specific characteristics:

* WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
* WANs are usually administered by multiple service providers.
* WANs typically provide slower speed links between LANs.

The internet is a worldwide collection of interconnected networks (internetworks, or internet for short).

Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. The red WAN connection lines represent all the varieties of ways we connect networks. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions (not shown).

The internet is not owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that were developed to help maintain the structure and standardization of internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

There are two other terms which are similar to the term internet: intranet and extranet.

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization. An intranet is designed to be accessible only by the organization's members, employees, or others with authorization.

An organization may use an extranet to provide secure and safe access to individuals who work for a different organization but require access to the organization’s data. Here are some examples of extranets:

* A company that is providing access to outside suppliers and contractors
* A hospital that is providing a booking system to doctors so they can make appointments for their patients
* A local office of education that is providing budget and personnel information to the schools in its district

Изображение выглядит как текст

Автоматически созданное описание

* **Cable** - Typically offered by cable television service providers, the internet data signal transmits on the same cable that delivers cable television. It provides a high bandwidth, high availability, and an always-on connection to the internet.
* **DSL** - Digital Subscriber Lines also provide high bandwidth, high availability, and an always-on connection to the internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
* **Cellular** - Cellular internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular internet access. Performance is limited by the capabilities of the phone and the cell tower to which it is connected.
* **Satellite** - The availability of satellite internet access is a benefit in those areas that would otherwise have no internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
* **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is not sufficient for large data transfer, although it is useful for mobile access while traveling.
* **Dedicated Leased Line** - Leased lines are reserved circuits within the service provider’s network that connect geographically separated offices for private voice and/or data networking. The circuits are rented at a monthly or yearly rate.
* **Metro Ethernet** - This is sometimes known as Ethernet WAN. In this module, we will refer to it as Metro Ethernet. Metro ethernets extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later module.
* **Business DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Line (SDSL) which is similar to the consumer version of DSL but provides uploads and downloads at the same high speeds.
* **Satellite** - Satellite service can provide a connection when a wired solution is not available.

As networks evolve, we have learned that there are four basic characteristics that network architects must address to meet user expectations:

* Fault Tolerance
* Scalability
* Quality of Service (QoS)
* Security

Fault Tolerance

A fault tolerant network is one that limits the number of affected devices during a failure. It is built to allow 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. Having multiple paths to a destination is known as redundancy.

Implementing a packet-switched network is one way that reliable networks provide redundancy. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the same destination. In the figure, the user is unaware and unaffected by the router that is dynamically changing the route when a link fails.

## Scalability

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. The figure shows how a new network is easily added to an existing network. These networks are scalable because the designers follow accepted standards and protocols. This lets software and hardware vendors focus on improving products and services without having to design a new set of rules for operating within the network.

## Quality of Service

Quality of Service (QoS) is an increasing requirement of networks today. New applications available to users over networks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? 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.

Congestion occurs when the demand for bandwidth exceeds the amount available. Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion.

When the volume of traffic is greater than what can be transported across the network, devices will hold the packets in memory until resources become available to transmit them. In the figure, one user is requesting a web page, and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences 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 Security

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. Network administrators must address two types of network security concerns: network infrastructure security and information security.

Securing the network infrastructure includes physically securing devices that provide network connectivity and preventing unauthorized access to the management software that resides on them, as shown in the figure.

* **Confidentiality** - Data confidentiality means that only the intended and authorized recipients can access and read data.
* **Integrity** - Data integrity assures users that the information has not been altered in transmission, from origin to destination.
* **Availability** - Data availability assures users of timely and reliable access to data services for authorized users.

Изображение выглядит как текст

Автоматически созданное описание

* Bring Your Own Device (BYOD)
* Online collaboration
* Video communications
* Cloud Computing

## Bring Your Own Device (BYOD)

The concept of any device, for any content, in any manner, is a major global trend that requires significant changes to the way we use devices and safely connect them to networks. This is called Bring Your Own Device (BYOD).

BYOD enables end users the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students may have advanced computing and networking devices for personal use. These include laptops, notebooks, tablets, smart phones, and e-readers. These may be purchased by the company or school, purchased by the individual, or both.

## Online Collaboration

Individuals want to connect to the network, not only for access to data applications, but also to collaborate with one another. Collaboration is defined as “the act of working with another or others on a joint project.” Collaboration tools, like Cisco WebEx, shown in the figure, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.

## Video Communications

Another facet of networking that is critical to the communication and collaboration effort is video. Video is used for communications, collaboration, and entertainment. Video calls are made to and from anyone with an internet connection, regardless of where they are located.

## Cloud Computing

Cloud computing is one of the ways that we access and store data. Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Applications such as word processing and photo editing can be accessed using the cloud.

Изображение выглядит как текст

Автоматически созданное описание

Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. No data cables need to be installed, and there is little to no additional electricity used. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

Powerline networking is especially useful when wireless access points cannot reach all the devices in the home. Powerline networking is not a substitute for dedicated cabling in data networks. However, it is an alternative when data network cables or wireless communications are not possible or effective.

­Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

There are several common external threats to networks:

* **Viruses, worms, and Trojan horses** - These contain malicious software or code running on a user device.
* **Spyware and adware** - These are types of software which are installed on a user’s device. The software then secretly collects information about the user.
* **Zero-day attacks** - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.
* **Threat actor attacks** - A malicious person attacks user devices or network resources.
* **Denial of service attacks** - These attacks slow or crash applications and processes on a network device.
* **Data interception and theft** - This attack captures private information from an organization’s network.
* **Identity theft** - This attack steals the login credentials of a user in order to access private data.

These are the basic security components for a home or small office network:

* **Antivirus and antispyware** - These applications help to protect end devices from becoming infected with malicious software.
* **Firewall filtering** - Firewall filtering blocks unauthorized access into and out of the network. This may include a host-based firewall system that prevents unauthorized access to the end device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In contrast, the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security. Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements:

* **Dedicated firewall systems** - These provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
* **Access control lists (ACL)** - These further filter access and traffic forwarding based on IP addresses and applications.
* **Intrusion prevention systems (IPS)** - These identify fast-spreading threats, such as zero-day or zero-hour attacks.
* **Virtual private networks (VPN)** - These provide secure access into an organization for remote workers.

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

**PART 2**

* **Shell** - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
* **Kernel** - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
* **Hardware** - The physical part of a computer including underlying electronics.

When using a CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt, as shown in the example. The system executes the command, often providing textual output. The CLI requires very little overhead to operate. However, it does require that the user have knowledge of the underlying command structure that controls the system

A CLI-based network operating system (e.g., the Cisco IOS on a switch or router) enables a network technician to do the following:

* Use a keyboard to run CLI-based network programs
* Use a keyboard to enter text and text-based commands
* View output on a monitor

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

* **User EXEC Mode** - This mode has limited capabilities but is useful for basic operations. It allows only 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. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the # symbol.

Global configuration mode is accessed before other specific configuration modes. From global config mode, the user can enter different subconfiguration modes. Each of these modes allows the configuration of a particular part or function of the IOS device. Two common subconfiguration modes include:

* **Line Configuration Mode -** Used to configure console, SSH, Telnet, or AUX access.
* **Interface Configuration Mode -** Used to configure a switch port or router network interface.
* Various commands are used to move in and out of command prompts. To move from user EXEC mode to privileged EXEC mode, use the **enable** command. Use the **disable** privileged EXEC mode command to return to user EXEC mode.
* **Note**: Privileged EXEC mode is sometimes called enable mode.
* To move in and out of global configuration mode, use the **configure terminal** privileged EXEC mode command. To return to the privileged EXEC mode, enter the **exit** global config mode command.
* There are many different subconfiguration modes. For example, to enter line subconfiguration mode, you use the **line** command followed by the management line type and number you wish to access. Use the **exit** command to exit a subconfiguration mode and return to global configuration mode.

To move from any subconfiguration mode to the privileged EXEC mode, enter the **end** command or enter the key combination **Ctrl+Z**.

You can also move directly from one subconfiguration mode to another. Notice how after selecting an interface, the command prompt changes from **(config-line)#** para **(config-if)#**.

Изображение выглядит как текст

Автоматически созданное описание

## Device Names

* Start with a letter
* Contain no spaces
* End with a letter or digit
* Use only letters, digits, and dashes
* Be less than 64 characters in length
* From global configuration mode, enter the command **hostname** followed by the name of the switch and press **Enter**. Notice the change in the command prompt name.
* **Note**: To return the switch to the default prompt, use the **no hostname** global config command.

Изображение выглядит как текст

Автоматически созданное описание

## Configuration Files

* **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
* **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.

If power to the device is lost, or if the device is restarted, all configuration changes will be lost unless they have been saved. To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

## IP Addresses

The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

**Note**: IP in this course refers to both the IPv4 and IPv6 protocols. IPv6 is the most recent version of IP and is replacing the more common IPv4.

With the IPv4 address, a subnet mask is also necessary. An IPv4 subnet mask is a 32-bit value that differentiates the network portion of the address from the host portion. Coupled with the IPv4 address, the subnet mask determines to which subnet the device is a member.

The example in the figure displays the IPv4 address (192.168.1.10), subnet mask (255.255.255.0), and default gateway (192.168.1.1) assigned to a host. The default gateway address is the IP address of the router that the host will use to access remote networks, including the internet.

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every four bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values. Groups of four hexadecimal digits are separated by a colon (:) . IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

Cisco IOS Layer 2 switches have physical ports for devices to connect. These ports do not support Layer 3 IP addresses. Therefore, switches have one or more switch virtual interfaces (SVIs). These are virtual interfaces because there is no physical hardware on the device associated with it. An SVI is created in software.

The virtual interface lets you remotely manage a switch over a network using IPv4 and IPv6. Each switch comes with one SVI appearing in the default configuration "out-of-the-box." The default SVI is interface VLAN1.

**Note**: A Layer 2 switch does not need an IP address. The IP address assigned to the SVI is used to remotely access the switch. An IP address is not necessary for the switch to perform its operations.

Изображение выглядит как текст

Автоматически созданное описание

To access the switch remotely, an IP address and a subnet mask must be configured on the 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.

## Module Quiz - Basic Switch and End Device Configuration

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

**PART 3**

## Network Protocol Requirements

The protocols that are used in network communications share many of these fundamental traits. In addition to identifying the source and destination, computer and network protocols define the details of how a message is transmitted across a network. Common computer protocols include the following requirements:

* Message encoding
* Message formatting and encapsulation
* Message size
* Message timing
* Message delivery options

## Message Encoding

One of the first steps to sending a message is encoding. Encoding is the process of converting information into another acceptable form, for transmission. Decoding reverses this process to interpret the information.

Encoding between hosts must be in an appropriate format for the medium. Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of voltages on copper wires, infrared light in optical fibers, or microwaves for wireless systems. The destination host receives and decodes the signals to interpret the message.

## Message Formatting and Encapsulation

When a message is sent from source to destination, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.

Similar to sending a letter, a message that is sent over a computer network follows specific format rules for it to be delivered and processed.

Internet Protocol (IP) is a protocol with a similar function to the envelope example. In the figure, the fields of the Internet Protocol version 6 (IPv6) packet identify the source of the packet and its destination. IP is responsible for sending a message from the message source to destination over one or more networks.

## Message Size

Likewise, when a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces, as shown in Figure 2. The rules that govern the size of the pieces, or frames, communicated across the network are very strict. They can also be different, depending on the channel used. Frames that are too long or too short are not delivered.

The size restrictions of frames require the source host to break a long message into individual pieces that meet both the minimum and maximum size requirements. The long message will be sent in separate frames, with each frame containing a piece of the original message. Each frame will also have its own addressing information. At the receiving host, the individual pieces of the message are reconstructed into the original message.

## Message Timing

Message timing is also very important in network communications. Message timing includes the following:

* **Flow Control -** This is the process of managing the rate of data transmission. Flow control defines how much information can be sent and the speed at which it can be delivered. For example, if one person speaks too quickly, it may be difficult for the receiver to hear and understand the message. In network communication, there are network protocols used by the source and destination devices to negotiate and manage the flow of information.
* **Response Timeout -** If a person asks a question and does not hear a response within an acceptable amount of time, the person assumes that no answer is coming and reacts accordingly. The person may repeat the question or instead, may go on with the conversation. Hosts on the network use network protocols that specify how long to wait for responses and what action to take if a response timeout occurs.
* **Access method -** This determines when someone can send a message. Click Play in the figure to see an animation of two people talking at the same time, then a "collision of information" occurs, and it is necessary for the two to back off and start again. Likewise, when a device wants to transmit on a wireless LAN, it is necessary for the WLAN network interface card (NIC) to determine whether the wireless medium is available.

## Message Delivery Options

Network communications has similar delivery options to communicate. As shown in the figure, there three types of data communications include:

* **Unicast** - Information is being transmitted to a single end device.
* **Multicast** - Information is being transmitted to a one or more end devices.
* **Broadcast** - Information is being transmitted to all end devices.

Click the unicast, multicast, and broadcast buttons in the figure for an example of each.

**Note**: The multicast animation is indicating the destination devices. By default, a switch will send multicast packets out all ports except the incoming port. However, only the hosts that are part of the multicast group will process the packet.

Изображение выглядит как текст

Автоматически созданное описание

## Network Protocol Overview

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

**Hypertext Transfer Protocol (HTTP) -** This protocol governs the way a web server and a web client interact. HTTP defines the content and formatting of the requests and responses that are exchanged between the client and server. Both the client and the web server software implement HTTP as part of the application. HTTP relies on other protocols to govern how the messages are transported between the client and server.

* **Transmission Control Protocol (TCP)** - This protocol manages the individual conversations. TCP is responsible for guaranteeing the reliable delivery of the information and managing flow control between the end devices.
* **Internet Protocol (IP) -** This protocol is responsible for delivering messages from the sender to the receiver. IP is used by routers to forward the messages across multiple networks.
* **Ethernet**- This protocol is responsible for the delivery of messages from one NIC to another NIC on the same Ethernet local area network (LAN).

Изображение выглядит как текст

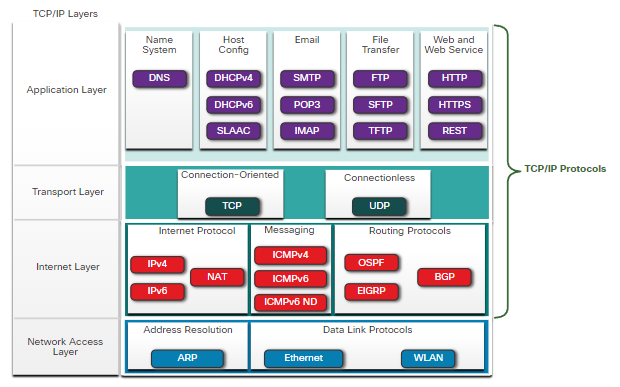
Автоматически созданное описание

Изображение выглядит как стол

Автоматически созданное описание

* **Internet Protocol Suite or TCP/IP** - This is the most common and relevant protocol suite used today. The TCP/IP protocol suite is an open standard protocol suite maintained by the Internet Engineering Task Force (IETF).
* **Open Systems Interconnection (OSI) protocols** - This is a family of protocols developed jointly in 1977 by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). The OSI protocol also included a seven-layer model called the OSI reference model. The OSI reference model categorizes the functions of its protocols. Today OSI is mainly known for its layered model. The OSI protocols have largely been replaced by TCP/IP.
* **AppleTalk** - A short-lived proprietary protocol suite released by Apple Inc. in 1985 for Apple devices. In 1995, Apple adopted TCP/IP to replace AppleTalk.
* **Novell NetWare** - A short-lived proprietary protocol suite and network operating system developed by Novell Inc. in 1983 using the IPX network protocol. In 1995, Novell adopted TCP/IP to replace IPX.

TCP/IP protocols are available for the application, transport, and internet layers. There are no TCP/IP protocols in the network access layer. The most common network access layer LAN protocols are Ethernet and WLAN (wireless LAN) protocols. Network access layer protocols are responsible for delivering the IP packet over the physical medium.



**Open standard protocol suite** - This means it is freely available to the public and can be used by any vendor on their hardware or in their software.

**Standards-based protocol suite** - This means it has been endorsed by the networking industry and approved by a standards organization. This ensures that products from different manufacturers can interoperate successfully.

**Application Layer**

Name System

* **DNS** - Domain Name System. Translates domain names such as cisco.com, into IP addresses.

Host Config

* **DHCPv4** - Dynamic Host Configuration Protocol for IPv4. A DHCPv4 server dynamically assigns IPv4 addressing information to DHCPv4 clients at start-up and allows the addresses to be re-used when no longer needed.
* **DHCPv6** - Dynamic Host Configuration Protocol for IPv6. DHCPv6 is similar to DHCPv4. A DHCPv6 server dynamically assigns IPv6 addressing information to DHCPv6 clients at start-up.
* **SLAAC** - Stateless Address Autoconfiguration. A method that allows a device to obtain its IPv6 addressing information without using a DHCPv6 server.

Email

* **SMTP** - Simple Mail Transfer Protocol. Enables clients to send email to a mail server and enables servers to send email to other servers.
* **POP3** - Post Office Protocol version 3. Enables clients to retrieve email from a mail server and download the email to the client's local mail application.
* **IMAP** - Internet Message Access Protocol. Enables clients to access email stored on a mail server as well as maintaining email on the server.

File Transfer

* **FTP** - File Transfer Protocol. Sets the rules that enable a user on one host to access and transfer files to and from another host over a network. FTP is a reliable, connection-oriented, and acknowledged file delivery protocol.
* **SFTP** - SSH File Transfer Protocol. As an extension to Secure Shell (SSH) protocol, SFTP can be used to establish a secure file transfer session in which the file transfer is encrypted. SSH is a method for secure remote login that is typically used for accessing the command line of a device.
* **TFTP** - Trivial File Transfer Protocol. A simple, connectionless file transfer protocol with best-effort, unacknowledged file delivery. It uses less overhead than FTP.

Web and Web Service

* **HTTP** - Hypertext Transfer Protocol. A set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the World Wide Web.
* **HTTPS** - HTTP Secure. A secure form of HTTP that encrypts the data that is exchanged over the World Wide Web.
* **REST** - Representational State Transfer. A web service that uses application programming interfaces (APIs) and HTTP requests to create web applications.

**Transport layer**

Connection-Oriented

* **TCP** - Transmission Control Protocol. Enables reliable communication between processes running on separate hosts and provides reliable, acknowledged transmissions that confirm successful delivery.

Connectionless

* **UDP** - User Datagram Protocol. Enables a process running on one host to send packets to a process running on another host. However, UDP does not confirm successful datagram transmission.

**Internet Layer**

Internet Protocol

* **IPv4** - Internet Protocol version 4. Receives message segments from the transport layer, packages messages into packets, and addresses packets for end-to-end delivery over a network. IPv4 uses a 32-bit address.
* **IPv6** - IP version 6. Similar to IPv4 but uses a 128-bit address.
* **NAT** - Network Address Translation. Translates IPv4 addresses from a private network into globally unique public IPv4 addresses.

Messaging

* **ICMPv4** - Internet Control Message Protocol for IPv4. Provides feedback from a destination host to a source host about errors in packet delivery.
* **ICMPv6** - ICMP for IPv6. Similar functionality to ICMPv4 but is used for IPv6 packets.
* **ICMPv6 ND** - ICMPv6 Neighbor Discovery. Includes four protocol messages that are used for address resolution and duplicate address detection.

Routing Protocols

* **OSPF** - Open Shortest Path First. Link-state routing protocol that uses a hierarchical design based on areas. OSPF is an open standard interior routing protocol.
* **EIGRP** - EIGRP - Enhanced Interior Gateway Routing Protocol. An open standard routing protocol developed by Cisco that uses a composite metric based on bandwidth, delay, load and reliability.
* **BGP** - Border Gateway Protocol. An open standard exterior gateway routing protocol used between Internet Service Providers (ISPs). BGP is also commonly used between ISPs and their large private clients to exchange routing information.

**Network Access Layer**

Address Resolution

* **ARP** - Address Resolution Protocol. Provides dynamic address mapping between an IPv4 address and a hardware address.

**Note**: You may see other documentation state that ARP operates at the Internet Layer (OSI Layer 3). However, in this course we state that ARP operates at the Network Access layer (OSI Layer 2) because it's primary purpose is the discover the MAC address of the destination. A MAC address is a Layer 2 address.

Data Link Protocols

* **Ethernet** - Defines the rules for wiring and signaling standards of the network access layer.
* **WLAN** - Wireless Local Area Network. Defines the rules for wireless signaling across the 2.4 GHz and 5 GHz radio frequencies.

Изображение выглядит как текст

Автоматически созданное описание

* **(ISOC)** - Responsible for promoting the open development and evolution of internet use throughout the world.
* **Internet Architecture Board (IAB)** - Responsible for the overall management and development of internet standards.
* **Internet Engineering Task Force (IETF)**- Develops, updates, and maintains internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols, which are known as Request for Comments (RFC) documents.
* **Internet Research Task Force (IRTF)**- Focused on long-term research related to internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).
* **Internet Corporation for Assigned Names and Numbers (ICANN)**- Based in the United States, ICANN coordinates IP address allocation, the management of domain names, and assignment of other information used in TCP/IP protocols.
* **Internet Assigned Numbers Authority (IANA)**- Responsible for overseeing and managing IP address allocation, domain name management, and protocol identifiers for ICANN.

## Electronic and Communications Standards

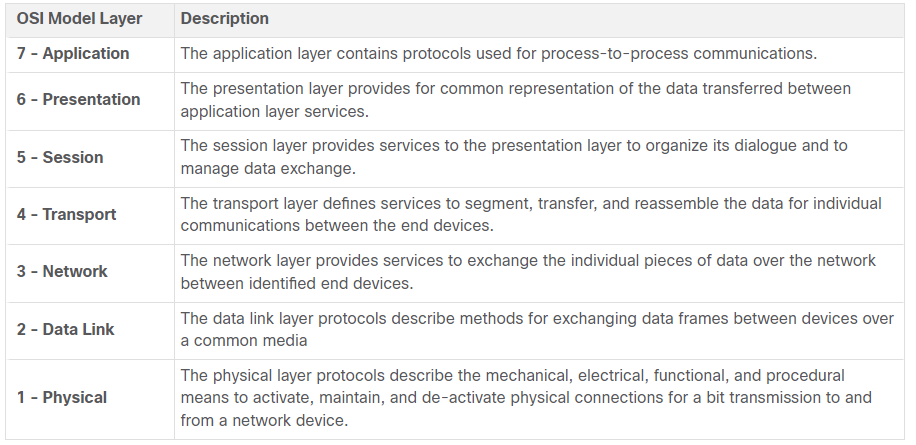
Other standards organizations have responsibilities for promoting and creating the electronic and communication standards used to deliver the IP packets as electronic signals over a wired or wireless medium.

These standard organizations include the following:

* **Institute of Electrical and Electronics Engineers**(**IEEE**, pronounced “I-triple-E”) - Organization of electrical engineering and electronics dedicated to advancing technological innovation and creating standards in a wide area of industries including power and energy, healthcare, telecommunications, and networking. Important IEEE networking standards include 802.3 Ethernet and 802.11 WLAN standard. Search the internet for other IEEE network standards.
* **Electronic Industries Alliance (EIA)** - Organization is best known for its standards relating to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
* **Telecommunications Industry Association (TIA)** - Organization responsible for developing communication standards in a variety of areas including radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more.
* **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T)** - One of the largest and oldest communication standards organizations. The ITU-T defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

Изображение выглядит как текст

Автоматически созданное описание



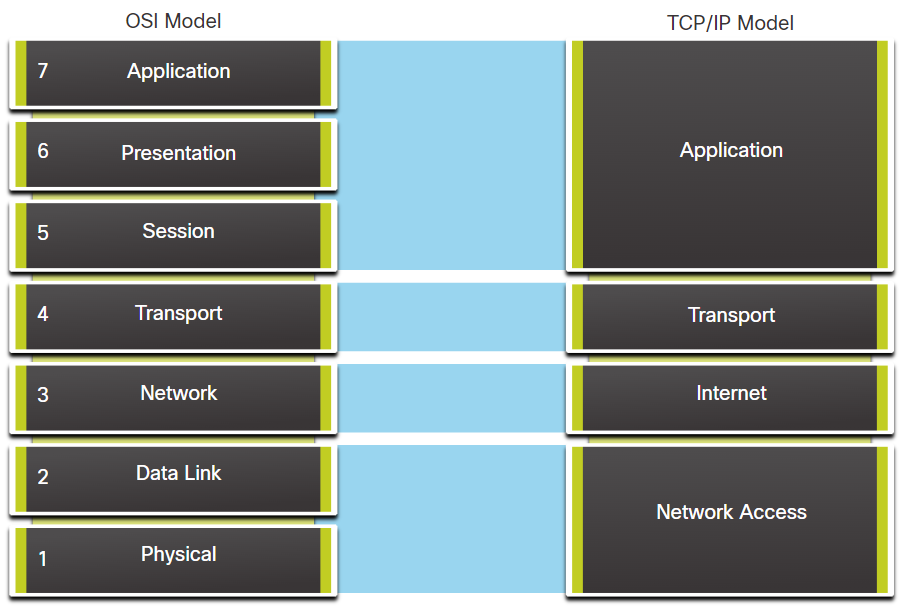
**Note**: Whereas the TCP/IP model layers are referred to only by name, the seven OSI model layers are more often referred to by number rather than by name. For instance, the physical layer is referred to as Layer 1 of the OSI model, data link layer is Layer2, and so on.

The TCP/IP Protocol Model

The TCP/IP protocol model for internetwork communications was created in the early 1970s and is sometimes referred to as the internet model. This type of model closely matches the structure of a particular protocol suite. The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite. TCP/IP is also used as a reference model. The table shows details about each layer of the OSI model.

| TCP/IP Model LayerDescription4 - ApplicationRepresents data to the user, plus encoding and dialog control.3 - TransportSupports communication between various devices across diverse networks.2 - InternetDetermines the best path through the network.1 - Network AccessControls the hardware devices and media that make up the network. | |
| --- | --- |
| **TCP/IP Model Layer** | **Description** |
| **4 - Application** | Represents data to the user, plus encoding and dialog control. |
| **3 - Transport** | Supports communication between various devices across diverse networks. |
| **2 - Internet** | Determines the best path through the network. |
| **1 - Network Access** | Controls the hardware devices and media that make up the network. |

The definitions of the standard and the TCP/IP protocols are discussed in a public forum and defined in a publicly available set of IETF RFCs. An RFC is authored by networking engineers and sent to other IETF members for comments.



## Segmenting Messages

This leads to segmenting messages having two primary benefits:

* **Increases speed** - Because a large data stream is segmented into packets, large amounts of data can be sent over the network without tying up a communications link. This allows many different conversations to be interleaved on the network called multiplexing.
* **Increases efficiency** -If a single segment is fails to reach its destination due to a failure in the network or network congestion, only that segment needs to be retransmitted instead of resending the entire data stream.

## Sequencing

The challenge to using segmentation and multiplexing to transmit messages across a network is the level of complexity that is added to the process. Imagine if you had to send a 100-page letter, but each envelope could only hold one page. Therefore, 100 envelopes would be required and each envelope would need to be addressed individually. It is possible that the 100-page letter in 100 different envelopes arrives out-of-order. Consequently, the information in the envelope would need to include a sequence number to ensure that the receiver could reassemble the pages in the proper order.

## Protocol Data Units

As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocol information is added at each level. This is known as the encapsulation process.

**Note**: Although the UDP PDU is called datagram, IP packets are sometimes also referred to as IP datagrams.

* 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**: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.

## De-encapsulation Example

This process is reversed at the receiving host and is known as de-encapsulation. De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.

Изображение выглядит как текст

Автоматически созданное описание

## Addresses

As you just learned, it is necessary to segment messages in a network. But those segmented messages will not go anywhere if they are not addressed properly. This topic gives an overview of network addresses. You will also get the chance to use the Wireshark tool, which will help you to ‘view’ network traffic.

The network and data link layers are responsible for delivering the data from the source device to the destination device. As shown in the figure, protocols at both layers contain a source and destination address, but their addresses have different purposes:

* **Network layer source and destination addresses** - Responsible for delivering the IP packet from the original source to the final destination, which may be on the same network or a remote network.
* **Data link layer source and destination addresses** - Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.

The IP packet contains two IP addresses:

* **Source IP address** - The IP address of the sending device, which is the original source of the packet.
* **Destination IP address** - The IP address of the receiving device, which is the final destination of the packet.

The IP addresses indicate the original source IP address and final destination IP address. This is true whether the source and destination are on the same IP network or different IP networks.

An IP address contains two parts:

* **Network portion (IPv4) or Prefix (IPv6)** - The left-most part of the address that indicates the network in which the IP address is a member. All devices on the same network will have the same network portion of the address.
* **Host portion (IPv4) or Interface ID (IPv6)** - The remaining part of the address that identifies a specific device on the network. This portion is unique for each device or interface on the network.

**Note**: The subnet mask (IPv4) or prefix-length (IPv6) is used to identify the network portion of an IP address from the host portion.

## Devices on the Same Network

In this example we have a client computer, PC1, communicating with an FTP server on the same IP network.

* **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
* **Destination IPv4 address** - The IPv4 address of the receiving device, FTP server: 192.168.1.9.

Notice in the figure that the network portion of both the source IPv4 address and destination IPv4 address are on the same network. Notice in the figure that the network portion of the source IPv4 address and the network portion of the destination IPv4 address are the same and therefore; the source and destination are on the same network.

MAC addresses are physically embedded on the Ethernet NIC.

* **Source MAC address** - This is the data link address, or the Ethernet MAC address, of the device that sends the data link frame with the encapsulated IP packet. The MAC address of the Ethernet NIC of PC1 is AA-AA-AA-AA-AA-AA, written in hexadecimal notation.
* **Destination MAC address** - When the receiving device is on the same network as the sending device, this is the data link address of the receiving device. In this example, the destination MAC address is the MAC address of the FTP server: CC-CC-CC-CC-CC-CC, written in hexadecimal notation.

The frame with the encapsulated IP packet can now be transmitted from PC1 directly to the FTP server.

## Role of the Network Layer Addresses

When the sender of the packet is on a different network from the receiver, the source and destination IP addresses will represent hosts on different networks. This will be indicated by the network portion of the IP address of the destination host.

* **Source IPv4 address** - The IPv4 address of the sending device, the client computer PC1: 192.168.1.110.
* **Destination IPv4 address** - The IPv4 address of the receiving device, the server, Web Server: 172.16.1.99.

## Role of the Data Link Layer Addresses: Different IP Networks

When the sender and receiver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host because the host is not directly reachable in the network of the sender. The Ethernet frame must be sent to another device known as the router or default gateway. In our example, the default gateway is R1. R1 has an Ethernet data link address that is on the same network as PC1. This allows PC1 to reach the router directly.

* **Source MAC address** - The Ethernet MAC address of the sending device, PC1. The MAC address of the Ethernet interface of PC1 is AA-AA-AA-AA-AA-AA.
* **Destination MAC address** - When the receiving device, the destination IP address, is on a different network from the sending device, the sending device uses the Ethernet MAC address of the default gateway or router. In this example, the destination MAC address is the MAC address of the R1 Ethernet interface, 11-11-11-11-11-11. This is the interface that is attached to the same network as PC1, as shown in the figure.

As the IP packet travels from host-to-router, router-to-router, and finally router-to-host, at each point along the way the IP packet is encapsulated in a new data link frame. Each data link frame contains the source data link address of the NIC card sending the frame, and the destination data link address of the NIC card receiving the frame.

The Layer 2, data link protocol is only used to deliver the packet from NIC-to-NIC on the same network. The router removes the Layer 2 information as it is received on one NIC and adds new data link information before forwarding out the exit NIC on its way towards the final destination.

The IP packet is encapsulated in a data link frame that contains the following data link information:

* **Source data link address** - The physical address of the NIC that is sending the data link frame.
* **Destination data link address** - The physical address of the NIC that is receiving the data link frame. This address is either the next hop router or the address of the final destination device.

Изображение выглядит как текст

Автоматически созданное описание

## Module Quiz - Protocols and Models

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описаниеИзображение выглядит как текст

Автоматически созданное описание