Network Ownership, Service Paradigm, and Performance

- by Ntalasha

Network Ownership

- ## Private network
  - ○ owned by individual or company
  - ○ To form a private WAN, a corporation must lease connections between its sites from public carriers.
  - ○ No other company will have access to the wires or the data.

- ## Public network
  - ○ owned by public carriers such as phone companies and service providers.
  - ○ WAN service is available to the public
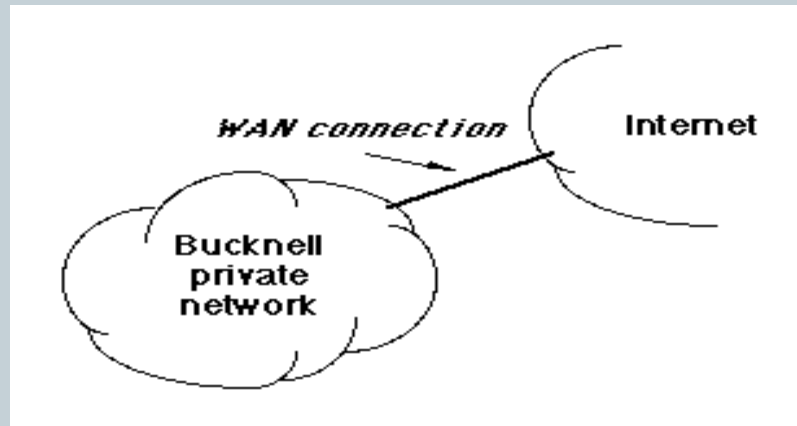 - ○ data transferred is still private.

Private network

- Often LAN technology
- Multiple LANs in a building or campus, linked together
- Sometimes called *intranet*

Private network architecture

- Operates autonomously from other networks (e.g., Internet) Usually includes one or few closely managed external connections May restrict access at connections
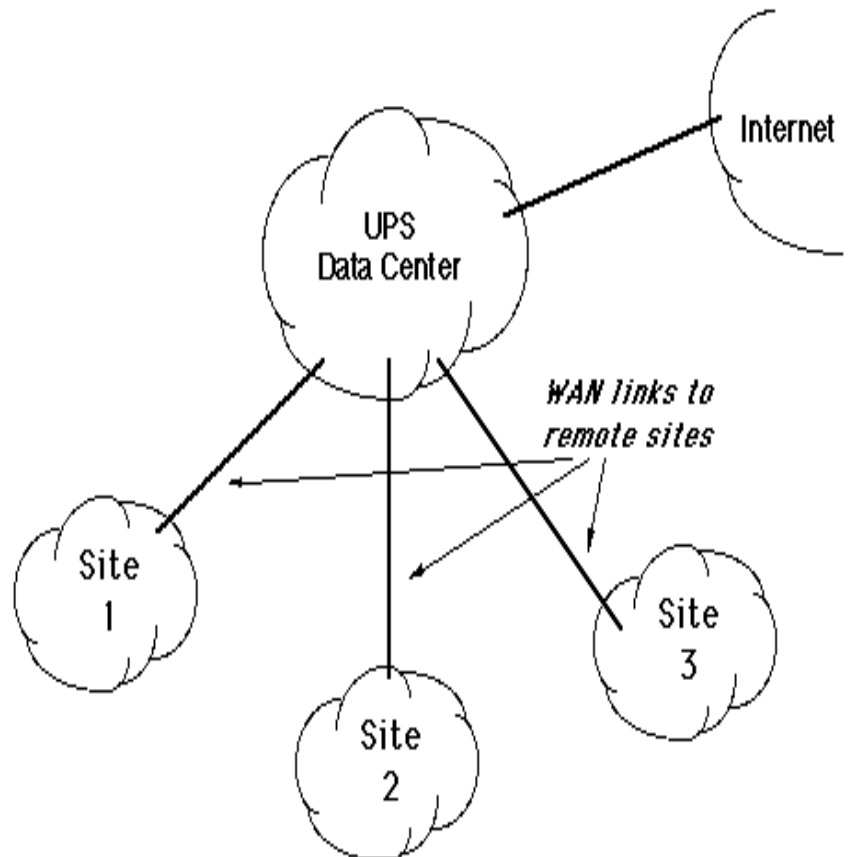
Managing private networks

- Organization buys own equipment
- Hires staff to design, implement, maintain and upgrade network
- Responsible for all network management

Extending private networks

- Large organizations may have multiple buildings or campuses

- Can only install cables on own property

- May contract for leased lines from common carrier

Advantages of a Private Network

- Owner has complete control
- Owner sets policies that determine how and when the network can be used as well as which computers are allowed to connect
- Owner can guarantee that the network is isolated from computers outside the organisation and that a computer never accidentally contacts a computer at another organisation

Public Network

- Operated by common carrier

- May be telephone company or other organization that builds network out of leased lines

- Multiple organizations subscribe and connect Data transits public network to other organizations
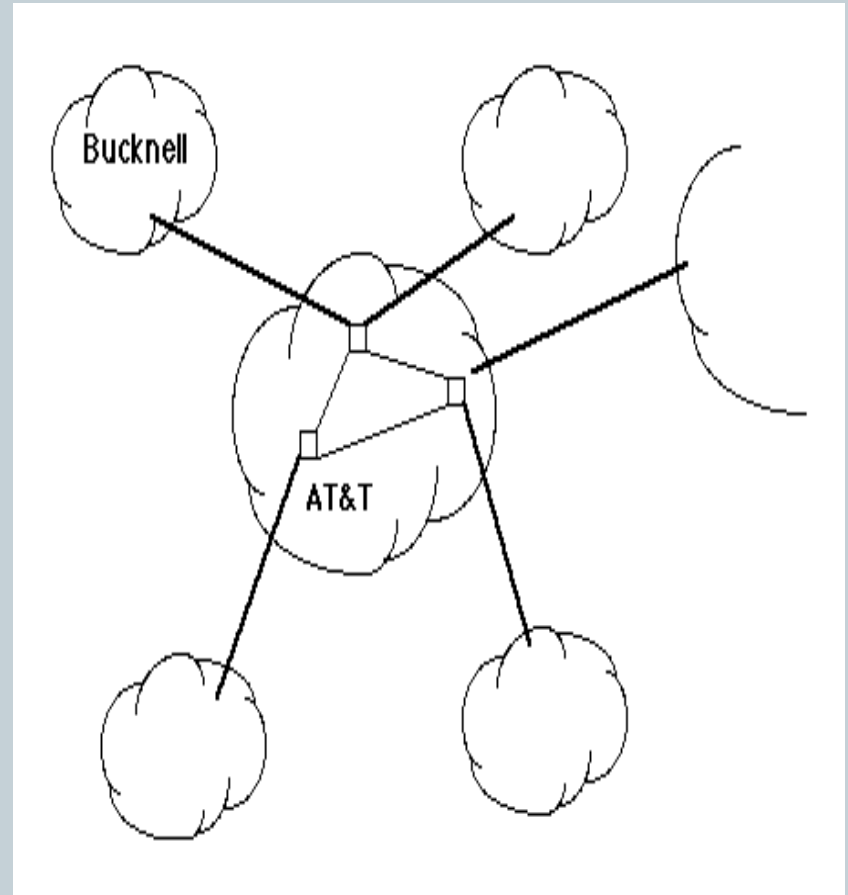
Advantages of a Public Network

- flexibility and the ability to use state-of-the-art networking without maintaining technical expertise.

- A public network is flexible because arbitrary subscribers at arbitrary locations can connect to the network.

- Furthermore, connections between a computer owned by one organisation and a computer owned by another can be made or broken the same way a public telephone system allows voice connections to be made or broken

Virtual Private Network

- *VPN* (Virtual Private Network) combines features of private and public networks
  - Limited to single organization
  - Uses public network for connectivity
- Connections, sometimes called *tunnels*, connect sites
  - Each site sees tunnel as point-to-point link direct to another site
  - Cannot be access by other users of public network

Network Service Models

- Connection-oriented
- similar to telephone system; endpoints establish and maintain a *connection* as long as they have data to exchange
- Connectionless oriented
- similar to postal system; endpoint puts data to send into a *packet* and hands to network for delivery

Connection-oriented Service

- circuit switching eg. Frame Relay,ATM
  - analogous to telephone system where a connection must be made between two computers prior to data transfer
  - provides stream interface for computer. Application need not know about packet size.
  - Provides ease of accounting and ability to inform communicating computers immediately when a connection breaks
  - uses connection identifiers instead of address of remote destination after a connection is established.
  - ATM's connection identifier consists of a 12-bit virtual path identifier(VPI) and a 16-bit virtual circuit identifier(VCI).
  - VPI specifies a switch while VCI specifies a computer connected to the switch

Connection-oriented Service (cont.)

- ## Connection Duration and Persistence
  - Switched connection is flexible because it can be created and changed electronically eg frame relay's and ATM's switched virtual circuits(SVC).
  - Permanent connection remains in place after reboot and crashes; availability is guaranteed eg frame relay's and ATM's permanent virtual circuit (PVC)

Connectionless Service

- Packet switching
  - eg. SMDS, Ethernet, Token ring, FDDI, LocalTalk
- analogous to postal mail system.
- each packet must be labeled with destination's address
- failure in a connectionless system may go unnoticed
  - computer may still be sending packets after a failure occurs
- advantage is less initial overhead
  - data is sent immediately without waiting for connection.

Comparions

- <u>Connection-oriented</u>: accounting easier, application can learn of network problems immediately
- <u>Connectionless</u>: less overhead, easier to implement network

Examples of service paradigms

- Technology comparisons
- *Fiber Distributed Data Interface*
- Switched Multi-megabit Data Service

Technology	Connection-Oriented	Connectionless	used for LAN	used for WAN
Ethernet		•	•	
Token Ring		•	•	
FDDI		•	•	
Frame Relay	•			•
SMDS		•		•
ATM	•		•	•
LocalTalk		•	•	

Network Delay Types

- Propagation delay
  - function of media and distance
- Switching delay
  - occurs in hubs, bridges or packet switches(router)
- Access delay
  - refers to delay in accessing media eg CSMA/CD or waiting for token in token ring.
- Queuing delay
  - occurs in store-and-forward WANs.

Network Throughput

- aka network capacity

- measured in bits/s

- number of bits that can enter the network per unit time.

Throughput measures rate at which data can be transmitted in network

300 bps (bits per second) - old modems

1 gps (gigabit [10^9] bits per second) - fastest today

Bandwidth - limit of underlying hardware

Effective throughput - real data delivery

Relationship between delay and throughput

- As throughput approaches theoretical maximum, delay increases
- Excessive traffic known as *congestion*
- Effective delay, *D*, can often be approximated:

- $D = D_0 / (1 - U)$
- If D_0 denotes the delay when the network is idle, and U is a value between 0 and 1 that denotes the current *utilisation*, the effective delay D
- *Throughput and delay are not completely independent. As traffic in a computer network increases, delays increase; a network that operates at close to 100% of its throughput capacity experiences severe delay.*

-

- *Throughput and delay are not completely independent. As traffic in a computer network increases, delays increase; a network that operates at close to 100% of its throughput capacity experiences severe delay.*

-

Congestion

- occurs when there is heavy network traffic
- causes longer queues in routers
- Packets may be dropped

Delay-Throughput Product

- Delay-throughput product = T * D
  - T is throughput(Mb/sec)
  - D is delay(sec)
- T * D measures the number of bits in transit in the network.