CTS2134
Introduction to Networking

Module 01 - Networking Basics

Components of a Network

1. Computer systems (nodes or hosts)
2. Transmission media - a path for electrical signals between devices
3. Network interfaces - devices that send and receive electrical signals
4. Protocols - rules or standards that describe how hosts communicate and exchange data

Why network

Despite the costs of implementation and maintenance, networks actually save organizations money by allowing them to share resources:

1. Consolidate (centralize) data storage and backup
2. Share peripheral devices like printers
3. Increase communication: internal and external
4. Increase productivity and collaboration

Network Types

Peer-to-Peer: In a peer to peer network, the hosts provide and consume network services, and each host has the same operating system.

Advantages

-Easy implementation

-Inexpensive

Disadvantages

-Difficult to expand (not scalable)

-Difficult to support

-Lack centralized control

-No centralized storage

Network Types

Client Server: In a client/server network, hosts have specific roles. For example, some hosts are assigned server roles which allows them to provide network resources to other hosts. Other hosts are assigned client roles which allows them to consume network resources. Unlike peer to peer networks, hosts in a client/server network have different operating systems.

Advantages

-Easily expanded (scalable)
-Easy support
-Centralized services
-Easy to backup

Disadvantages

-Server operating systems are expensive
-Requires extensive advanced planning

Network Size

Local Area Network (LAN)

-LANs reside in a small geographic area, like in an office. A series of connected LANs, or a LAN connected across several buildings or offices, is called an *internetwork.*

Wide Area Network (WAN)

-A WAN is a group of LANs that are geographically isolated but connected to form a large internetwork. When implementing a WAN, remember to provide local access to user resources to prevent a high rate of WAN traffic.

Network Communication

Communication between hosts on a network generally takes one of three forms:

- Simplex
  - one-way communication from a sender to a receiver.
- Half-duplex
  - two-way communication between two hosts. Communication only travels in one direction at a time.
- Duplex
  - two-way communication between hosts. Communication travels in both directions simultaneously.

Topology

Topology is the term used to describe how devices are connected and how messages flow from device to device.

There are two types of network topologies:

-Physical topology describes the physical way the network is wired.

-Logical topology describes the way in which messages are sent.

Bus Physical Topology

A physical bus topology consists of a trunk cable with nodes either inserted directly into the trunk, or nodes tapping into the trunk using offshoot cables called drop cables.

- –Signals travel from one node to all other nodes on the bus.
- –A device called a terminator is placed at both ends of the trunk cable.
- –Terminators absorb signals and prevent them from reflecting repeatedly back and forth on the cable.

Bus Physical Topology

Advantages compared to star:

- **Requires less cable than the star**

Disadvantages compared to star:

- **Difficult to troubleshoot cabling problems**
- **Not fault tolerant**
- **Not scalable**

Ring Physical Topology

A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring. In ring topologies, each device on the network acts as a repeater to send the signal to the next device.

With a ring:

-Installation requires careful planning to create a continuous ring.

-Isolating problems can require going to several physical locations along the ring.

-A malfunctioning node or cable break can prevent signals from reaching nodes further along on the ring.

Star Physical Topology

A star topology uses a hub (or switch) to concentrate all network connections to a single physical location. Today it is the most popular type of topology for a LAN.

With the star:

-All network connections are located in a single place, which makes it easy to troubleshoot and reconfigure.

-Nodes can be added to or removed from the network easily.

-Cabling problems usually affect only one node.

-Requires more cable than the bus or ring topology. Every node has its own cable.

Star Physical Topology

Disadvantages compared to bus:

- **Requires more cable than the star**

Advantages compared to bus:

- **Easier to troubleshoot cabling problems**
- **More fault tolerant**
- **More scalable**

Mesh Physical Topology

A mesh topology exists when there are multiple paths between nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because alternate paths can be used when one path fails.

Two variations of mesh topologies exist:

-Partial Mesh--Some redundant paths exist.

-Full Mesh--Every node has a point-to-point connection with every other node. Full mesh topologies are usually impractical because the number of connections increases dramatically with every new node added to the network.

Logical Topologies (review fact sheet)

Bus

-Messages are sent to all devices connected to the bus.

Ring

-Messages are sent from device-to-device in a predetermined order until they reach the destination device.

Star

-Messages are sent directly to (and only to) the destination device.

Common TCP/IP Protocols

- Web browsing
  - Hypertext Transfer Protocol (HTTP)
  - HTTP over SSL (HTTPS)
    - uses SSL
- Security protocols
  - Secure Sockets Layer (SSL)
    - RSA: Public Key cryptography
  - Transport Layer Security (TLS)
    - Handshake

Common TCP/IP Protocols

- File Transfer
  - File Transfer Protocol (FTP)
  - Trivial File Transfer Protocol (TFTP)
    - no user authentication and no error detection.
  - Secure File Transfer Protocol (SFTP)
    - uses Secure Shell (SSH)
  - Secure Copy (SCP)
    - Unix/Linux networks, relies on SSH

Common TCP/IP Protocols

- E-mail
  - Simple Mail Transfer Protocol (SMTP)
  - Internet Message Access Protocol (IMAP)
  - Post Office Protocol (POP)
- Transport protocols
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

Common TCP/IP Protocols

- Network services
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)
  - Network Time Protocol (NTP)
  - Network News Transport Protocol (NNTP)
  - Lightweight Directory Access Protocol (LDAP)

Common TCP/IP Protocols

- Network management
  - Simple Network Management Protocol (SNMP)
    - Lets network hosts exchange configuration and status information
  - Remote Terminal Emulation (Telnet)
  - Secure Shell (SSH)
    - uses RSA public key cryptography

Common TCP/IP Protocols

- Control protocols
  - Internet Control Message Protocol (ICMP)
    - use ICMP messages to check network connectivity.
      - Ping
      - Traceroute (**tracert**)
  - Internet Group Membership Protocol (IGMP)
    - group members can receive broadcast messages intended for the group (called multicasts).

Internet Connectivity Parameters

- IP address
  - The IP address Identifies both the logical host and the logical network addresses.
- Subnet mask
  - identifies which portion of the IP address is the network address
- Default gateway
  - the IP address of the router interface on the same subnet
- DNS server (maps hostnames to IP address)
- Host name (logical name of device)

OSI Model Facts

Using the OSI model to discuss networking concepts has the following advantages:

- Provides a common language or reference point between network professionals
- Divides networking tasks into logical layers for easier comprehension
- Allows specialization of features at different levels
- Aids in troubleshooting
- Promotes standards of interoperability between networks and devices
- Provides modularity in networking features (developers can change features without changing the entire approach)

OSI Layer Facts

- Application (Layer 7)
  - integrates network functionality into the host operating system
- Presentation (Layer 6)
  - Formats data into a compatible form
- Session (Layer 5)
  - managing the sessions in which data is transferred.

OSI Layer Facts

Transport (Layer 4)

1. End-to-end flow control
2. Port and socket addressing
3. Sequencing (segmentation and combination)
4. Connection services, either reliable (connection-oriented) or unreliable (connectionless) delivery of data.

Data at the Transport layer is referred to as a *segment*.

OSI Layer Facts

Network (Layer 3): The Network layer describes how data is routed across networks and on to the destination.

1. Uses logical addresses to identify hosts and networks
2. Routing: Determining the next network point to which data should be sent.
   - Maintaining a list of known networks and neighboring routers.
   - Routers use a routing protocol to take into account various factors such as the number of hops in the path, link speed, and link reliability to select the optimal path for data.

Data at the Network layer is referred to as a *packet*.

OSI Layer Facts

Data Link (Layer 2): The Data Link layer defines the rules and procedures for hosts as they access the Physical layer. There are two sublayers: MAC and LLC

1. MAC or physical addressing of hosts on the network
2. How and when devices can transmit on the network medium (media access control and logical topology).
3. How to verify that the data received error free from the Physical layer (parity and CRC).
4. How devices control the rate of data transmissions between hosts (flow control).

Data at the Data Link layer is referred to as a *frame*.

OSI Layer Facts

Physical (Layer 1): The Physical layer of the OSI model sets standards for sending and receiving electrical signals between devices.

- How digital data (bits) are converted to pulses
  - Electrical pulses, radio waves, or pulses of lights.
- Specifications for cables and connectors.
- The physical topology.

Data at the Physical layer is referred to as *bits*.