Module 1: Introduction to Networks

Notes: This summary is made based on lecture notes of CSCI 3171 Network Computing taught by Dr. Srinivas Sampalli in fall 2019.

Network basics

Definition 1.1: A **network** is an interconnected collection of autonomous devices (workstations, laptops, tablets, mobile devices, sensors, etc.) that can

1) Exchange information (text, voice, video, image, sensor data)
2) Use specific protocols (e.g., TCP/IP)
3) Over different media (wireline and wireless)
4) Across different platforms (Unix, Linux, Windows, Mac, legacy systems, etc.)

Classification 1.2: **Network** can be classified as

1) **A Local Area Network (LAN)** is typically a network that connects hosts within an office building or an organization or a campus. The geographical diameter of a LAN is usually less than a few km.
2) **A Metropolitan Area Network (MAN)** connects hosts across a city or across multiple branch offices of an organization. The geographical diameter of a MAN is usually 10's to 100's of kms.
3) **A Wide Area Network (WAN)** is a network that connects hosts anywhere in the world. The Internet is the largest WAN in operation today.

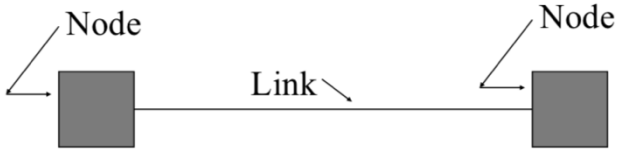
Definition 1.3: A network can be built using two types of basic building blocks.

1) Nodes: hosts (PCs, workstations, servers, audio-video equipment, mobile devices, etc.) or interconnection devices (repeaters, hubs, bridges, switches, routers)
2) Links: twisted pair copper cable, coaxial cable, optical fiber, wireless, etc.

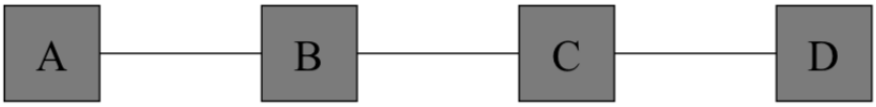
Definition 1.4: **Network topologies** (or configurations) is the different way of putting together nodes and links.

Classification 1.5: There are seven types of topologies.

1) **Two-node point-to-point topology**
   - **Definition 1.6:** **Two-node point-to-point topology** is a simple topology where two nodes are connected by one link. It can serve as a building block for other topologies.

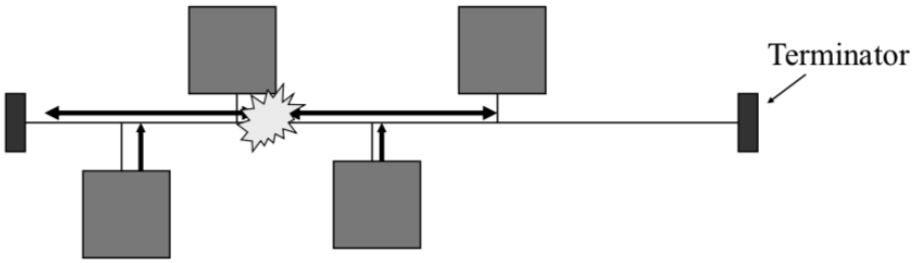


   - **Application 1.7:** It is popular in WANs. For example, two nodes in different cities are connected by a point-to-point topology.
2) **Linear topology**



- **Definition 1.8:** **Linear topology** is a linear fashion of a multiple point-to-point connections.
- **Drawbacks 1.9**
  a) Data transfer between nodes may need to go through other nodes. → Poor fault tolerance because the failure of one link can break the network communication.
  b) The bandwidth of a link is not shared by all nodes.

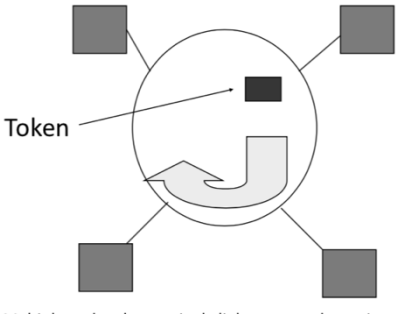
3) Bus topology

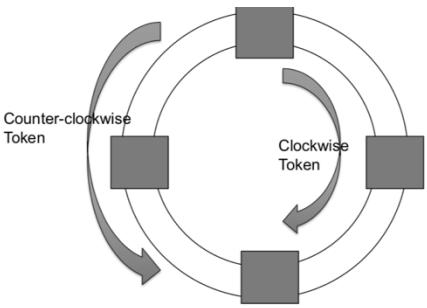


- **Definition 1.10:** **Bus topology** is like linear topology but all nodes share a singe link. The electrical signals from a node travels in both directions along the link. Terminators are devices placed at each end to absorb the signals so that they are not reflected back onto the link.
- **Advantage 1.11:** This topology provides better bandwidth utilization since the link is shared.
- **Disadvantage 1.12:** A problem with this topology is collisions—if two nodes start transmitting simultaneously, the transmission may collide.
  Note: A special *medium access control mechanism* must be incorporated to deal with such collision.
- **Application 1.13:** Earlier LANs were based on this topology. They were called the Classical or Traditional Ethernets.

4) Ring topology

- **Definition 1.14:** Multiple nodes share a single link connected as a ring.
- **Advantage 1.15:** Orderly transmission without collisions by a *token passing mechanism*.
  How does it work?
  Token is a special bit pattern that rotates around the ring. Only the node that captures the token can send the message.
- **Application 1.16:** *The Token Ring Network* is a popular network based on this topology.





5) Dual ring topology

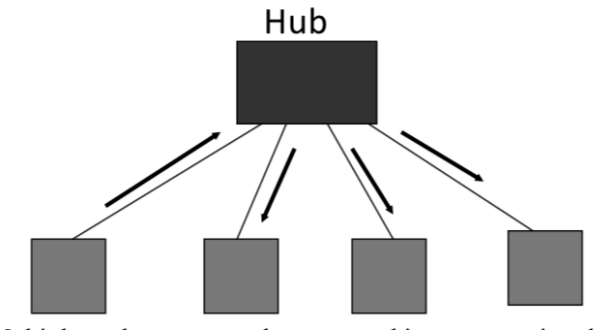
- **Definition 1.17:** Nodes are

interconnected by two rings. One ring circulates a token in the clockwise direction. The other ring circulates another token in the counter-clockwise direction.

- **Advantage 1.18:** The topology provides better fault tolerance than the single ring.
- **Application 1.19:** *The Fiber Distributed Data Interface (FDDI)* was a network based on this topology.

6) **Star topology**

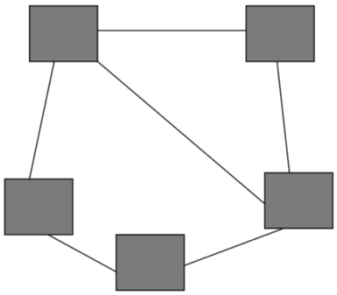
- **Definition 1.20:** Multiple nodes connected to a central interconnection device called a hub. A hub is like a collapsed bus because it serves the same function, broadcasting data to all nodes.



- **Advantage 1.21:** (Over bus topology)
  a) Easier to install than the bus topology.
  b) Has better fault tolerance than the bus topology
- **Application 1.22:** Current LANs or Ethernets are based on this topology.
  Note: In current networks, the hub is typically a switch. This is why current LANs are called *Switched Ethernets*.

7) Mesh topology

- **Definition 1.23:** Multiple point-to-point links connected in an arbitrary topology. If every node is directly connected to every other node, it is a **full mesh**. If some links are not present, then it is a **partial mesh**.



We need to address two problems for building larger networks

How can we increase the capacity of the basic topologies?

Example 1.24: If the length of the link is increased, the signal may get corrupted with noise or the signal level may fail.

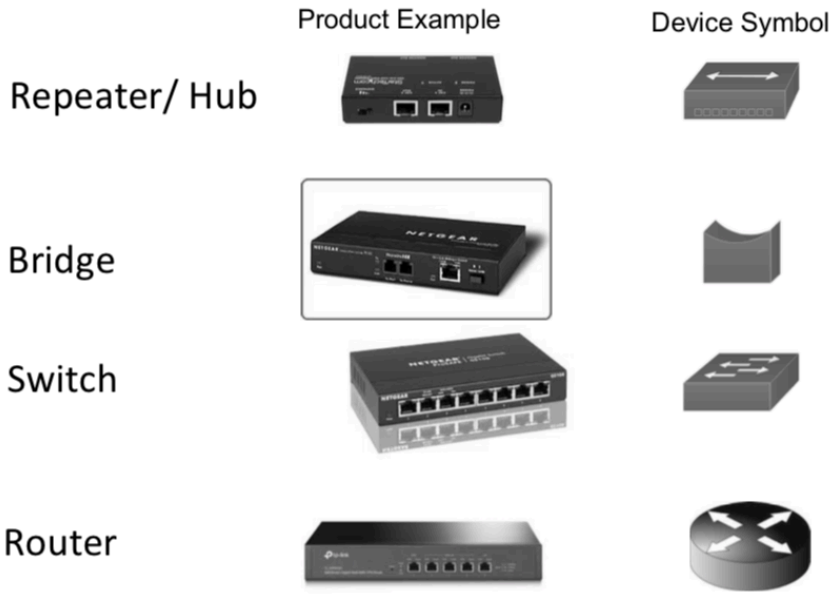
Example 1.25: If the number of nodes is increased in a bus topology, the number of collisions may increase and affect the performance.

How can we interconnect two different topologies and/or different characteristics?

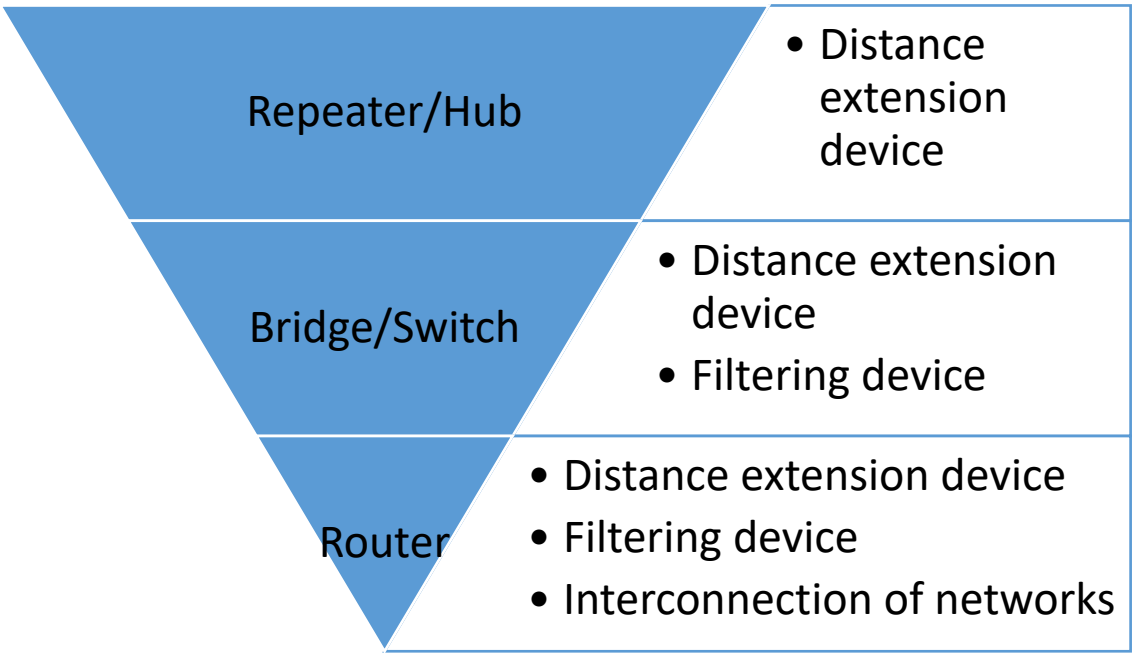
Example 1.26: For building heterogeneous networks, we need to interconnect a bus to a ring, a ring to as star, and so on.

Example 1.27: We will also need to connect networks of different bandwidth.

We can use interconnection devices. They act like nodes in the network topology.



Classification 1.28: Different types of interconnection devises.



1) **Repeater/Hub**
   - **Definition 1.29**
   -

1. Network utility: traceroute
   Traceroute is a network utility that allows you to send management packets to any Internet host (from source to destination across the Internet) and collect statistics about the route and the round-trip time. For mac user, you can run traceroute by entering `traceroute <IP address or URL of a host or a server>` in a terminal window. The traceroute command has a number of

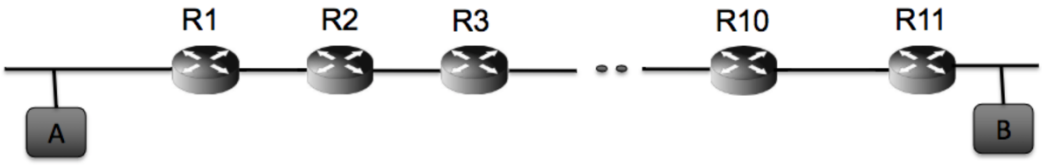
options.

How does traceroute work and what information does it collect?

- traceroute uses a network management packet called ICMP echo request and manipulates a parameter called TTL(time to live) in the packet.
- Normally the TTL value (default) is 64 when a packet starts its journey.
- Each router along the path decrements TTL by 1.
- If TTL = 0, the packet gets discarded and the node that discards the packet sends an ICMP Time Exceeded packet back to the source.

Why do we need TTL?

- TTL prevents a packet without a proper address from endlessly looping on the Internet.



Mechanism

- traceroute first sends an ICMP echo request packet with TTL set to 1.
- The first router along the path decrements TTL by 1.
- Thus the TTL becomes 0. The router R1 discards the packet and sends a reply back to the source.
- The source will record the IP address of the sender (R1) and also the round trip time.
- …
- The source then sends an ICMP echo request packet with TTL set to $i(2 \leq i \leq 64)$.
- This packet get discarded by the ith router Ri. Then the source is able to collect information about Ri along the path.
- It continues to do this until the packet reaches the destination.
- For every hop, it sends three packets for getting the average round trip time.

What is a hop?

- A hop is a computer networking term that refers to the number of routers that a packet (a portion of data) passes through from its source to its destination.
- Sometimes a hop is counted when a packet passes through other hardware on a network, like switches, access points, and repeaters. This isn't always the case and it depends on what role those devices are playing on the network and how they're configured.

What's the value in knowing a path's hop count?

- Every time packets flow from one computer or device to another, like

from your computer to a website and back again (i.e. viewing a web page), a number of intermediate devices, like routers, are involved.

- Each time that data passes through a router, it processes that data and then sends it along to the next device. In a multi-hop situation, which is very common on the internet, several routers are involved in getting your requests where you wanted them to go.
- That processing-and-passing-along process takes time. More and more of that happening (i.e. more and more hops) adds up to more and more time, potentially slowing down your experience as the hop count increases.
- There are many, many factors that determine the speed in which you can use certain websites or web-based services, and hop count isn't the most important, but it often plays a part.
- A lower hop count also doesn't necessarily mean that the connection between two devices will be faster. A higher hop count via one path might perform better than a lower hop count via a different path thanks to faster and more reliable routers along the longer path.

How do Internet packets travel across oceans?

- Via undersea cables.

The route from a source to a destination across the internet may not be the same path for each transmission. The path from a source to a destination across the Internet is not necessarily the shortest.

Reference

Fisher, T. (2019, August 19). What Are Hops & Hop Counts? Retrieved September 28, 2019, from https://www.lifewire.com/what-are-hops-hop-counts-2625905.