Post 7

Thursday, January 24, 2019 11:09 PM

INTRODUCTION TO NETWORKS

Internet: Global network combines enterprise, users, and ISP's (A network of networks)

Data networks: By business to record/manage systems *Evolved services (email/video/messaging/telephony)

IoE: Internet of Everything: Adding devices of all kinds on the Internet

The Human Network: Cisco term: Explains how Internet changed social/commercial/political/personal actions

Communication collaboration: Transmission/receipt of information

Clients & Servers: Computers connected to a network participate in communication classified as hosts or end devices

Hosts send/receive messages	End devices act as a client/server/both	Software installed determines role

Servers: Hosts have software installed to enable request/display info obtained from server
*Required web server software to provide web services

Clients: Computers have software installed to enable request/display info obtained from server
*Web browsers access pages stored on web server – Client/server software can run on separate computers or 1

Peer-to-Peer Network: Many business/home computers function as server/client on the network

Peer-to-Peer Networking:

Advantages	**Disadvantages**
○ Easy set up ○ Less complex ○ Lower cost (devices may not be required) ○ Used for simple tasks: ○ File transfers/Printer sharing	○ No centralized administration ○ Not as secure ○ Not scalable ○ Devices may act as both clients/servers which slows performance

Network Infrastructure: The physical architecture/hardware/connections used to define and transmit data

Network components: 1. Devices 2. Media 3. Services Provide stable/reliable channels where communication occurs

1. **Media:** Hardware components: Network components are used to provide services/processes

2. **Service:** Provides information based on a request

Processes: Provide functionality that directs/moves messages through a network

End Devices (AKA hosts): Form the interface between users & the underlying communication network

End devices:

Computers – Work stations, laptops, file/web servers	**Network Printers**	**VoIP Phones**	**Telepresence Endpoints**
Mobile phones – Smartphones, tablets, PDA's – Bar-code scanners, wireless card readers	**Security Cameras**		

Telepresence endpoints: Cisco products for business virtual meetings/collaboration

Intermediary Network Devices		○ Interconnect end devices ○ Work behind scenes to ensure data flows on network ○ Can connect individual hosts to network ○ Can connect multiple individual networks to form an "internetwork"
Examples		○ Network access (switches, wireless access points) ○ Internetworking (routers) ○ Security (firewalls)
		○ Manage data flow

	○ Direct path of data but don’t generate/change content ○ Use destination host address along with info about network interconnections ○ To determine path messages should take w.in the network

Processes on intermediary network devices functions:

- Regenerate/re-transmit data signals
- Maintain info about what pathways exist through the network/internetwork
- Notify other devices of errors/communication failures
- Direct data along alternate pathways when there is a link failure
- Classify/direct messages according to QoS (Quality of Service) priorities
- Permit/deny data flow based on security settings

Network Media: Communication carried through a median in a network: Provides the channel over which msg travels.

Types of Transmission media: Modern networks use 3 types of media to interconnect devices through pathways.

1. Metallic wires (cable)
2. Glass or plastic (fiber-optics)
3. Wireless transmission (radio frequency)

Encoding: Process by which bits are represented by media: Transmitted differently for each media type

Types of Encoding

Metallic Wires	Data is encoded into electrical impulses that match specific patterns
Fiber-Optic	Rely on pulses of light within infrared or visible light ranges
Wireless	Various wave bit values are depicted by patterns of electro-magnetic waves

Criteria for choosing network media

- Distance medium can carry a signal
- Environment media is to be installed on
- Amount of data/speed to be transmitted
- Cost of medium & installation

Interface: Specialized ports on internetworking device connect to individual networks (ports on a router)
Routers = Network interfaces

Two Types of Topology Diagrams:

Physical Topology	○ Identifies the physical location of intermediary devices, configured ports, and cable installation
Logical Topology	○ Identifies devices, ports, and IP addressing scheme

Network infrastructure can vary greatly in terms of:

1. Size of area covered
2. Number of users connected
3. Number/types of services available

Types of Networks

LAN	○ **Local Area Network** ○ Access to users in a small area ○ Single location: Can be multiple logical networks ○ High Bandwidth
WAN	○ **Wide Area Network** ○ Connects LANs ○ Access to other networks over a wide geographical area
MAN	○ **Metropolitan Area Network** ○ Infrastructure that spans a physical area larger than a LAN, but smaller than a WAN ○ Example: A city ○ Typically operated by a single entity such as a large organization (school)
WLAN	○ **Wireless LAN** ○ Wirelessly interconnects users & end points in a small area
SAN	○ **Storage Area Network** ○ Designed to support file servers & provide data storage, retrieval and replication

	○ High-end servers, multiple disk arrays, fiber channel interconnection technology

Local Area Networks (LANs)

1. Interconnect devices in a limited area: Home, school, office, building or campus
2. Single Admin/organization: Control governs security/access control policies are enforced (network level)
3. Provides high-speed bandwidth to internal end devices/intermediary devices

Wide Area Networks (WANs)

1. Typically managed by Service Providers (SP), or Internet Service Providers (ISP)
2. Interconnections over wide geographic areas: Cities, states, provinces, countries or continents
3. Administered usually by multiple service providers
4. Typically provides slower-speed links between LANs

The Internet is a conglomerate of networks: It's not owned by any individual group: Organizations have been developed for the purpose of helping maintain structure/standardization of Internet Protocols/processes

IETF	Internet Engineering Task Force
ICANN	Internet Corporation for Assigned Names/Numbers
IAB	Internet Architecture Board

internet: LOWER CASE: Describes multiple interconnected networks **||** **Internet:** Services like WWW
Intranet: Refers to private LANs/WANs that belong to an organization. Designed to be accessible only from within
Extranet: Provides safe/secure access to individuals who work for different organizations but require company data (contractors)

Connecting Users to the Internet

Cable	○ Offered by cable television providers ○ Signal is carried by same coaxial cable as television ○ **High-bandwidth, always on, connection**
DSL	▪ Modem separates DSL signal from telephone signal ▪ Runs over phone line split into 3 channels 1. Voice Telephone 2. Internet 3. Sending/uploading information ○ **High-bandwidth, always on connection**
Cellular	○ Uses a cell phone network to connect to the Internet ○ Performance is limited by phone type and towers
Satellite	○ Requires direct access to light
Dial-up	○ Uses an ISP access number to connect to the Internet ○ **Low-Bandwidth**

Connecting Businesses to the Internet

Dedicated Lease Line	○ Reserves circuits that connect geographically separated offices for private/data networking ○ Rented at monthly or yearly rates ○ Expensive ○ T1 (1.4mbps) or T3 (44.7mbps) ○ E1 (2mbps) and E3 (34 mbps)
Metro Ethernet	○ Available from a provider to the customer ○ A dedicated copper or fiber connection ○ Bandwidth speeds of 10mbps to 10gbps
Ethernet over Copper (EoC)	○ More economical than fiber optics ○ Reaches up to 40mbps
SDSL	○ Symmetrical Digital Subscriber Lines ○ ADSL fluctuates download/upload speeds (bottle necks) ○ SDSL does not

Port Density: How many ports can we put on a device?

Copper	○ Least expensive ○ Less distance ○ Prone to interference from EMI (electromechanical interference)
Fiber	○ More expensive ○ Farther distances ○ Glass/plastic: Uses light signals
Wireless	○ Shared medium ○ Radio signals/frequencies ○ Prone to interference

Converged network: Consolidation of different types of networks onto 1 platform (separate/distinct communication converged)

Supporting Network Architecture: 1. Fault tolerance	2. Scalability	3. QoS (Quality of Service)	4. Security

Fault tolerance: The expectation that the Internet is always available

Fault tolerant network: A network that limits the impact of a failure so that the fewest amount of devices are affected

- These networks depend on multiple paths between source/destination of a message

Redundancy: Having multiple paths to a destination

Circuit-switched connection oriented networks: A temporary path/circuit used for the duration of that pathway

- Example: Old phone circuit switch boards || Referred to as a circuit-switch process
- Gives priority to existing circuit connections at the expense of new circuit requests

Packet-switched Networks: A message can be broken down to blocks, with each block having address info to origin/destination

Packet	○ Message blocks of information or data sent through various paths ○ Address is only visible info || Referred to as IP addresses ○ Each packet is sent independently from 1 location to another ○ At location routing decision is made: Which path to fwd packet to destination ○ Packets lost can be retransmitted via another pathway ○ Reserved circuits aren’t needed in packet-switched networks
Internet	Fault tolerant method of communication (very scalable)

Scalable Network: Can expand quickly to support new users/applications without impacting performance

Quality of Service: Expectation for quality of delivered services/applications

- Packet-switched networks don’t guarantee all packets will arrive on time/in correct order
- Bandwidth measures data-carrying capacity on a network

Priority decisions for organizations may include:

Time-sensitive	Increase priority: Telephony/Video distribution
Non-time-sensitive	Decrease priority: Web retrieval/Email
High Importance	Increase priority: Production control/business transaction data
Undesirable	Decrease/Block: P2p/Live entertainment

Security Consequences: Outages, Property theft, Publicized public info, data/labor loss, Misdirection: Loss of funds

2 types of SecConcerns: 1. **Infrastructure:** Physical 2. **Information**: Protecting packets transmitted/info stored on network/devices

Security should prevent: Unauthorized disclosure, theft of info, unauthorized info modification, DoS

Primary goals of security: Confidentiality, communication integrity, availability

BYOD = Bring your own device (tools to access info/communicate across a business/campus)

Security threats: Viruses/worms/Trojans, Spyware/adware, 0day/0hr, DoS, Interception/identity theft

Cloud Computing: Use of computing resources delivered as a service over a network

1. Organizational flexibility: Information can be accessed any time/where

   2. Agility/rapid deployment
   3. Reduced cost of infrastructure
   4. Refocus IT resources
   5. Creation of new business models

   Cloud Types

Private	○ For a specific entity, organization or government

	○ Can be expensive to build/maintain ○ Can be managed by an outside source
Public	○ Available to general population ○ Can be free/pay-per-use
Hybrid	○ 2 or more clouds distinctive yet connected through 1 architecture
Custom	○ Made specifically to fit a need ○ Cloud computing is available because of data centers

Rollover cable: Cable has been 'rolled over' or twisted one time: Flat
Patch panel: Termination point for cabling
Router: Forwards packets to/receives from Internet
Switch: Connects end devices using cables
Wireless Access Point: Radio transceiver connects end devices wirelessly
Firewall appliances: Secures outgoing/restricts incoming traffic
In larger businesses:

- End devices (PC's/Laptops) are connected to network switch using wired connections
- Network switches connect to routers to send traffic beyond network

Cisco IOS: Collection of OS's used on Cisco networking devices
Kernel: Portion of OS that interacts directly with hardware
Shell: Portion of kernel that interfaces with applications/user
CLI: Usage is direct with system (txt based cmd) **||** **GUI:** Graphical software **||** **Firmware:** OS on home routers
OS's Allow us to: Use mouse/view monitor output/enter txt cmds/select options in a dialog box/manage processes

Location of Cisco IOS	○ 7MB in size ○ Stored in semi-permanent memory or flash ○ Flash can be used to store multiple versions of IOS software simultaneously
Flash memory	○ Provides non-volatile storage (not lost when device loses power) ○ Can be changed/overwritten as needed ○ Many devices IOS copies from flash into RAM when powered on ○ It runs from RAM while operating
RAM	○ Stores data used by device to support network operations ○ Running IOS in RAM increases performance ○ RAM is volatile (lost when powered off)

Major functions by Cisco routers/switches:

Security	IP addressing of virtual/physical interfaces	Configurations to optimize connectivity
Routing	Quality of Service (QoS)	Frame switching/Packet forwarding

Console access methods: Console/Telnet or SSH/AUX port
Console port: Port that provides out-of-band access to Cisco device
Out-of-Band: Access through dedicated channel for device maintenance purposes only

- Console port can be used when networking services have failed/remote access of IOS isn't available
- Should be configured to have passwords

Telnet: Method for remote CLI session, through a virtual interface over a network

- Unlike console connection: Telnet sessions require active networking services on device
- The device must have at least 1 active interface configured with an Internet address, such as IPv4
- IOS devices include a Telnet server process to allows users to enter configuration cmds from client
- Not encrypted

SSH: Protocol with remote login like Telnet, but more secure services

- Provides stronger password authentication than Telnet (uses encryption)
- Keeps userID, password & details of management session private
- Use whenever possible

AUX: Older way to establish a CLI session remotely through a telephone dial-up connection via modem on router

- Doesn't require any networking services to be configured/available on a device
- In the event network services fail, this may be another way to access a router/switch
- Can be used locally, like the console port, with a direct connection

Terminal Emulation: PuTTY, SecureCRT, Tera Term, Hyper Terminal, OSX Terminal