CISSP® 2015

Domain 4: Communication & Network Security

V1

Domain 4: Communication & Network Security

- Overview cover:
  - OSI,
  - TCP/IP,
  - Different Protocols,
  - Wireless,
  - Devices,
    - Switching
    - Routing
  - Mobile device
  - Media,
  - Endpoint,
  - Voice,
  - Remote Access,
  - VPN,
  - Attacks

A.1 Open Systems Interconnection Reference Model (OSI)

- Developed by ISO, international standard, 1984, ISO standard 7498
- Abstract or academic framework, not practical framework
- important guideline to vendor, engineer, developer..
- Segment into **7 layers**; each layer has its own **responsibilities** regarding how two computer communication over network
- Open network, no vendor own
- **Encapsulation**: as go down the layer stack, data grows until to Physical level, then send to another system, then reverse encapsulation.
- Each layer has a special interface to interact with 3 other layers (1) above (2) below and (3) same layer in target system
- In form of **header and trailer** of packet

Encapsulation

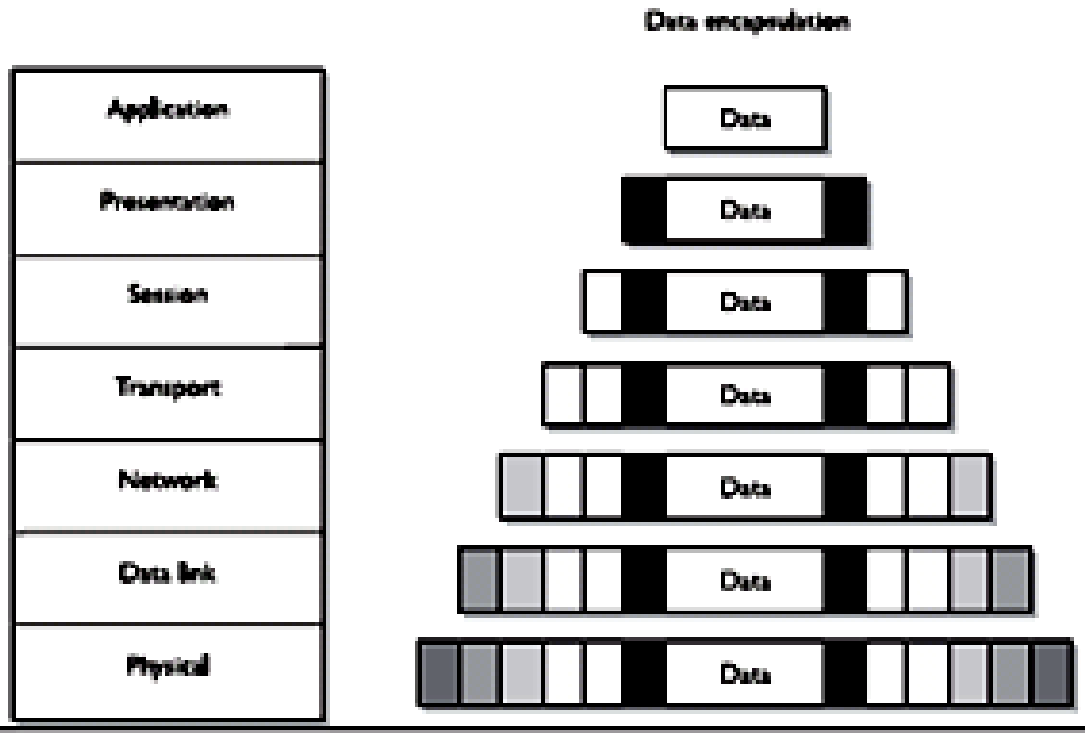
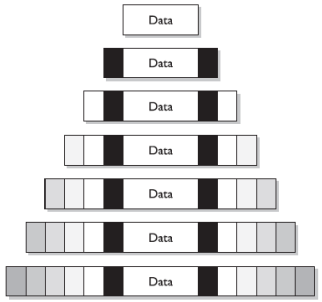


Figure 7-2 Each OSI layer adds its own information to the data packet.

OSI

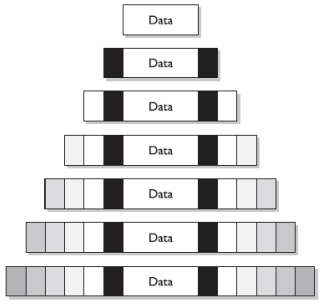
- **Application Layer (7)**
  - closest to user
  - not the actual application, but the protocol that support the application
  - example protocol in this layer:
    - **Simple Mail Transfer Protocol (SMTP)**
    - **Hypertext Transfer Protocol (HTTP)**
    - Line Print Daemon (LPD)
    - **File transfer Protocol (FTP)**
    - **Telent**
    - Trivial File Transfer (TFTP)
  - Email client send message to SMTP and SMTP adds its information to the user's information and passes it down to Presentation Layer



OSI

- **Presentation Layer (6)**
  - this layer provide a common means of **representing** data
  - translate data to a standard format regardless of system or application
  - example: a word 2000 document send to user B who use Open Office, User B still can open the file, because this layer translate the file to ASCII, so the user b computer knows it open this type of file with Open Office.
  - This layer also handle data **compression and encryption** issues. This layer will provide necessary information for receiver to decompress and decrypt the data.
  - Presentation layer standards:-
    - **ASCII, EBCDIC,** TIFF, **JPEG, MPEG,** MIDI

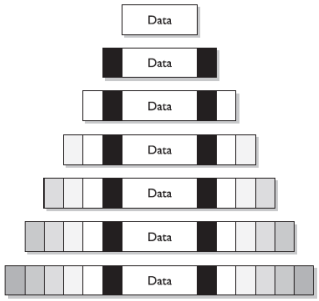
OSI



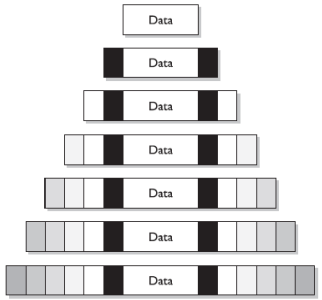
- **Session Layer (5)**
  - when **two applications** need to communicate, a connection session is needed
  - this layer is responsible for (1) establishing a connection between two applications, (2) maintaining it during data transfer and (3) controlling the release of this connection.
  - It also provide **session restart and recovery** if necessary
  - Also called dialog management
  - Different modes: Simplex (one direction only), Half-duplex, full-duplex
  - This layer control application-to-application communication
  - Some protocol work at this layer:
    - Network file system (NFS)
    - Structured Query Language (SQL)
    - NetBIOS
    - Remote Procedure Call (RPC)

OSI

- **Transport Layer (4)**
  - handle **computer-to-computer** communication, agree on how much information, how to verify, how to determine data lost.
  - This handshaking process to agree these parameters at Transport Layer
  - These parameter help provide **reliable data transfer, error detection, correction, recovery and flow control**
  - May be from many different application and assembles the data into a stream to be transmitted over the network (analogy: a bus of applications)
  - Diff to Session Layer: Session layer at application level; Transport Layer at computer level
  - Main protocols in this layer
    - TCP
    - User Datagram Protocol (UDP)
    - Sequenced Packet Exchange (SPX)



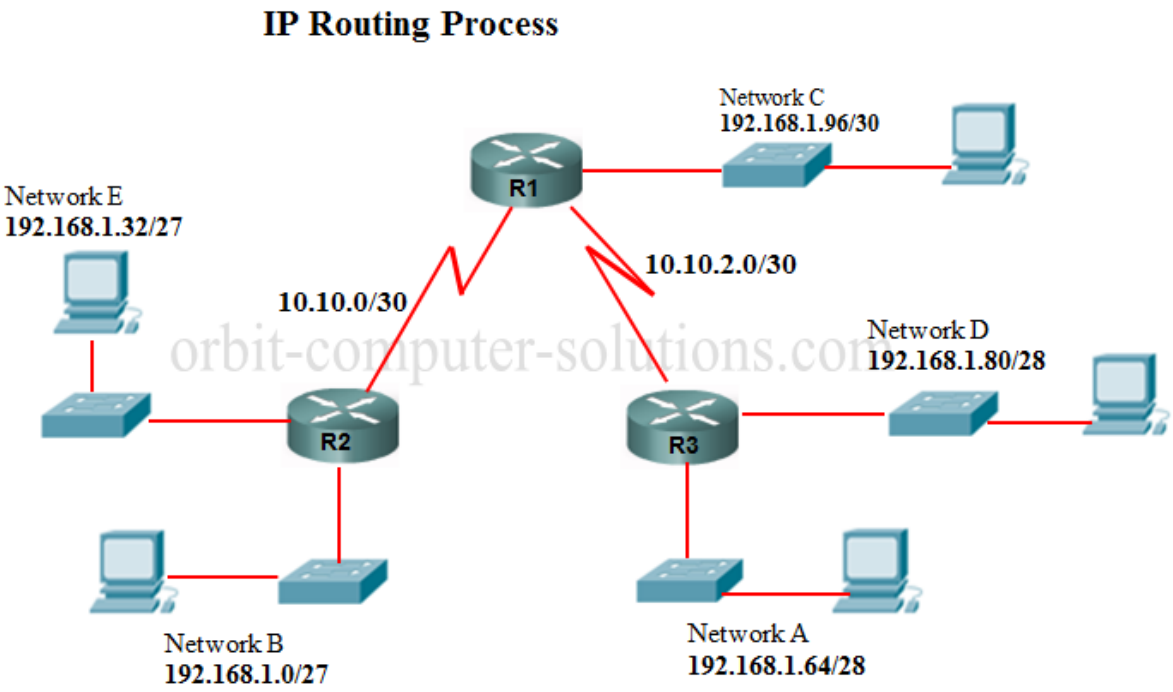
OSI



- **Network Layer (3)**
  - Insert information into packet's header for **address and routing**
  - The protocol must determine the **best path**
  - Routing protocols build and maintain their routing tables at this layer
  - Protocol in this layer
    - **IP**
    - Internet Control Message Protocol (ICMP)
    - Routing Information Protocol (RIP)
    - Open shortest Path First (OSPF)
    - Border Gateway Protocol (BGP)

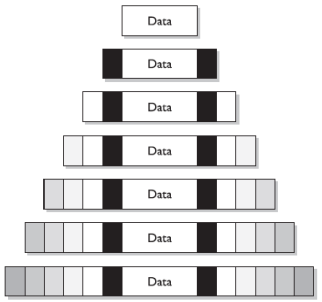
Routing Basics

- Host delivers packets to directly connected machines.
- Host sends packet that cannot be delivered directly to router.
- Routers forward packets to other routers. Final router delivers packets directly.



OSI

- **Data Link Layer (2)**
  - to translate into LAN or WAN technology binary format for proper line transmission
  - LAN and WAN use different protocol (Ethernet, Token ring etc.), NIC, cable and transmission methods
  - Also manage to reorder frames that are received out of sequence.
  - Two sublayers:
    - **Logical Link Control** (LLC): IEEE 802.x for diff protocols, such Ethernet, token ring etc.
    - **Media Access control** (MAC): provide addressing to communicate within network
  - Protocol work in this layer
    - Serial Line Internet Protocol (SLIP)
    - Point-to-point Protocol (PPP)
    - Reverse Address Resolution Protocol (RARP)
    - Layer 2 Forwarding (L2F)
    - Layer 2 Tunneling Protocol (L2TP)
    - Integrated Services Digital Network (ISDN)



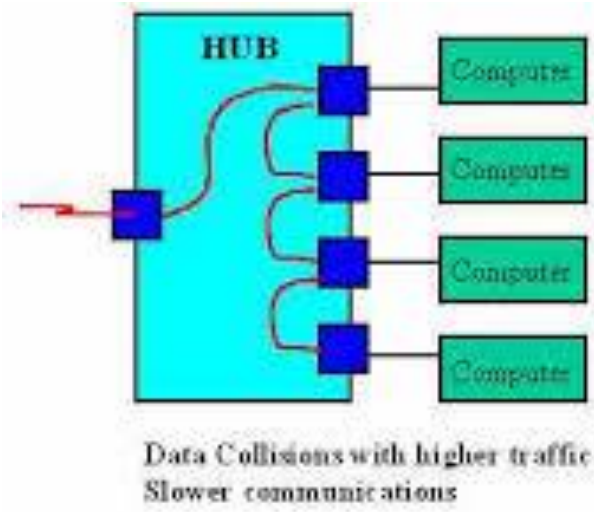
OSI

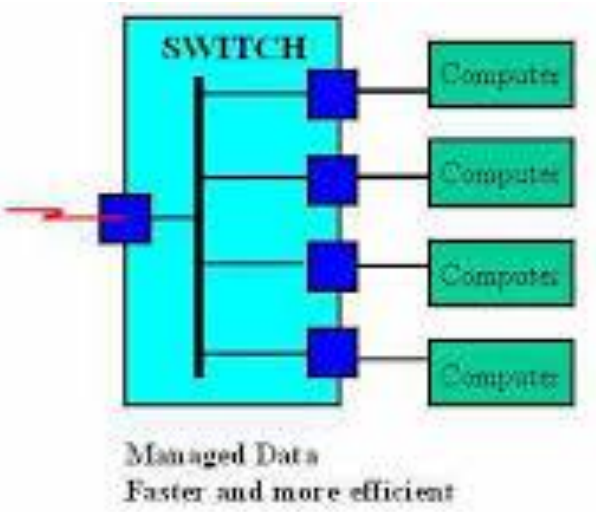
```
C:\Documents and Settings\Vien>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : Dominic
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Conn
on
        Physical Address. . . . . . . . . : 00-0D-60-CA-88-70

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 11a/b/g Wireless CardBus Adapter
        Physical Address. . . . . . . . . : 00-20-E0-37-00-8B
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.197
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.8
        DHCP Server . . . . . . . . . . . : 192.168.1.8
        DNS Servers . . . . . . . . . . . : 192.168.1.8
```

MAC communication: HUB vs. Switch

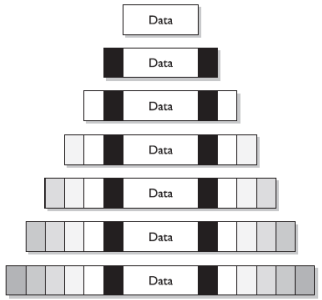
- A HUB does understand MAC address, so have to send packet to all ports (or all computers).
- The final control is done by computer's NIC

- A SWITCH can memorize the computer's MAC by port.
- Computer A can send to B without affecting other computers.
- Two modes:
  - Store-and-forward: Cyclic Redundancy Check
  - Cut-Through: no checking





OSI

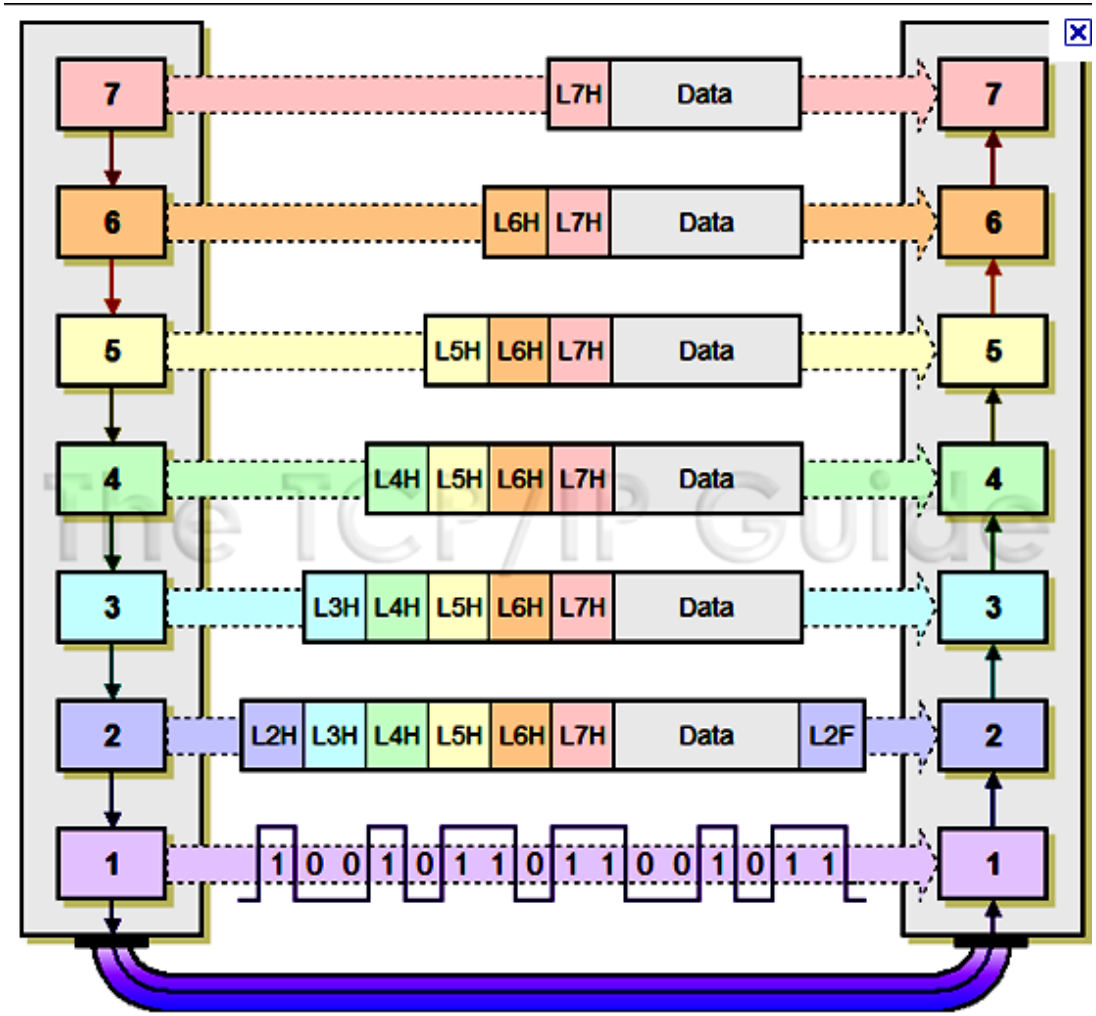


- **Physical Layer (1)**
  - converts bit into **voltage** for transmission
  - voltage schemes are **different** from LAN and WAN; from different lines, modem, NIC etc. >> Driver
  - this layer controls synchronization, data rate, line noise, medium access
  - specify timing of voltage change, voltage level etc.
  - Standard
    - High-speed serial interface (HSSI)
    - X.21
    - EIA/TIA-232 and EIA/TIA-449

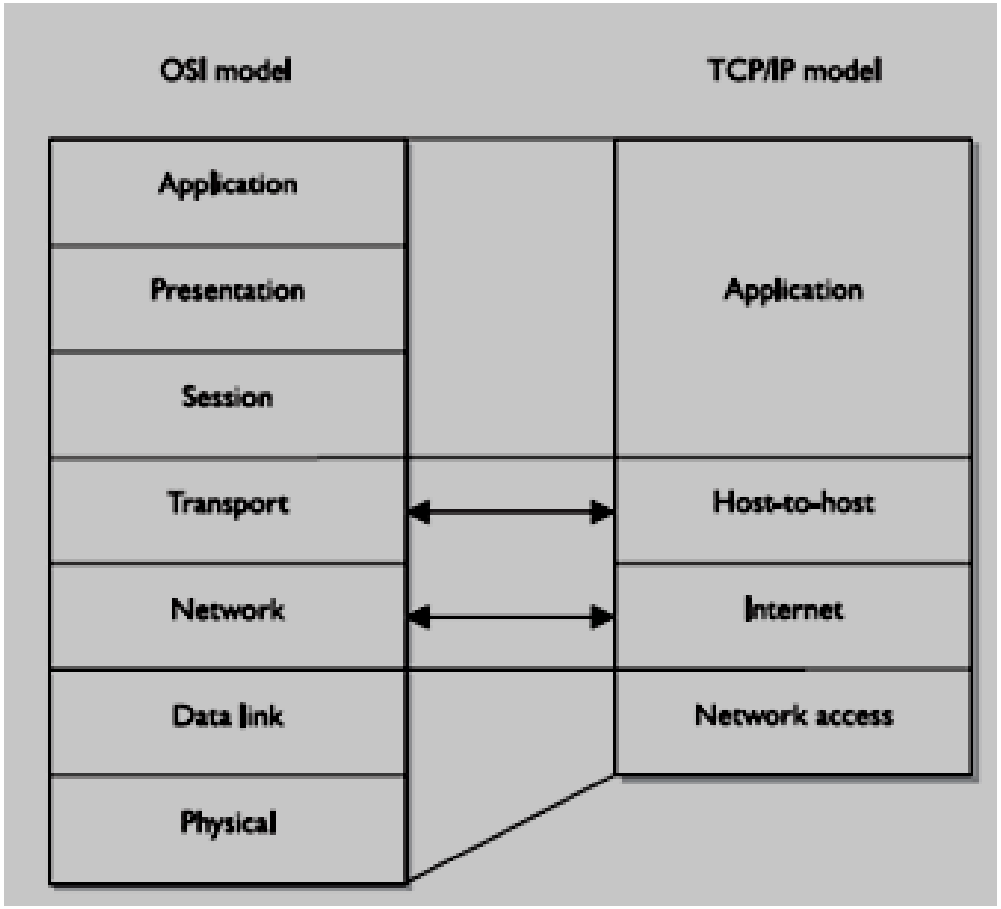
OSI

- **Tying the layers together**
  - diff type of devices and protocol work at different parts of this seven-layer
  - Computer: can work each of 7 layer
  - Router: up to Network Layer (3)
  - Bridge: update Data Link layer (2)
  - Repeater or Hub: up to Physical layer (1)
  - Switch: normally layer 2, but can be 2 to 7
  - Gateway: can be any layer

Encapsulation and Reverse-Encapsulation



OSI vs. TCP/IP



OSI vs. TCP/IP Models

A2. IP Networking

- **IP Addressing**
  - IP is a numerical identification and **logical address**;
  - Currently IPv4: 32 bit; start to run out;
  - The private addresses used on private network and often use Network Address Translator (NAT) to connect to the global public internet.
  - **Private Internet Protocol (IP) Network:**
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255

Class	Range of First Octet	Number of Octets for Network Number	Number of Hosts in Network
A	1 – 127	1	16,777,216
B	128 – 191	2	65,536
C	192 – 223	3	256
D	224 – 239	Multicast	
E	240 – 255	Reserved	

A2. IP Networking

- **IPv6**
  - 128 bit; example: **2001:0db8:85a3:08d3:1319:8a2e:0370:7344**
  - restrict specific address for file server or file and print sharing,
  - allow for Quality of Service (QoS)
  - **An improvement of Security:** can distinguish type of devices

TCP/IP

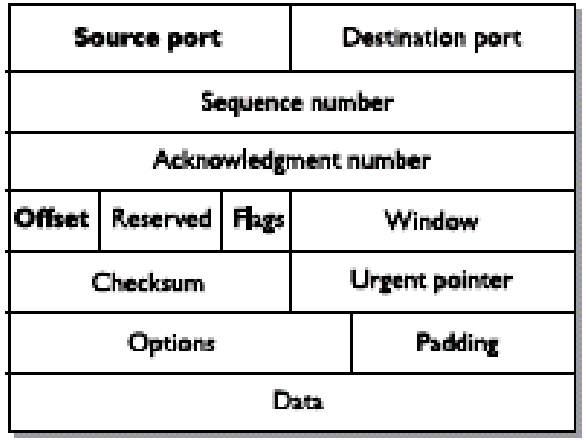
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Govern the way data travel from one device to another
- **IP**
  - Network layer
  - Support internetwork addressing and packet routing
  - **Connectionless** protocol
  - Contain source and destination IP Addresses
  - Analog: Data=letter; IP=addressed envelope; Network=Postal system
- **TCP**
  - Transport layer
  - **Reliable and connection-oriented** protocol
  - Ensure packet are delivered to destination computer
  - Include ability to identify issue and resend, sequencing, flow and congestion control, error detection and correction
  - Will do handshaking
  - Full-duplex
  - Requires a **lot of system overhead**

UDP

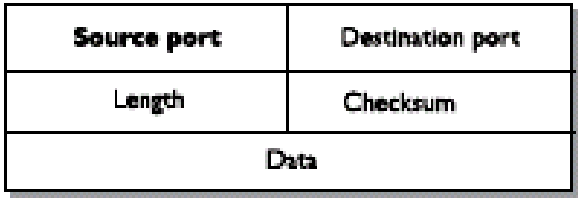
- **UDP** (User Datagram Protocol)
  - Transport Layer
  - **Best-effort** and **connectionless**
  - No packet sequencing, not flow & congestion control,
  - Just send without first contacting and does not know whether the packet was received properly or dropped

TCP and UDP selection

- developer can choose
- Many times, **TCP** is the choice, example email because it must make sure the data are delivered.
- If not critical, **UDP** is a better choice, example sending status info to all listening nodes on the network. It will be resent every 30 minutes anyway. It is faster and requires fewer resources
- Both use port to communicate with upper OSI layers and keep track various conversation simultaneously
- **Port**: software drive; 0-1023 is "well-known ports (telnet 23; smtp 25, http 80); 1024-49151: registered ports; 49152 – 65535 temporary ports



TCP format



UDP format

Figure 7-12 TCP carries a lot more information within its segment format because it offers more services than UDP.

TCP Handshake

- **Also Called "3-ways Handshake"**

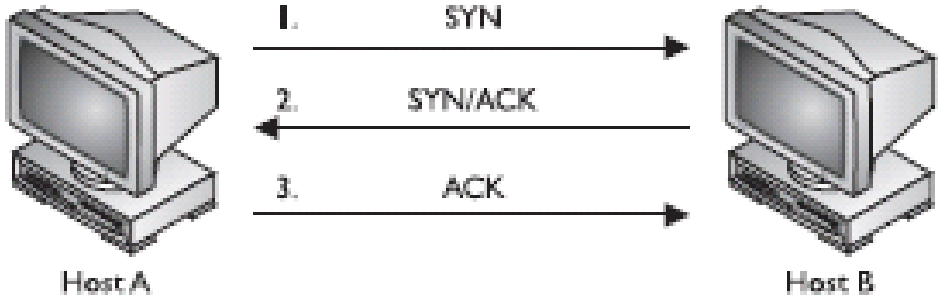
  (1) SYN (request for connection)

  (2) SYN/ACK (received request and ready)

  (3) ACK (acknowledged, start connection)

  - After Handshaking, agree certain parameters, data flow, windowing, error detection and options

Figure 7-13
The TCP three-way handshake

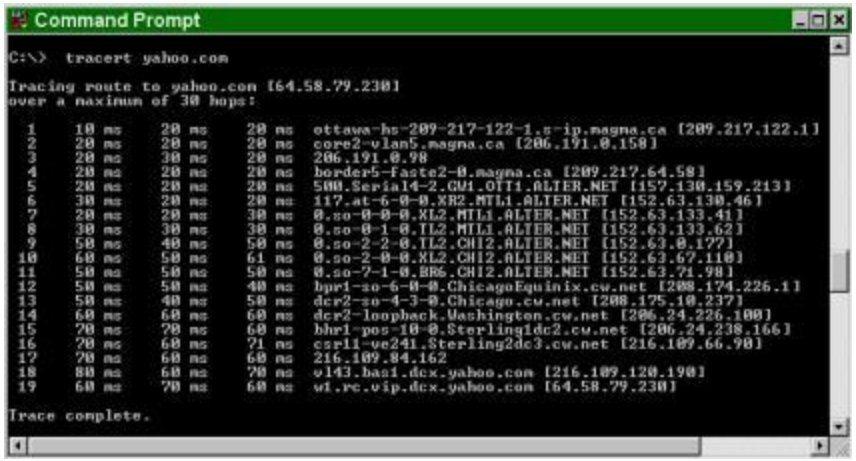


Intranets and Extranets

- **Intranet**: internal web site inside the company's network
- **Extranet**: extends outside the bounds of the company's network to enable two or more companies to share common information and resource; for example **business partners**; use Electronic Data Interchange (EDI); if implement over Internet, require configured **VPN and security policy**.

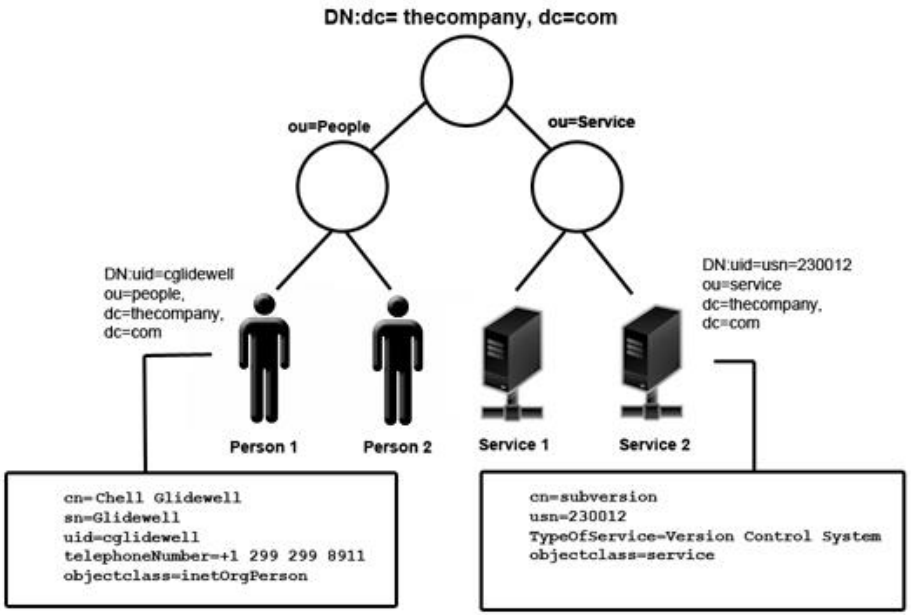
Other Protocols

- **Dynamic Host Configuration Protocol (DHCP):** dynamically assign IP address when OS start
- **Internet Control Message Protocol (ICMP):** Network messenger (eg. Ping), ignorance from administrator
  - **Ping of Death:** OS will die if receive ICMP packet > 65536 bytes
  - **ICMP Redirect Attack**: ICMP to tell a victim host the default route is attacker's PC and attacker forward the traffic to router, then victim will not know all traffic route thru attacker's pc
- **Traceroute Exploitation:** to gather network and routing information



Other Protocols

- **Ping Scanning:** attacker uses tool to ping all IP in a range to find out valid IP or host
- **Remote Procedure Call**: to allow executing objects across hosts; **Risks**: weak authentication, plaintext, privilege escalation
- **Lightweight Directory Access Protocol (LDAP)**
  - Client/server-based directory **query** protocol
  - Loosely based **X.500**
  - To specific entity
  - **Risks**: cleartext communication, weak communication
  - **Control**: SSL



Other Protocols

- **Domain Name Service (DNS)**
  - Most useful network function to **translate** host name (or domain) to IP which is not user-friendly. External & Internal
  - **Risk:** DNS poisoning, attack end user communication without attacking endpoint
  - **Control**: DNSSEC: introducing authentication

Location	Type	FQDN	IP address	Port	Maps to/Comments
Consolidated Edge					
External DNS	A	SIP.Domain.com	12.34.56.78		SIP Access Edge Server external interface
	A	WebConf.Domain.com	12.34.56.79		Web Conferencing Edge Server external interface
	A	AV.Domain.com	12.34.56.80		A/V Edge Server external interface
	SRV	_sip._tls.Domain.com	SIP.Domain.com	443	Required for automatic configuration of Lync 2010 clients to work externally
	SRV	_sipfederationtls._tcp.Domain.com	SIP.Domain.com	5061	Required for automatic DNS discovery with Federated partners
Internal DNS	A	LyncEdge.domain.com	12.34.56.81		Consolidated Edge Server internal interface
Reverse Proxy					
External DNS	A	WebFarm.domain.com	12.34.56.82		Front End pool external web services FQDN. Used to publish Address Book Service, Distribution Group Expansion, and Conference content, Lync Web App
	A	dialin.Domain.com	12.34.56.82		Dial-in Conferencing published externally
	A	meet.Domain.com	12.34.56.82		Conference published externally

	A	B	C	D	E
1	name	ip	type	zone	dnsserver
2	Server01	192.168.1.10	A	domain.local	dnsserver.domain.local
3	Server02	192.168.1.11	A	domain.local	dnsserver.domain.local
4	Server03	192.168.1.12	A	domain.local	dnsserver.domain.local
5	Server04	192.168.1.13	A	domain.local	dnsserver.domain.local
6	Server05	192.168.1.14	A	domain.local	dnsserver.domain.local
7	Server06	192.168.1.15	A	domain.local	dnsserver.domain.local
8	Server07	192.168.1.16	A	domain.local	dnsserver.domain.local
9	Server08	192.168.1.17	A	domain.local	dnsserver.domain.local
10	Server09	192.168.1.18	A	domain.local	dnsserver.domain.local
11	Server10	192.168.1.19	A	domain.local	dnsserver.domain.local
12	Server11	192.168.1.20	A	domain.local	dnsserver.domain.local
13	Server12	192.168.1.21	A	domain.local	dnsserver.domain.local
14	Server13	192.168.1.22	A	domain.local	dnsserver.domain.local
15	Server14	192.168.1.23	A	domain.local	dnsserver.domain.local
16	Server15	192.168.1.24	A	domain.local	dnsserver.domain.local
17	Server16	192.168.1.25	A	domain.local	dnsserver.domain.local
18	Server17	192.168.1.26	A	domain.local	dnsserver.domain.local
19	Server18	192.168.1.27	A	domain.local	dnsserver.domain.local
20	Server19	192.168.1.28	A	domain.local	dnsserver.domain.local
21	Server20	192.168.1.29	A	domain.local	dnsserver.domain.local
22	Server21	192.168.1.30	A	domain.local	dnsserver.domain.local

Other Protocols

- **Vendor products:**
  - **Network Basic Input Output System (NetBIOS)**
  - **Network Information Service NIS, NIS+**
  - **Common Internet File System (CIFS)**
  - **Server Message Block (SMB)**
  - **Network File System (NFS)**
- **Simple Mail Transfer Protocol (SMTP)**
  - **Risk:** Lack of authentication and encryption
- **Enhanced Simple Mail Transfer Protocol (ESMTP)**
  - Address shortcoming of SMTP

Other Protocols

- **File Transfer Protocol (FTP)**
  - **Risks**: plaintext, weak authentication
  - **Control:** Secure FTP, over Secure Shell (SSH)
- **Hypertext Transfer Protocol (HTTP)**
  - **Risks:** plaintext, no encryption
  - **Controls:** HTTPS, Content Filtering

Questions

Which best describes the IP protocol?

A. A connectionless protocol that deals with dialog establishment, maintenance, and destruction

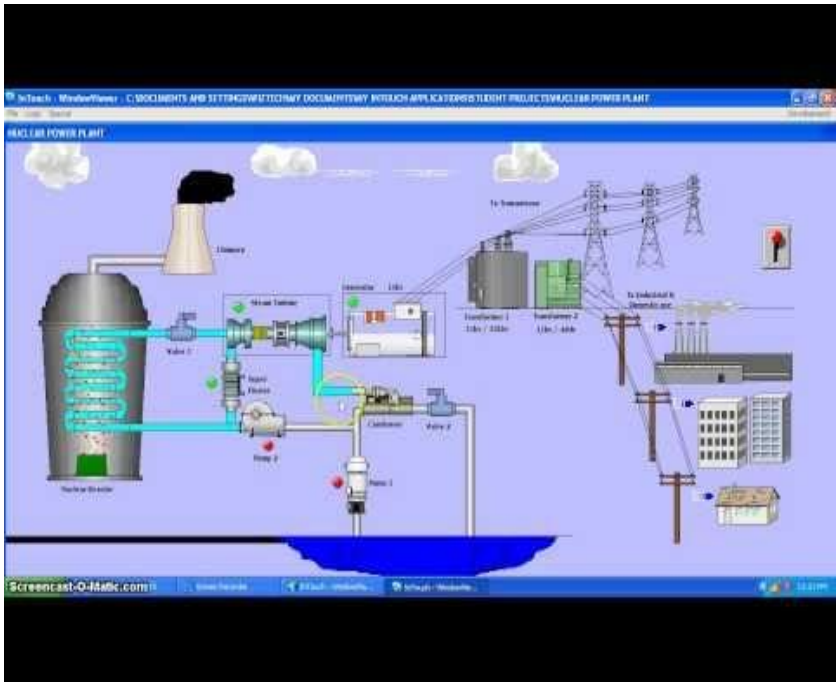
B. A connectionless protocol that deals with the addressing and routing of packets

C. A connection-oriented protocol that deals with the addressing and routing of packets

D. A connection-oriented protocol that deals with sequencing, error detection, and flow control

A3. Implication of multilayer protocols

- **Why Multilayer:** looking for functionality, convenience, remote control, industry specific, but not security
- **Example of Multilayer**:
  - **ICS**: Industrial Control System
  - **SCADA**: Supervisory Control And Data Acquisition
- **Industries:** Energy, Water, Health
- **Security concerns**:
  - Protocol moves from proprietary to more **standardized and open**.
  - The latest generation connects to **Internet**
  - Diversify suppliers
  - **High impact** in public health and safety

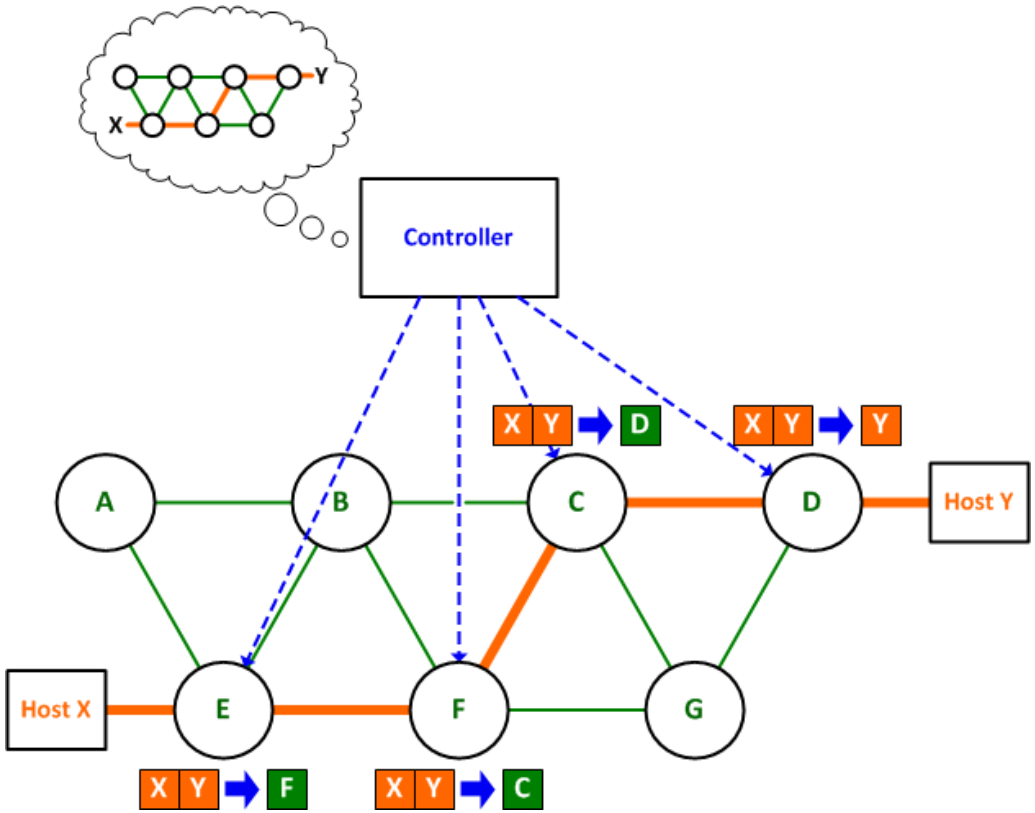


A4. Converged Protocols

- ***Convergence*** is integration of two or more **different** technologies in a **single** device or system.
- **Examples:**
  - **Mobile phone:** can make call and take picture
  - **FCoE**: Fibre Channel over Ethernet
  - **iSCCI**: Internet Small Computer System Interface → Storage consolidation, Disaster Recovery
  - **MPLS**: Multi-Protocol Label Switching: Label can switch and route and is called 2.5th layer
  - **VoIP**: Voice over Internet Protocol

A5. Software-Defined Network (SDN)

- SDN entails the **decoupling** of the control plane from the traditional **forwarding plane** (which each node in the network making its own forwarding decisions) and offloads its functions to a **centralized controller** (likely running on commodity server **hardware**), effectively & efficiency.



A6. Wireless Networks

- **Wireless Communications**
  - via **radio waves** through air and space
  - **frequency**: higher frequency can transmit more data, but shorter distance. Free and legal: 2.4GHz, for example
    - **802.11b**: first extension, **11Mbps**, **2.4GHz, 140m outdoor**
    - **802.11a**: **54Mbps**, **5GHz**, **50m**, Legal in US, but not all
- **Types of Wireless Networks**
  - **Wi-Fi**: **IEEE 802.11** (Institute of Electrical and Electronics Engineers) and extension, 802.11i is WPA2 and secure
  - **Bluetooth**:
    - IEEE 802.15; 1-3Mbps; 10 meters; **2.4GHz**
    - security risk: transferring unprotected data in a public area; **Bluejacking**: someone sends information (say business card) to the Bluetooth enabled device.
  - **WiMAX**: wider area, 6-30Mb, Solution to providers

A6. Wireless Networks

- **Types of Wireless Networks**
  - **Wireless PAN:** Personal reachable, mainly Bluetooth & invisible infrared light, eg. Digital camera connect to PC
  - **Wireless LAN:** WLAN in IEEE 802.11 and extensions, 802.11i addresses security issues
  - **Wireless MAN:** Wireless metropolitan area network, eg. WiMAX or Microwave
  - **Wireless WAN:** cover large area, from city to city, using parabolic dish on 2.4GHz with supplement of photovoltaic solar panel or wind system to renew energy
  - **Cellular Network:** a fixed-location transceiver serves radio network over land area called cell. Cells can join togather form wider geographic area, eg. GSM, PCS
  - **Wireless Mesh Network:** in mesh topology, can “self-heal”, automatically re-routing for a failed node.

Wireless Technologies

- **Orthogonal Frequency Division Multiplexing (OFDM): Spread Spectrum** to subdivide frequency without interfering, two kinds below

1. **Frequency Hopping Spread Spectrum (FHSS)**
   - **one communication (or a pair of users)** use different frequency in different time slot
   - sender and receive know the **hop sequence**
   - **benefit**: minimize interference, difficult to eavesdrop
2. **Direct Sequence Spread Spectrum (DSSS)**
   - Use all sub-frequencies independently, maximize bandwidth
   - Security: Pseudorandom noise code (PN code): sender modulates PN code and receiver filters out after synchronizing PN code generator.

Wireless Technologies

- **FHSS vs. DSSS**
  - FHSS use a portion of total bandwidth, lower data throughput
  - DSSS use all the available bandwidth continuously, higher data throughput
  - 802.11 use FHSS, provide 1 to 2 Mbps
  - 802.11b use DSSS, provide 11Mbps

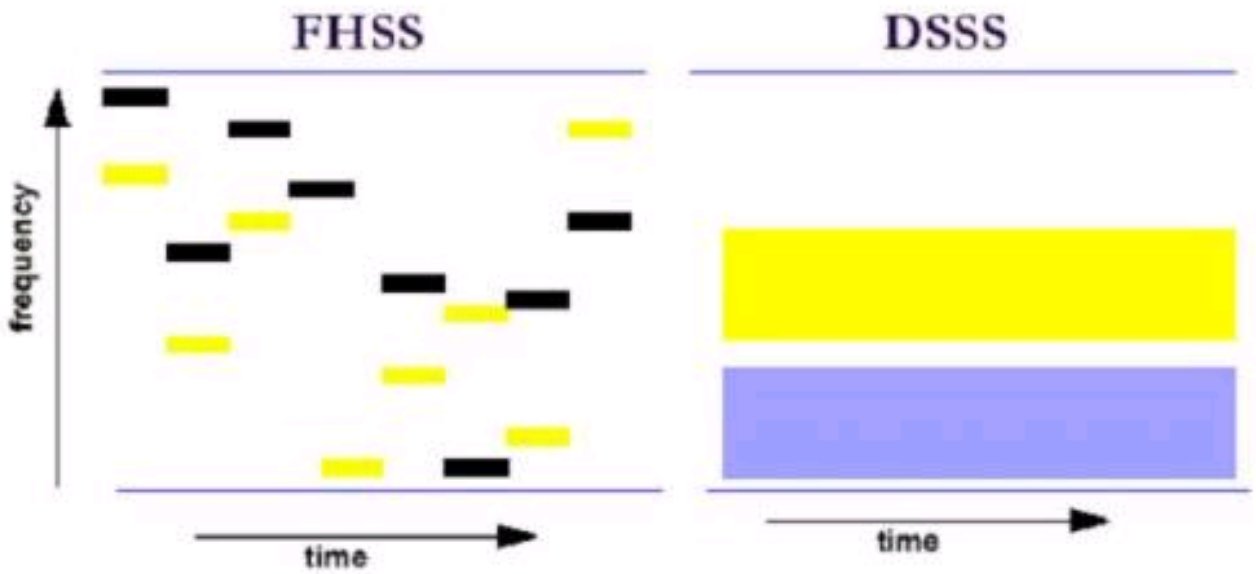


Figure 1: Spectrum Use by FHSS (Left) and DSSS (Right) Technologies

Wireless Security Issues

- **Very long vulnerability list**
- **Wired Equivalent Privacy Protocol (WEP)**: very basic security feature considered “insecure” , use encryption to provide confidentiality, but the WEP key can be cracked in a few minutes. Used in OSA and SKA.
- **Open system authentication (OSA**): cleartext authentication in WEP, consider as low security. Encryption only after authenticated.
- **Shared Key Authentication (SKA**): in WEP, AP sends random value (Challenge), the PC to encrypt with cryptographic key (Response) and return it; AP compares the result; But default is off.
- **Shared Key Authentication Flaw**: RC4 in WEP is stream cipher algorithm, both limited length challenge and response text can be eavesdrop easily

Wireless Security Issues

- **Wi-Fi Protected Access (WPA):** using Temporal Key Integrity Protocol (TKIP) to add more key material, but still can crack the key in 15 mins and considered “insecure”.
- **Wi-Fi Protected Access 2 (WPA2): or IEEE 802.11i** considered most secure Wireless network protocol using stronger algorithm AES. In 2010, “Hole 196” can crack the key, but if better key management to prevent this “man-in-middle” kind attack.
- **Ad-hoc Mode WLAN**: no AP, Peer-to-Peer, less expense but less scalability and less security (lack MAC filtering and access control)
- **“Parking Lot**” or “**Wardriving**” Attack: Inside a car to eavesdrop the Wi-Fi traffic of organization.
- **Service Set Identifier (SSID) Flaw**: SSID broadcasting and default SSID name allow attackers to perform further attacks.

Satellites

- wireless connectivity between different locations
- **footprint**: coverage of communication, can be 1/3 world or only a few hundred feet.
- **Satellite Delay** is main obstacle of data communication nowadays. But it is good resilience of communication infrastructure on the earth.

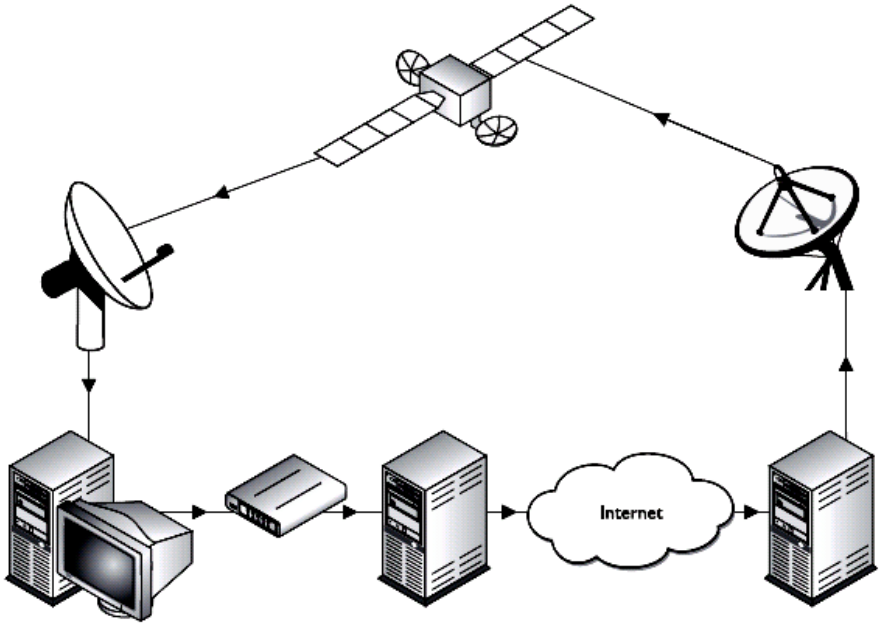


Figure 7-56 Satellite broadband

A7. Cryptography used to Maintain Communication Security

- Previously mentioned "**PKI**" in Digital Signature, Electronic Payments etc.
- Special considerations in Cryptographic
  - **User trust** or confidence
  - **User Choice**: among different methods, HW, SW,…
  - **Standardization** is required
  - **Protection of Privacy**
- Security at the **Transport Layer**: SSL and TLS
- Security at the **Application Layer**: PGP and S/MIME

Transport Layer Security
Secure Sockets Layer: SSL

- **HTTP: H**yper**T**ext **T**ransfer **P**rotocol
  - HTTP is a protocol of the web, send information between Server & Client (Browser)
- **HTTP Secure**
  - Use https://
  - Provide public key encryption, **server authentication,** message integrity.
  - Sometimes, **client authentication** (the bank's website needs to authenticate the customer)
  - Transport Layer

Transport Layer Security (TLS)

- TLS uses X.509 certificates in **asymmetric cryptography** to authenticate the counterparties and to **exchange a symmetric key**.
- Transport layer
- This **session key** is then used to **encrypt** data flowing between the parties. This allows for data/message **confidentiality**, and message authentication codes for message **integrity**.
- Widespread use in applications such as **email**, web browsing, Internet faxing, instant messaging, and voice-over-IP (VoIP).

Application Layer Security: Secure MIME (S/MIME)

- **Multipurpose Internet Mail Extension (MIME)**
  - Technical specification indicating how multimedia data and email attachment to be transferred.
- **Secure MIME (S/MIME)**
  - A standard for encryption and digitally signing email
  - Provide confidentiality, integrity, authentication and nonrepudiation

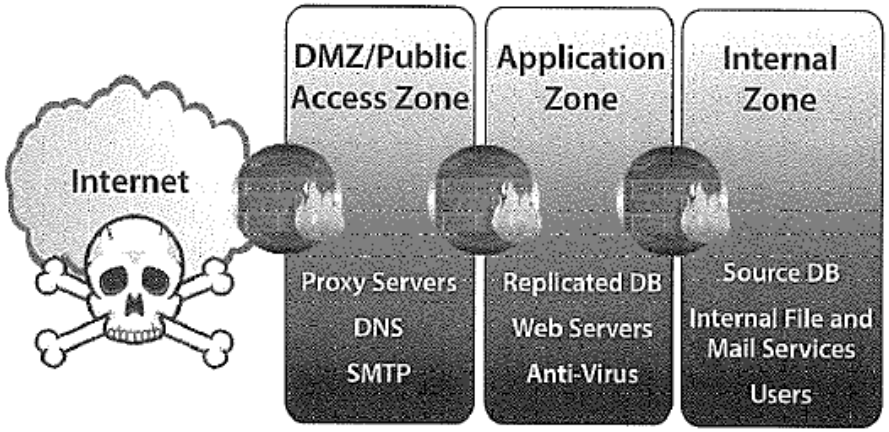
Application layer security: Pretty Good Privacy (PGP)

- the **first widespread public key** encryption program
- to protect email and file
- use RSA for key management and IDEA for encryption, SHA-1 for hashing
- Provide confidentiality, Integrity, authentication and nonrepudiation: **complete solution**
- But **not a CA**, but use "web of trust" in key management, can generate and store user's private key etc.
- User randomly type to **gen user's private key**, then use passphrase to encrypt private key and store in HD.
- **User generates and distributes own public key**
- Users can exchange and sign public keys directly or indirectly **(friend of friend)**
- **Key ring** = a collection of public keys and can set diff trust levels

B. Secure Network components

B1. Operation of Hardware – Routers

- **Boundary Router**: (or Perimeter, External) in between internal and external network (ie. Internet), need to control the traffic before firewall, say block access to some internal network.
- **Secure Routing / Deterministic Routing**: not desirable to use Internal and VPN to form WAN for company (why?) Prefer to use limited number of routers supplied by large network provider. More secure.
- **Network partitioning**: a protection

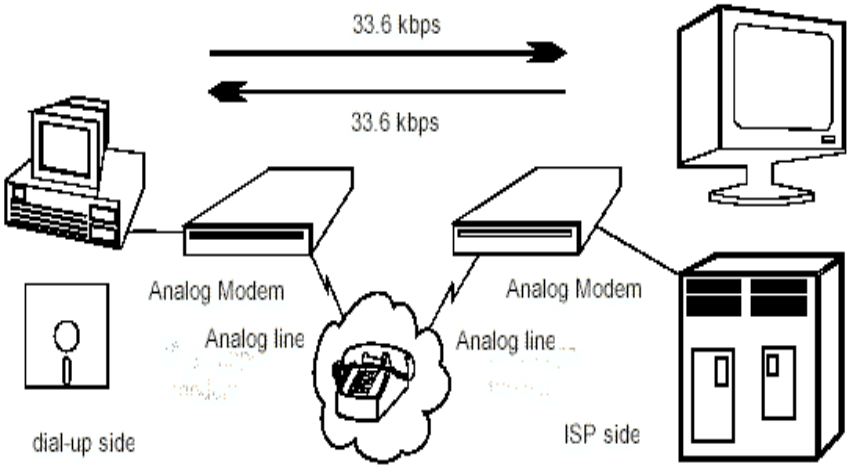


B. Secure Network components

B1. Operation of Hardware: Modem

- A common type of modem (**mo**dulator-**dem**odulator) is one that turns the **digital data** of a computer into modulated **electrical signal** for transmission over telephone lines and demodulated by another modem at the receiver side to recover the **digital data**.
- **Risk**: weak authentication, default admin pwd, always on, auto-reply, can execute DOS commands, war dialing attack (try tel. # range)
- **Countermeasure**: strong authentication, proper setup, turn-on when needed, increase ring tone (against war dialing), DMZ, call back

Callback: register staff phone number >> staff to call in the company and provide login ID >> disconnect >> the company calls the staff registered number and make connection



Question

What can be used to compromise and defeat callback security?

A. Passive wiretapping

B. Call forwarding

C. Packet spoofing

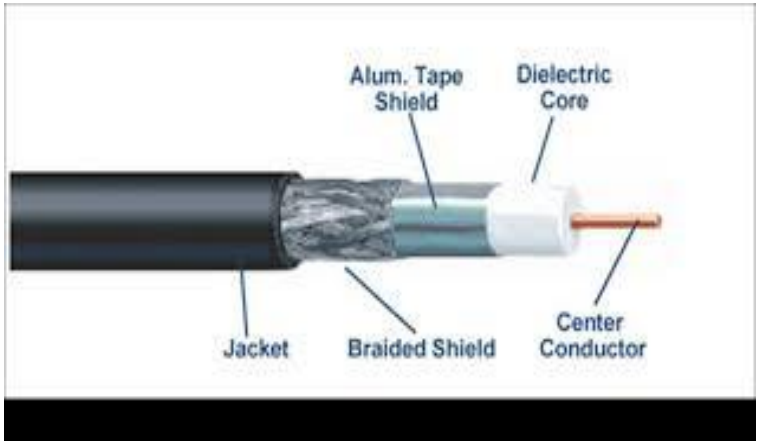
D. A brute force attack

B2. Transmission Media = Cable

- vary in speeds, maximum lengths, connectivity issues with NICs
- **negatively** affected by motors, **fluorescent** lighting, **magnetic** forces and other electrical devices
- Bandwidth: highest frequency range (10Base-T 10MHz; 100Base-T 80MHz)

Coaxial Cable

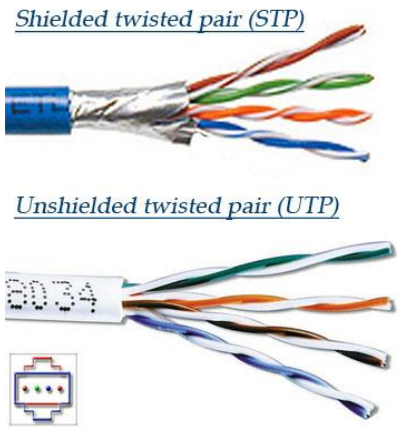
- copper core, shielding layer and grounding wire
- more resistant to electromagnetic interference (EMI), high bandwidth, longer distance
- a bit **expense** and **hard** to work with (comparing to UTP)
- can work both of baseband or broadband
- Example: TV cable

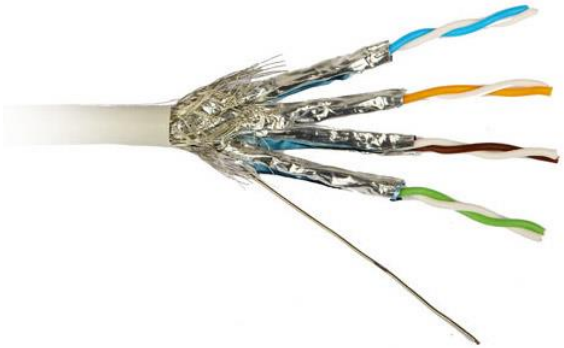


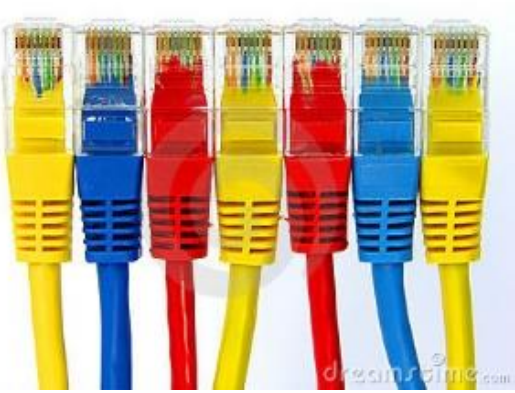
Twisted-Pair Cable

- insulated copper wires surrounded by outer protective jacket
- 2 types
  - **Shielded twisted pair (STP):** outer foil shielding
  - **Unshielded twisted pair (UTP)**
- Twisting protects radio frequency and electromagnetic interference, a balanced circuit
- Cheaper and easier to use
- **Problem**: Signal degrade, certain distance, insecure (radiate energy, can be captured)
- Mostly used in telephone system and LAN
- Category 1-7 (voice-grade to 1 Gbps)

Twisted-Pair Cable







RJ-45

Crimping Tool

RJ45 tester

Cabling Problems (copper cable)

- **Noise**: caused by surrounding devices or by environment
- **Crosstalk**: electrical signals of one wire spill over to another wire; caused by diff electrical signal mix; UTP is more vulnerable to crosstalk than STP or coaxial
- **Attenuation**: loss of signal strength as it travels; the effects of attenuation increase with higher frequencies.

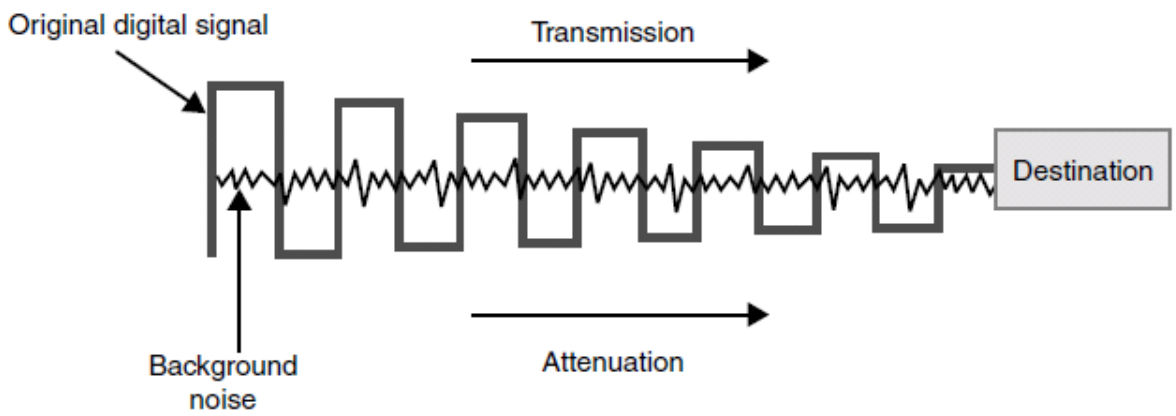
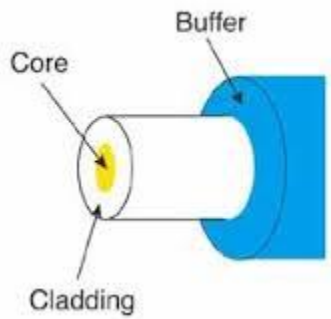


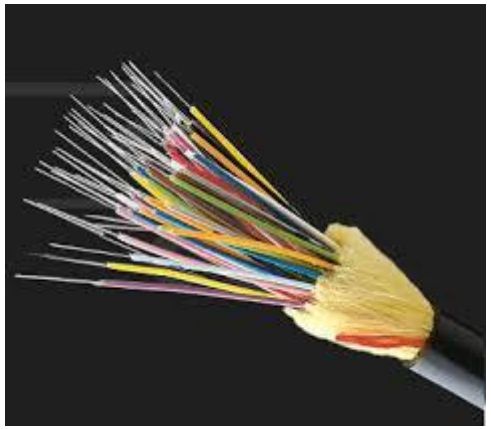
Figure 7-23 Background noise can merge with an electronic signal and alter the signal's integrity.

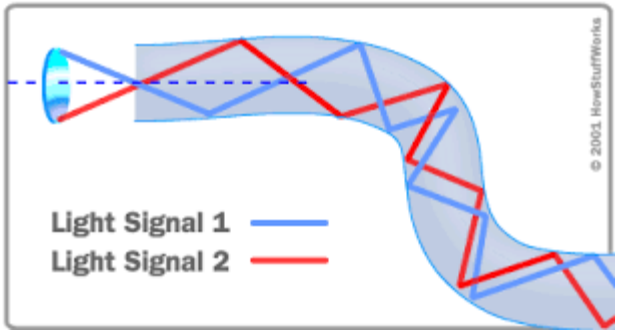
Fiber-Optic Cable

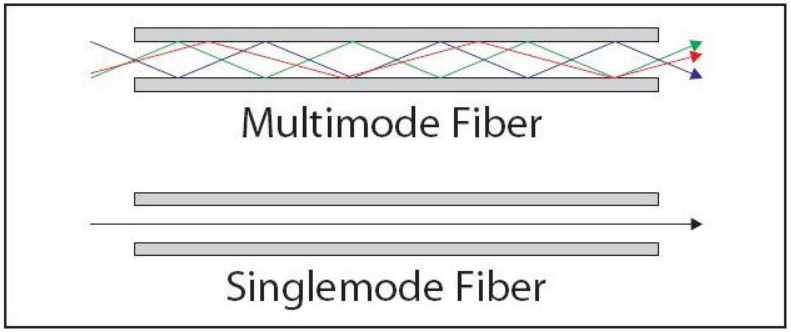
- use **glass** or plastic, slightly thicker than a human hair, that carries **light** waves
- Optical fibers typically include a transparent core surrounded by a **transparent cladding material** with **a lower index of refraction**. Light is kept in the core by **total internal reflection**. This causes the fiber to act as a waveguide or light pipe.
- Single-mode, Multi-mode and Plastic Optical Fiber (POF) (see next page)
- higher transmission speed (10-40 Gbit/s or 400G/s in lab) and long distance (1-3km)
- **Advantage**: do not affected by attenuation and EMI, do not radiate signals, more secure
- **Problem**: extremely expensive and difficult to work with

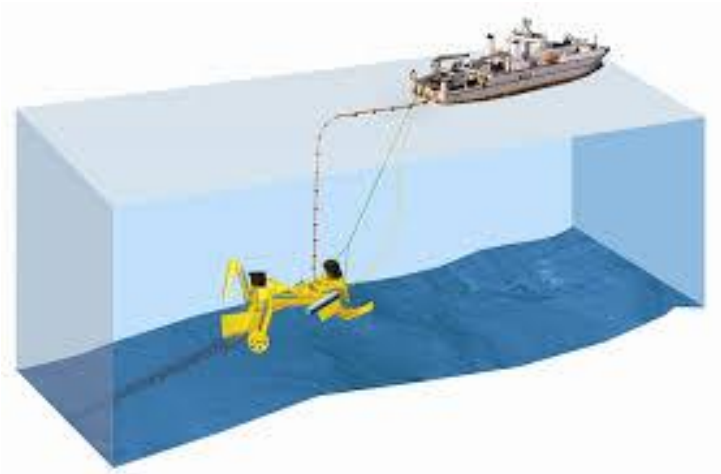
Fiber-Optic Cable











Under the sea

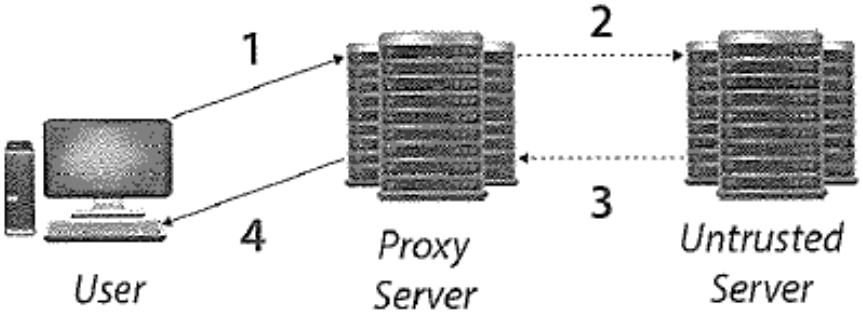
The Fire Rating of Cables

- must meet certain **fire codes**
- produce **hazardous gas** when fire
- Factor to chose cable: budget, ease of handling, possible signal interference, distance, speed, security fire rating
- Installed in unexposed areas, behind wall and protected area
- **Pressurized conduit**: if someone access the cable, pressure change will alarm

B3. Network access control devices

Firewall

- To restrict access to one network from another network by IP and Port or other types
- May be a specialized HW device, router or server
- Normally used in DMZ (demilitarized zone) which normally store web server, mail gateway, DNS server, IDS sensor etc.
- What is Proxy?



1. User's request goes to the proxy server.
2. Proxy server forwards the request to the untrusted host. To the untrusted host it will appear as if the request originated from the proxy server.
3. The untrusted host responds to the proxy server.
4. The proxy server forwards the response to the user.

B3. Network access control devices Firewall

- **Different types of Firewall**

Firewall type	OSI Layer	Characteristics
Packet filtering	Network	Looks at destination and source addresses, ports and services requested. Using ACLs allow acceptable access to a network; simple; 1st generation
Application level proxy	Application	Looks deep into packets and make access control decisions at application level; example: distinguish FTP PUT and GET; 2nd generation
Circuit level proxy	Session	Looks only at the header packet information. It protects a wider range of protocols and services (example: UDP, TCP); analogy: train different languages at custom.

Firewall

Firewall type	OSI Layer	Characteristics
Stateful	Network	Looks at the state and context of packets. Keeps track of each conversation using a state table; It may allow UDP packets only if an internal user requested before; extra protection, but higher cpu, memory, HD etc; 3rd generation.
Dynamic packet filtering	Network	Client chooses high port dynamically and create / remove ACL; Allow any type of traffic outbound and permitting only response traffic inbound; 4th generation
Kernel proxy	Application	Faster because kernel; 5th generation

Firewall Architecture

- **Bastion Host**: Locked down or hardened for the device facing Internet or untrusted network
- **Dual-Homed Firewall**: two NIC for internal and external networks; packet forwarding and routing should be turned off; today multi-homed for several different networks
- **Screened Host**: is a firewall that communicates directly with perimeter router (or Screening Device) and internal network

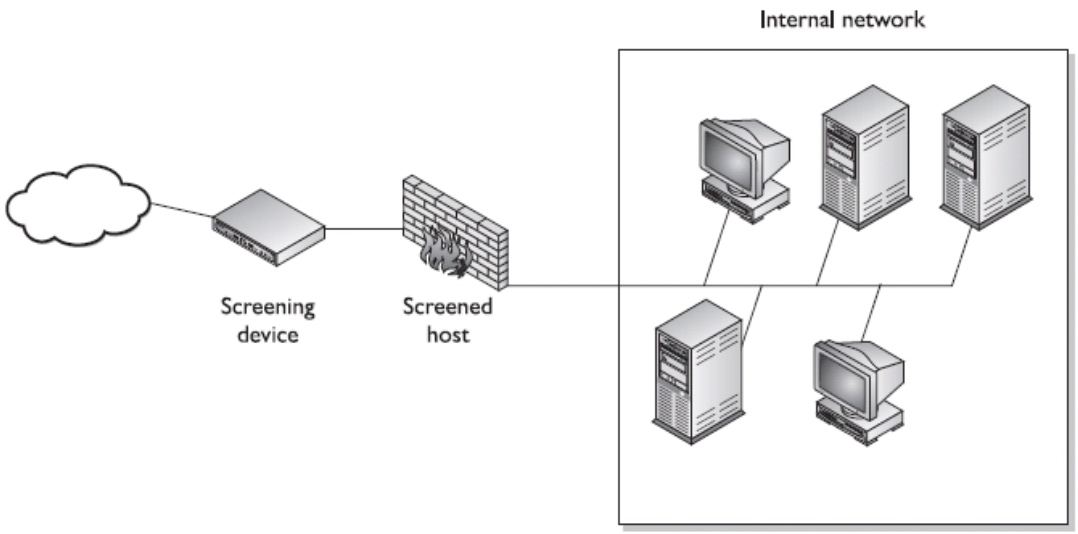


Figure 7-35 A screened host is a firewall that is screened by a router.

Firewall Architecture

- **Screened Subnet**: add another layer of security to screened-host architecture, example DMZ (Demilitarized Zone)

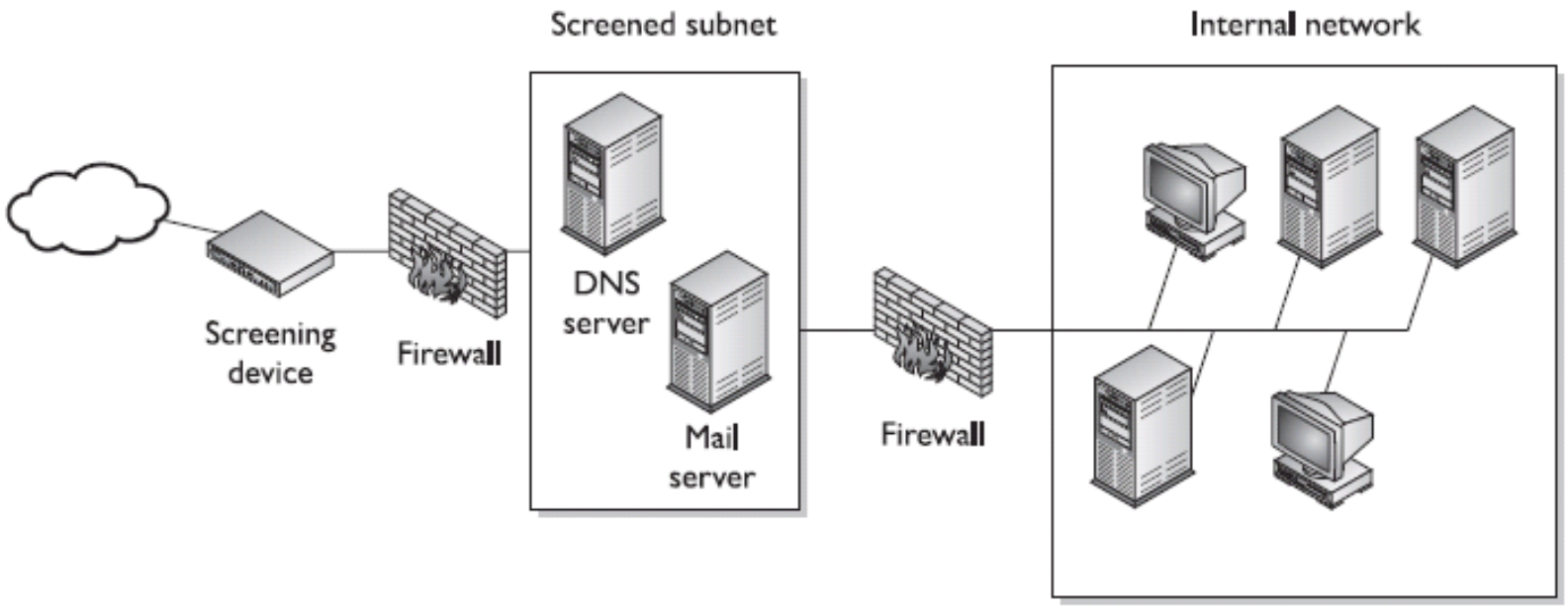


Figure 7-36 When using a screened subnet, two firewalls are used to create a DMZ.

The “Shoulds” of Firewalls

- the default action should be **implicitly deny** any packet **not explicitly allowed**. (no rule says “accept”, then denied)
- **Reject** incoming packet if source address is internal host (Masquerading or spoofing attacks)
- **Reject** outgoing packet that does not have an internal source address (carrying DDoS as a Zombie)
- **Reassemble** fragmented packet to see the whole picture
- **Reject** incoming packet with source routing information (not router’s decision)

Network Address Translation (NAT)

GREAT LEARNING EDUCATION CENTRE

- IPv4 address have become scarce (until IPv6)
- NAT enables an internal network that does not follow the internet addressing scheme to communicate over Internet.
- NAT Gateway is placed between a network and the internet, that translate the internal IP to a public Internet IP when only communicating outside.
- Change of header information is required
- 3 types of **implementation**
  - **Static Mapping**: statically 1 to 1, usually for server that need to keep the same public IP at the time.
  - **Dynamic Mapping**: has a pool of public IP, dynamically assign on first come first serve basis, estimate the number of IP needed
  - **Port address translation (PAT):** only one public IP, use port to distinguish,
- Must be Stateful: until the session is ended
- Usually performed on routers or firewall
- **Benefit**:
  - A temp fix of scarce of public IP address and
  - Security protection (hacker not easy to know the internal network information)

Question

Which is not considered a firewall architecture used to protect networks?

A. A screened host

B. A screened subnet

C. A NAT gateway

D. A two-tiered DMZ

B4. Endpoint security

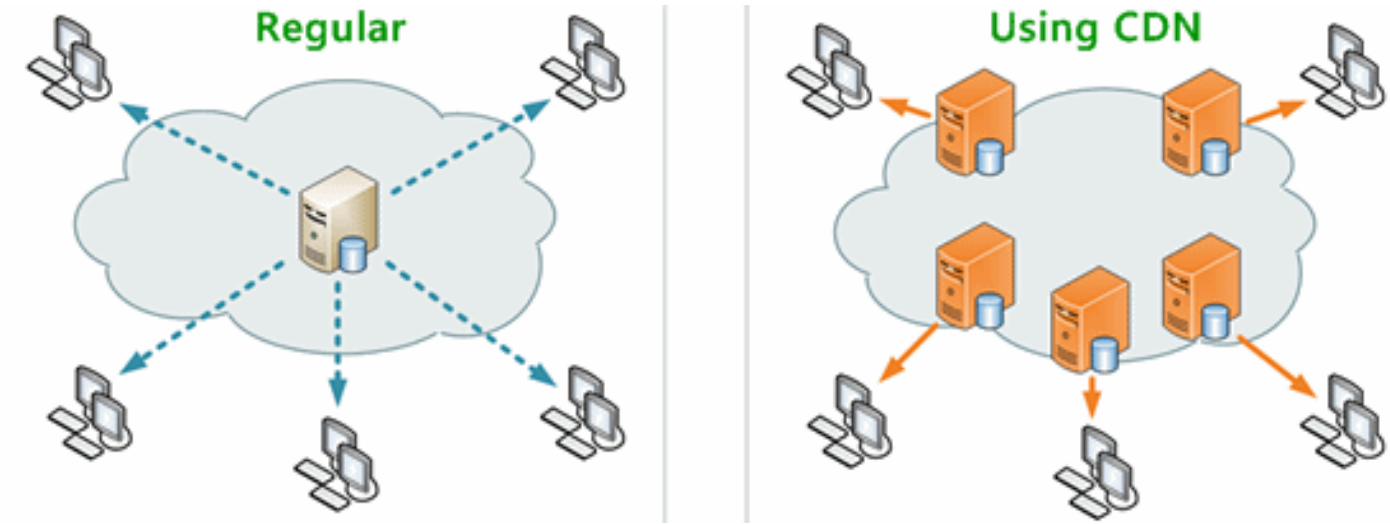
- Endpoint security is an approach to network protection that requires each computing device on a corporate network to **comply with certain standards** before network access is granted.
- Including PCs, laptops, smart phones, tablets and specialized equipment such as bar code readers or point of sale (POS) terminals.
- Comply with defined corporate security policies including an approved operating system, a VPN client and anti-virus software with current updates.
- Devices that do not comply with policy are given limited access or quarantined on a virtual LAN (VLAN).

Endpoint security

B5. Content Distribution Network (CDN)

- Or Content **Delivery** Network, Examples Microsoft Azure CDN and Amazon CloudFront.
- CDN is a large distributed system of servers deployed in **multiple data centers** across the Internet.
- The goal of a CDN is to serve Internet content to end-users with **high availability, high performance and cost saving.**
- In addition, CDNs provide the content provider a degree of **protection** from **DoS** attacks by using their large distributed server infrastructure to absorb the attack traffic.
- DNS will resolve to an **optimized** server (based on location, availability, cost, and other metrics) and that server will handle the request.

Content Distribution Network (CDN)



B6. Physical devices

- **Security concerns:**
  - **Physical access**: to move console or network equipment from public area into computer room (hardening)
  - **Disaster:** BCP
  - **Steal**: slot lock, security guard
  - **Out of order**: maintenance
  - Etc.

C. Design & Establish secure communication channels
C1. PBX (or Private Branch Exchange)

- Normally organization owns
- Normally with **modem** for vendor support (power off when not using)
- **Default manager password** vulnerability: Phreaker (phone hacker) may use brute force or other attacks, then enjoy IDD; listen or change voice mail.

C2 Multimedia collaboration
Remote Meeting Technology

- In general, web conferencing is made possible by **Internet** (TCP/IP) connections, across geographically multiple locations.
- Applications for web conferencing include meetings, training events, lectures, or presentations from a web-connected computer to other web-connected computers.
- Example: Cisco Webex, Skype, AnyMeeting etc.
- **Risk**: Vulnerable for hacking, Theft of Trade secrets, Employee records, Product knowledge and Earnings projections

Instant Message (IM)

- allow people to communicate with another through a type of real-time and personal chat room, **example**: AOL, ICQ, Yahoo Messenger etc
- **Security risk**: no encryption of traffic; file transfer; spread virus, worm, Trojan horse
- Blocking port is not effective, because web-based IM may use common port, such as 80.
- **Countermeasure**: security **policy**; integrated antivirus / firewall product; block IM traffic; **corporate IM server**; do not allow IM and force to use old-fashioned way (eg email or phone).

C3. Remote Access

VPN: Virtual Private Network

- **VPN**
  - is a secure, private connection through a public network
  - use **tunneling (logical connection)**, *optionally* **authentication** and **encryption** protocol
  - ensure confidentiality and integrity
  - common application is to allow remote user via Internet to access company network and resource securely.
- **Steps**
  - PPP
  - Authentication
  - Tunneling
- **PPP (Point-to-Point Protocol)**
  - allow internal traffic to be transmitted over telephone line (encapsulation)
  - Do not require both end to have IP before data transfer can occur

3 x Authentication Protocols

1. PAP (Password Authentication Protocol)

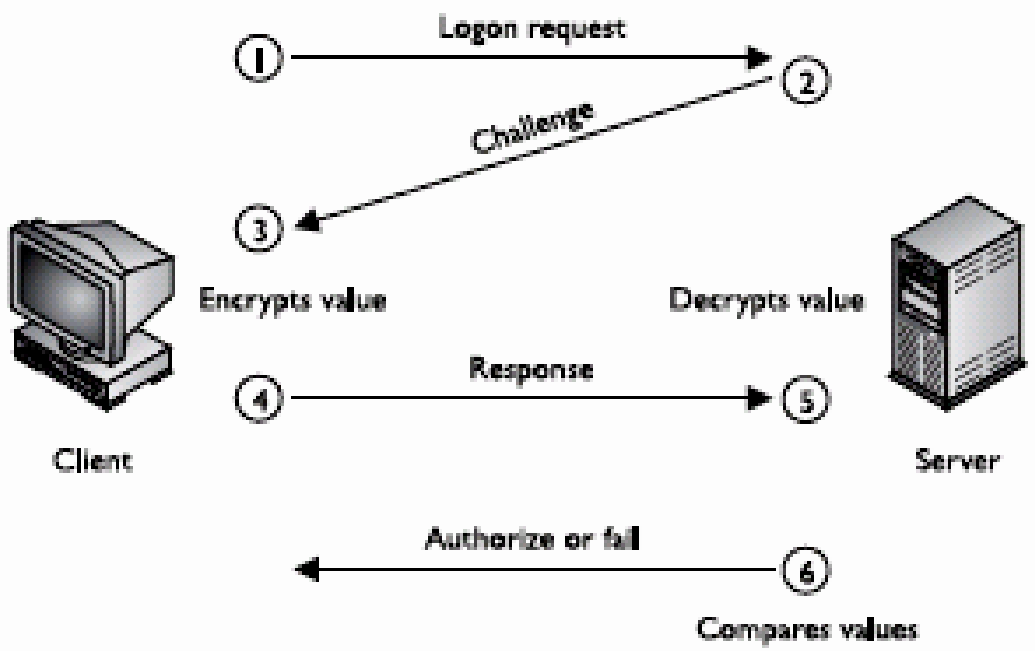
- Identification and authentication with user name and password
- Match password database at authentication server
- Over PPP protocol
- Least secure as sending password in clear text
- Should use CHAP first if have CHAP capabilities

3 x Authentication Protocols

2. CHAP (Challenge Handshake Authentication Protocol)

- Use challenge/response mechanism
- Over PPP protocol
- More secured

Figure 7-53
CHAP uses a challenge/response mechanism instead of having the user send the password over the wire.



3 x Authentication Protocols

3. EAP (Extensible authentication Protocol)

- Is a framework to enable many types of authentication techniques, **such as one-time password, token cards, biometrics, kerberros, etc.**
- Over PPP
- To fix PAP and CHAP issues, **more secure**

3 x Tunneling Protocols

- **Tunneling Protocols**
  - A tunnel is a virtual path across a network that delivers packet that are encapsulated
  - Encapsulation: insert header or trailer to convert to another protocol
  - 3 main methods of Tunneling for VPN: PPTP, L2TP and IPSec
- **PPTP (Point-to-Point Tunneling Protocol)**
  - Microsoft protocol to create a tunnel for VPN
  - Encapsulate header and IP header, allow to work in IP Network
  - **Limitation**: can work *only IP* network, need other protocols for other networks, such as X.25, Frame relay and ATM

3 x Tunneling Protocols

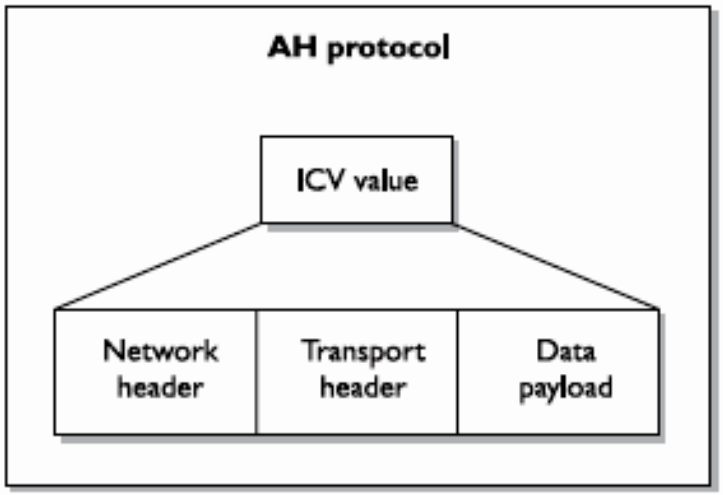
- **L2TP (Layer 2 Tunneling Protocol)**
  - same functionality of PPTP and plus
  - **L2TPv3** provides additional security features, improved encapsulation and can work IP, X.25, Frame Relay, Ethernet and ATM
  - An alternative of MPLS
  - Data Link layer
- **IPSec**
  - Handles **multiple connection** at the same time
  - Provide secure authentication and encryption
  - Support IP network only
  - Chapter 8, Cryptography have full description of IPSec

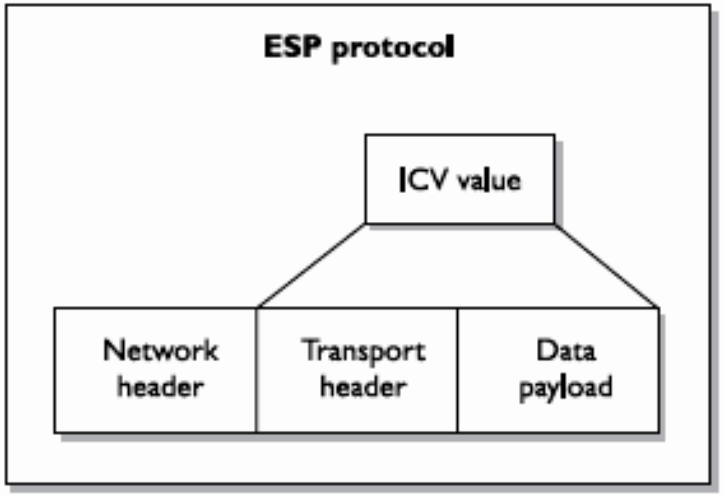
Internet Protocol Security (IPSec)

- Internet Protocol Security (IPSec) is a protocol suite provides a **secure channel** for data exchange.
- **Widely accepted** standard, more flexible and less expensive than End-To-End and Link encryption
- Network layer
- Used in VPN **across internet**
- It is **not strict protocol**, but an open modular to have choice of algorithm, keys and authentication methods
- Two basic protocols: AH and ESP
  - **AH**: Authentication Header: provides **authentication and integrity** (see ICV), normally used in **internal network without NAT**
  - **ESP** (Encapsulating Security Payload): provides **authentication, encryption and partially integrity** (see ICV), normally used in **Internet**

Internet Protocol Security (IPSec)

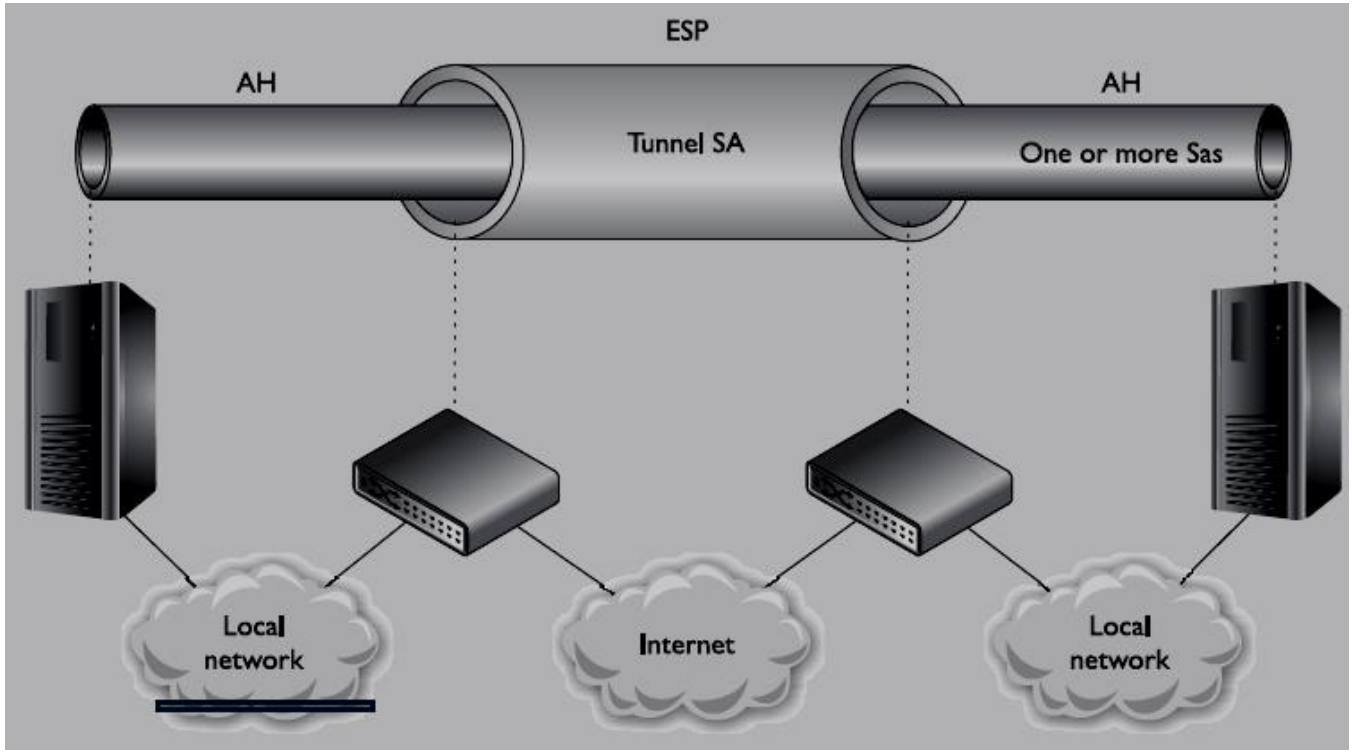
- Diff of using **AH** protocol and **ESP** protocol is mainly **depending on NAT or not.**
- **ICV** = Integrity Check Value, something similar to MAC (Message Authentication Code)





Internet Protocol Security (IPSec)

- AH vs ESP



Internet Protocol Security (IPSec)

- **Security Association (SA):**
  - For each device, SA is the **record of configuration**, contains authentication, encryption keys, algorithms, key lifetime, source IP
  - One device may have **two** SA, one for **inbound** and one for **outbound**
  - **Security Parameter Index (SPI**): each device should have a list of SA and SPI **tells which one** should be used.
  - This figure shows how to decrypt an **incoming** encrypted packet, all components should be inside the computer.

Internet Protocol Security (IPSec)

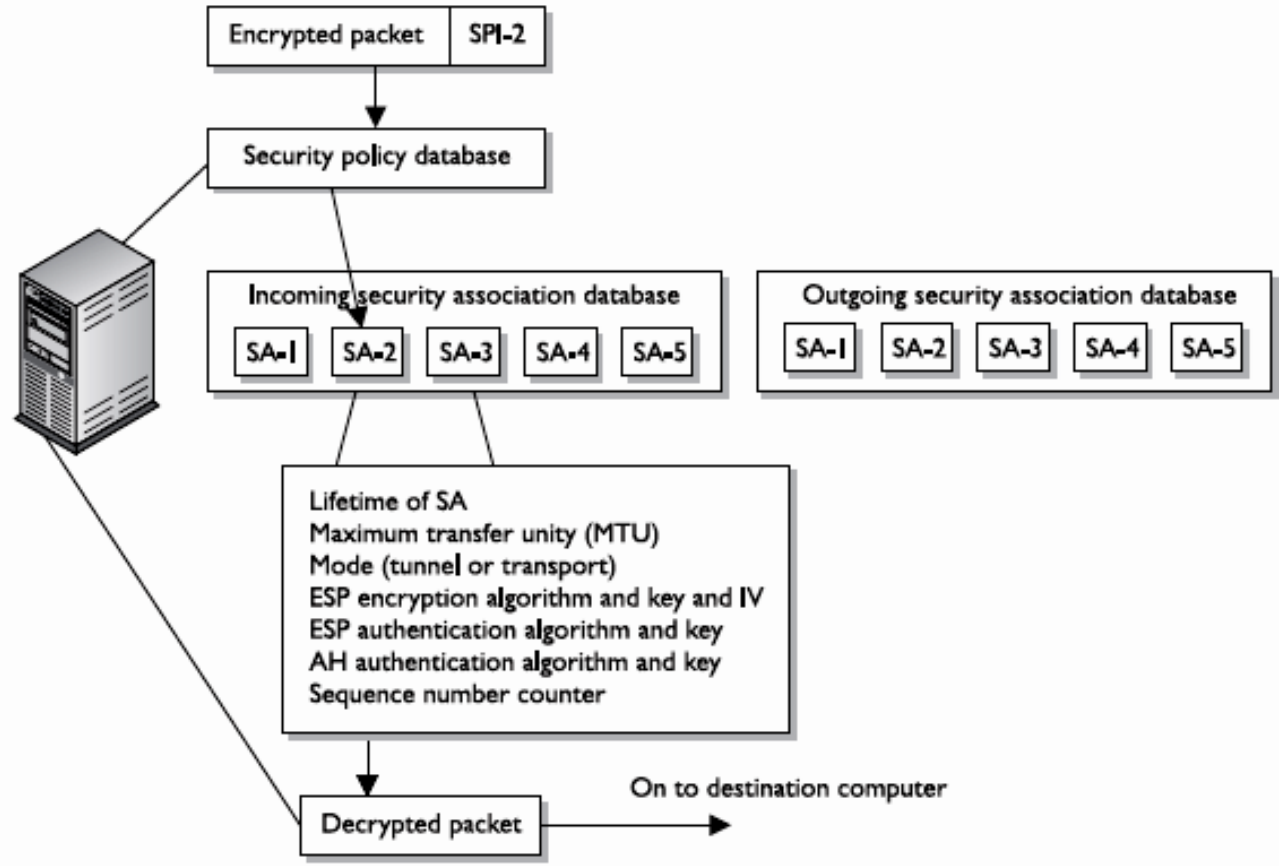


Figure 8-27 The SPI and SA help the system process IPSec packets.

Remote Access Guidelines

- modem set to more than 4 rings answer to prevent war dialing
- strong authentication
- Firewall to protect internal servers
- Fixed IP and list of IP in database for connection

Screen /Web Scraping

- **Screen scraping** is normally converting visual data from a source system to another system. For example, capturing the bitmap data from the screen and running it through an OCR engine. **Attack** to capture PIN at banking website.
- **Web Scraping**: Web pages contain a wealth of useful data in text form. However, most web pages are designed for human end-users and not for ease of automated use. A web scraper is an API to extract data from a web site.
- Companies like Amazon AWS, Google provide web scraping tools, services and public data available free of cost to end users.
- **Security Concerns**: Copyright, legal issue, increase traffic (23% increased in 2013 related to scraping)

Web Scraper


Women's Singles
More
Rank Country Player Member ID Points Tournaments Confederation Country
1 CHN LI Xuerui Profile 64643 79214 9 Asia Chinese Badminton Association
2 IND Saina NEHWAL Profile 52748 74381 13 Asia India
3 CHN WANG Shixian Profile 83064 72227 12 Asia Chinese Badminton Association
4 ESP Carolina MARIN Profile 18228 72098 13 Europe Spain
http://bwfcontent.tournamentsoftware.com/ranking/ranking.aspx?rid=70 - Original Source
File Edit Format
Player</th><th class="extraheader left"> </th><th class="extraheader left">Member ID</th><th class="extraheader right rankingpoints">Points</th><th class="extraheader right">
Tournaments</th><th class="extraheader ">Confederation</th><th class="extraheader ">Country</th>
416 </tr><tr>
417 <td class="rank"> 1 </td><td class="rank_equal" title="Previous rank: 1"> </td><td> </td><td>CHN</td><td><img
src="//static.tournamentsoftware.com/images/flags/16/CHN.png" class="intext flag" width="16" height="14" alt="CHN" title="CHN"/>[CHN] <a
href="player.aspx?id=8619&player=109508">LI Xuerui</td><td>
Profile</td><td>64643</td><td class="right rankingpoints">79214</td><td class="right">9</td><td><a href="category.aspx?id=8619&category=473&ogid=0EB2BA3B-3867-465E-8D04-
CEDE4A566474">Asia</td><td>Chinese Badminton Association</td>
418 </tr><tr>
419 <td class="rank"> 2 </td><td class="rank_equal" title="Previous rank: 2"> </td><td> </td><td>IND</td><td><img
src="//static.tournamentsoftware.com/images/flags/16/IND.png" class="intext flag" width="16" height="14" alt="IND" title="IND"/>[IND] <a
href="player.aspx?id=8619&player=107881">Saina NEHWAL</td><td>
Profile</td><td>52748</td><td class="right rankingpoints">74381</td><td class="right">13</td><td><a href="category.aspx?id=8619&category=473&ogid=0EB2BA3B-3867-465E-8D04-
CEDE4A566474">Asia</td><td>India</td>
420 </tr><tr>
421 <td class="rank"> 3 </td><td class="rank_equal" title="Previous rank: 3"> </td><td> </td><td>CHN</td><td><img

Virtual applications and Desktops

- **Virtual Network Terminal Services:** tool used for remote access to server resources.
- **Example:** Citrix, remote desktop..
- **Advantages:** avoid physical access to server, prevent potential malicious code, SSH can provide security
- **Disadvantage:** patching can be tricky and complex as interdependencies with Web server, client and server and application.

Type of Transmission

- **Analog** transmission signal are *continuously* varying electromagnetic waves. More natural, in air, water or cable
- **Digital** signals represents binary digits as electrical pulses. 0 or 1, More reliable than analog over long distance, provide clear-cut and efficient. Represented by voltage on (=1) or off (=0)

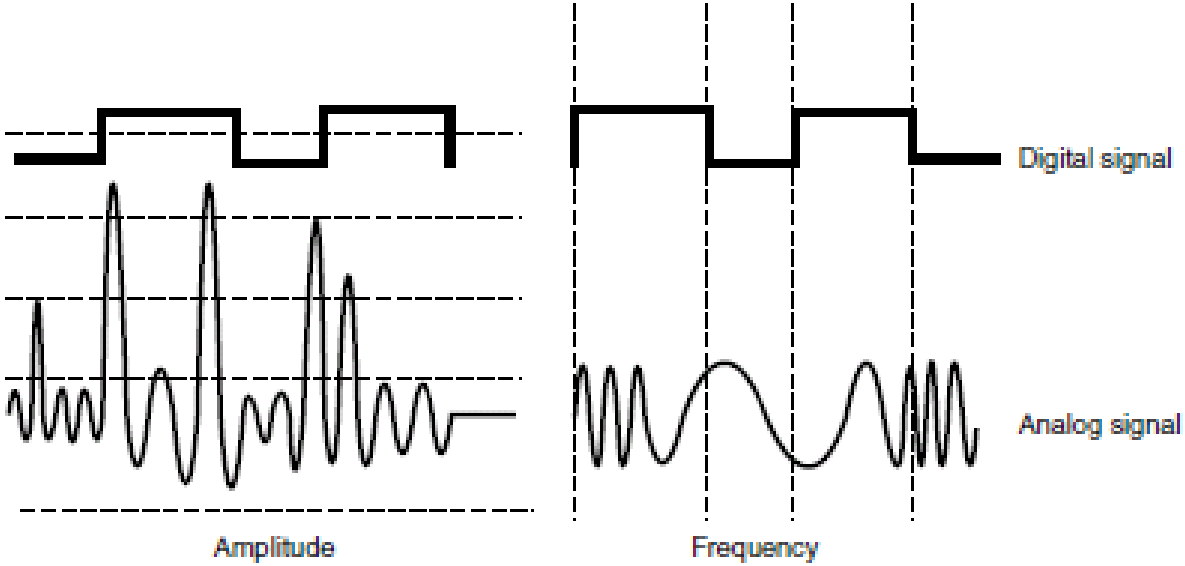


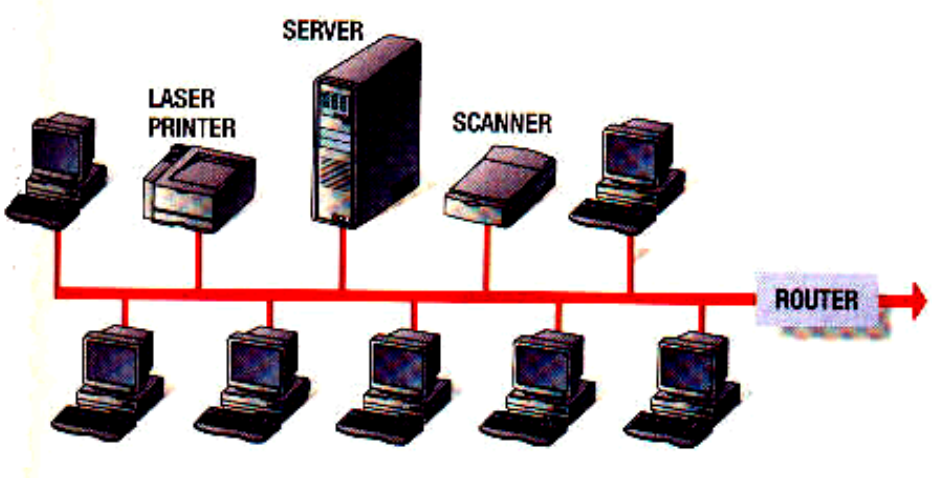
Figure 7-15 Analog signals are measured in amplitude and frequency, whereas digital signals represent binary digits as electrical pulses.

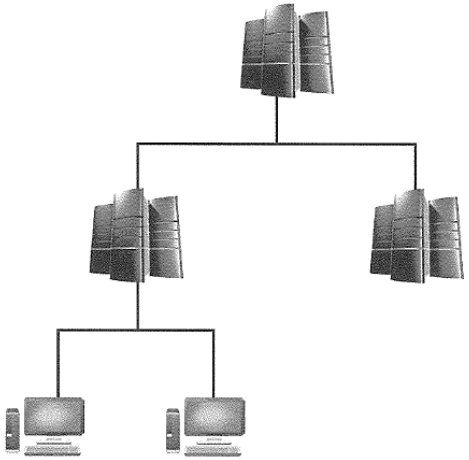
LAN Networking

- **Main reasons for LAN**
  - to **share** information & resources
  - to provide **central administration**
- **Network Topology**
  - Network Topology is the ***physical*** arrange of computers and devices
  - Can be different logical arrangement, for example, Token Ring: physical is star and logical is ring.

Bus / Tree

- **Bus Topology**
  - a single cable runs the entire length of the network
  - packet is being “looked at” by all nodes, node can accept or reject the packet depending on destination address
  - 2 types**: Linear Bus Topology** (single cable) & **Tree Bus Topology** (branch)
  - Problem: one fail, others be negatively affected; cable is a potential single point of failure

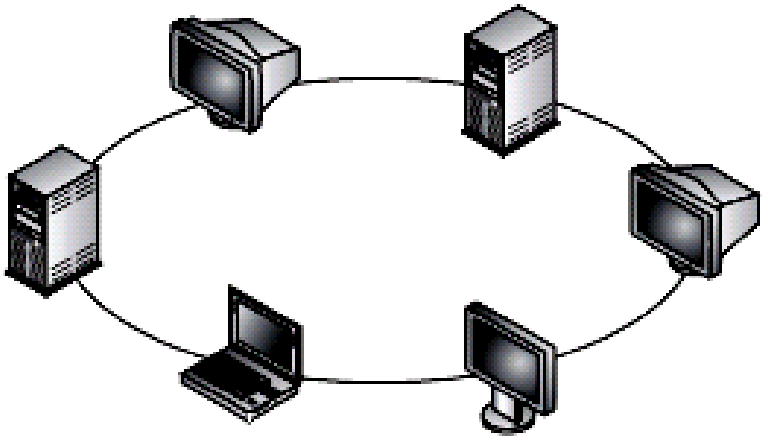




Ring

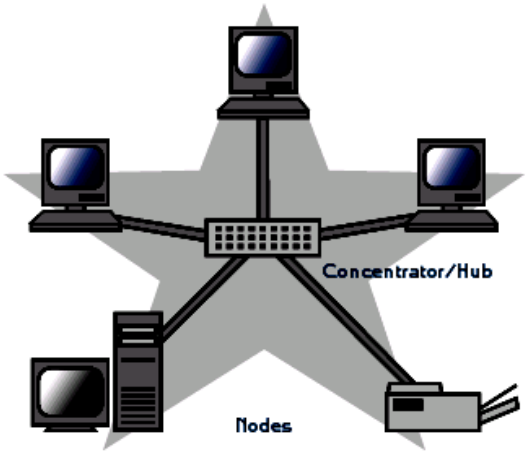
- **Ring Topology**
  - unidirectional transmission link, a closed loop and do not connect to a central system
  - **problem**: one fail, then all others could be negatively affected, because of interdependence

Figure 7-16
A ring topology forms a closed-loop connection.



Star

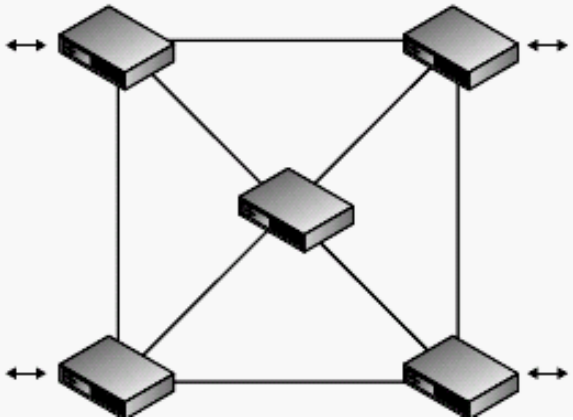
- **Star Topology**
  - all nodes connect to a central device such as switch
  - easier to detect cable problem
  - **Problem**: central device could be single point of failure, so redundancy is required
  - Most LAN implement in Star topology



Mesh

- **Mesh Topology**
  - all nodes are connected to each other
  - full Mesh Topology every node is directly connected to every other node, provide great degree of redundancy.
  - usually interconnected routers and switches to provide multiple paths
  - Example: Internet
- **Backbone**: no matter what topology, most LANs have a backbone in place to connect network segments together. Usually require high speed

Figure 7-17
In a mesh topology, each node is connected to all other nodes, which provides for redundant paths.

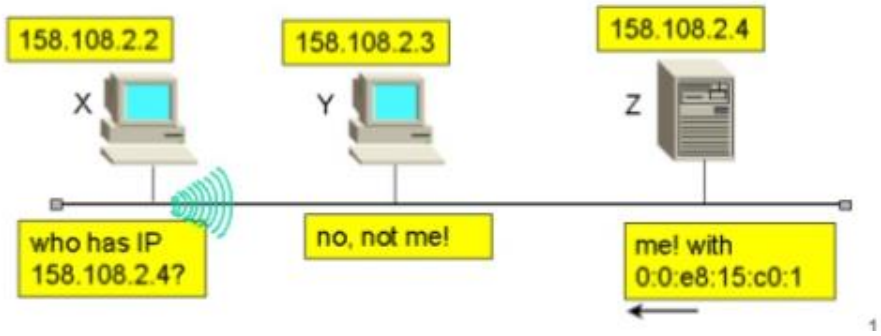


Transmission Methods

- **Unicast** Transmission Method: from the source computer to one particular system; **one to one**; example: Ethernet
- **Multicast** Method: to a specific group of systems; **one to many**; example: radio station in computer; user selects one program → software tell the NIC driver to pick up not only self-address, but a specific multicast group address.
- **Broadcast** Method: **to all** computers on the subnet; one to all; everyone gets the data; **example** Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP)

- Requesting MAC for a known IP
- http://www.theitstuff.com/cisco/ccna/how-arp-worksvideo/
- **How it works**: ARP broadcasts a frame requesting MAC for an IP → the destination IP Address PC responds with MAC → store onto table for predefined period;
- ARP table poisoning attack: alter a system's ARP table; masquerading attack



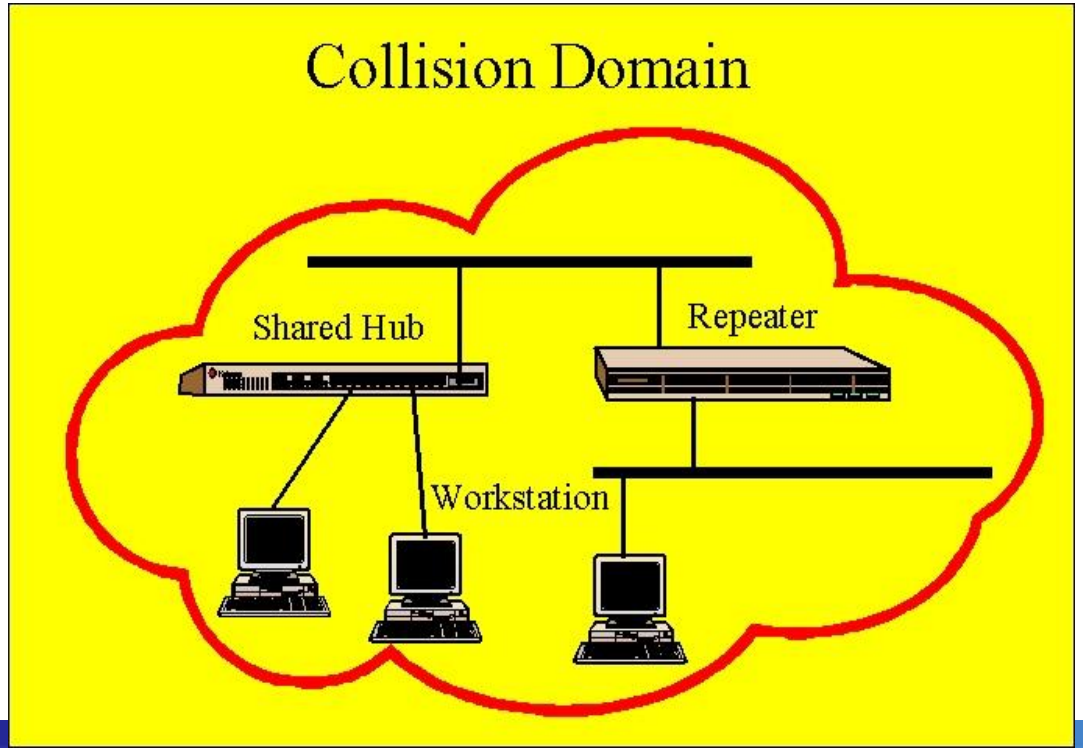
ARP table

Table ARP pourRouter0

Adresse IP	Adresse Matériel	Interface
192.168.1.1	000C.CFD2.4CCA	FastEthernet0/0
192.168.1.33	0004.9A0D.2255	FastEthernet2/0
192.168.1.70	00D0.BADC.C62C	FastEthernet3/0
192.168.1.72	00D0.FF0E.7966	FastEthernet3/0
192.168.2.1	0060.7025.CA54	FastEthernet1/0
192.168.2.33	0040.0BC9.B05D	FastEthernet4/0
192.168.2.70	0090.2B46.E022	FastEthernet5/0
192.168.2.72	0090.2BA7.B63A	FastEthernet5/0

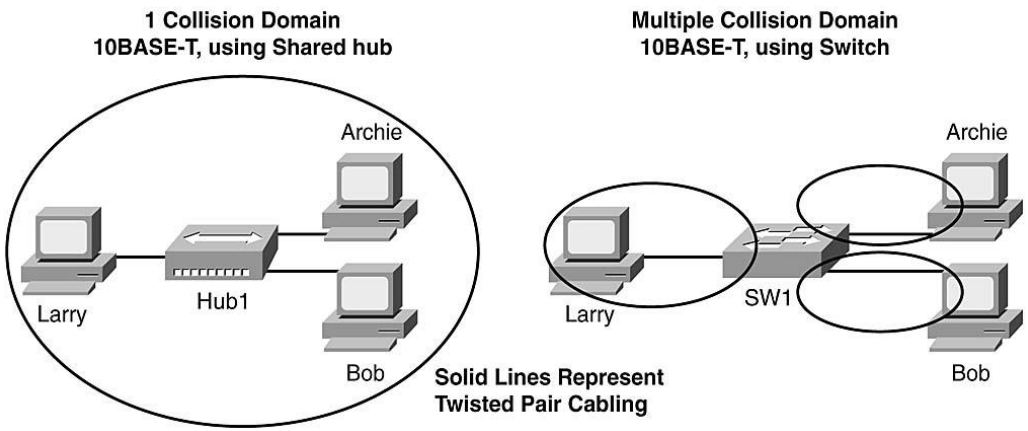
Ethernet

- Standard IEEE 802.3
- Most common one now
- Topology: usually in Bus (single cable) or Star (central device)
- deal with **collisions**, data integrity, communication mechanism and transmission controls
- Ethernet type: 10Base2, 10Base5, 10Base-T, 100Base-TX (Fast Ethernet), 1000Base-T (Gigabit Ethernet)



CSMA : Carrier Sense Multiple Access

- **CSMA/CD (CSMA/Collision Detection):** computer listen for the absence of carrier tone on the cable.
  - If two computers sense the absence (wait until free) at the same time, contention and collision will occur.
    - **Contention**: nodes have to compete
    - **Collision**: corrupts both frames, abort, alert all other stations
  - All stations will execute a **random collision timer (or back-off algorithm**) to force delay the transmission.
  - Collisions are usually *reduced* by dividing a network with bridge or switch



CSMA : Carrier Sense Multiple Access

- **CSMA/CA (CSMA/Collision Avoidance)**:
  1. signals (or tells) its intent to transmit data to all other stations
  2. listen to the cable determine it is busy or free
  3. once it is free, put data on the cable;
  - **Example**: wireless LAN, 802.11
  - **Analogy**: classroom rule: students require to raise the hand before speaking

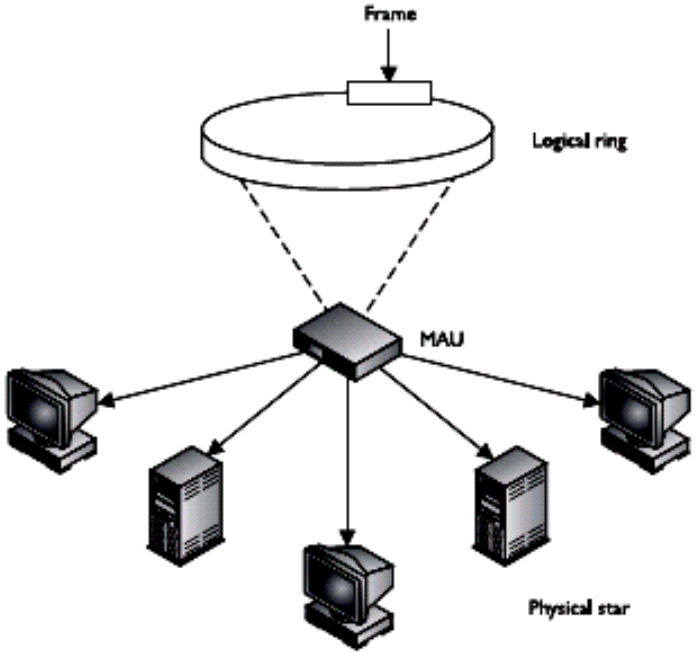
Token Ring

- **not very popular**, developed by IBM
- physical: star; logical: ring
- the central device is called Multistation Access Unit (MAU)
- **no collision, but more slowly compared to Ethernet**
- 4Mbps to 16Mbps
- IEEE 802.5

Token Passing

- **Token**: 24-bit control frame used to control which computer communicate
- Used in Token Ring and FDDI

Figure 7-19
A Token Ring network



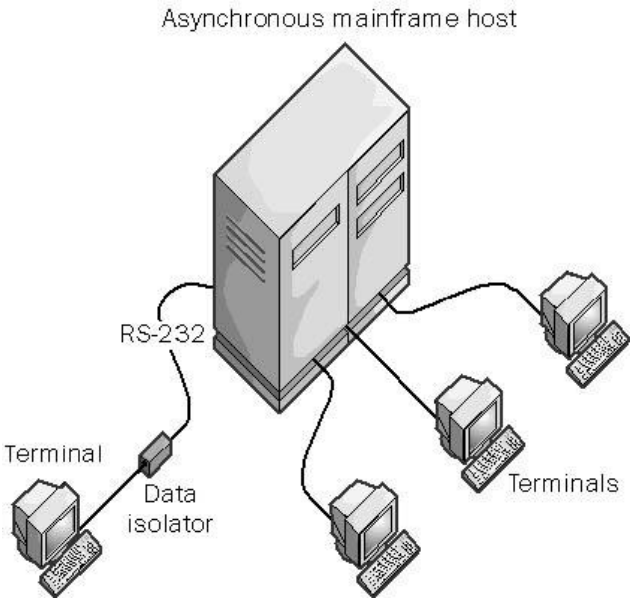
- **How it works**
  1. Multistation Access Unit (MAU) distributes a token once a time
  2. Computer receive a **token** (right to communicate)
  3. Put data with token and put it on the wire
  4. Everyone check the packet until the destination
  5. Make a copy and flip a bit
  6. Get back to source computer
  7. Remove the frame from the network

FDDI : Fiber Distributed Data Interface

- Developed American National Standards Institute (ANSI)
- High speed token passing media access technology
- 100 Mbps
- Usually backbone network using fiber optic cable
- Provide fault tolerance: **primary ring** (clockwise) and **secondary ring** (counterclockwise)
- Long distance and high speed with minimal interference
- Can also work on UTP cable
- IEEE 802.8

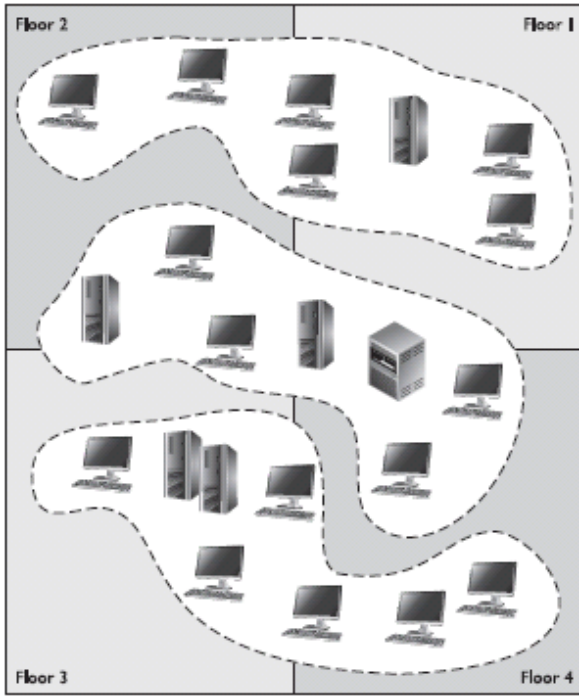
Polling

- In **Polling** environment, some systems are configured as **primary** stations and some are **secondary** stations.
- The primary will ask secondary to communicate and that is only time the secondary can communicate.
- Mainly in **mainframe** environment
- **Analogy**: Teacher asks students one by one whether they want to talk.



C4. Data communication

- Virtual LAN
  - enable administrator to separate computers logically based on resource requirement, security or business needs. Eg. Marketing dept is in the same VLAN
  - Can be implemented in Switch
  - Use routing to communicate cross VLAN



Wide Area Networks (WAN)

- When communication needs to travel over a larger geographical area.
- Most likely a router that communicates with the company's service provider or telephone company facility
- A communication link is required to connect two or more LANs.

Telecommunication Evolution

- Telephone system is switching and multiplexing system, about **100 years**
- In 1960, **T1** line can carry 24 voice calls over a pair of copper wires, provide 1.533Mbps
- **T3** can carry up 28 T1, normally for long distance call
- Fiber optic: **OC-1** = 51Mbps; **OC-3** = 155Mbps; **OC-12** = 622Mbps
- SONET standard
- ATM: high-speed network technology which encapsulates data into fixed cell size to provide better performance and reduced overhead for error handling
- **In Europe**, use Synchronous Digital Hierarchy (SDH) (instead of SONET), **E1** = 2.048Mbps and **E3** = 34.368Mbps
- SDH and SONET are similar, but not compatible, need gateway to translate

Dedicated Links

- **Leased line or point-to-point** link, purpose of WAN communication
- expensive, but secured
- **T-Carriers**
  - T-Carrier is dedicated lines that can carry voice and data over trunk lines. It is a designed for Telecommunication Carrier. E-Carriers in Europe (E1, E3)
  - Developed by AT&T in 1960
  - Most common T1 and T3
  - Use **Time-division Multiplexing (TDM):** one T1 frame is divided into 24 time slots, 8 bit each. Each channel insert the 8 bit data into the corresponding time slot.

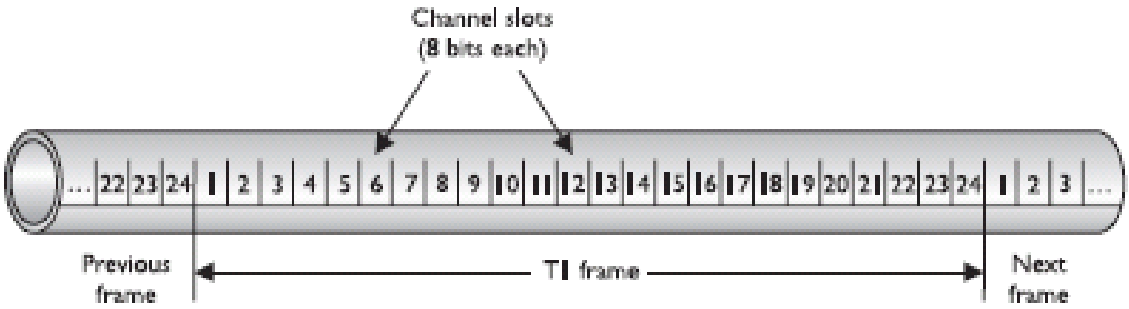
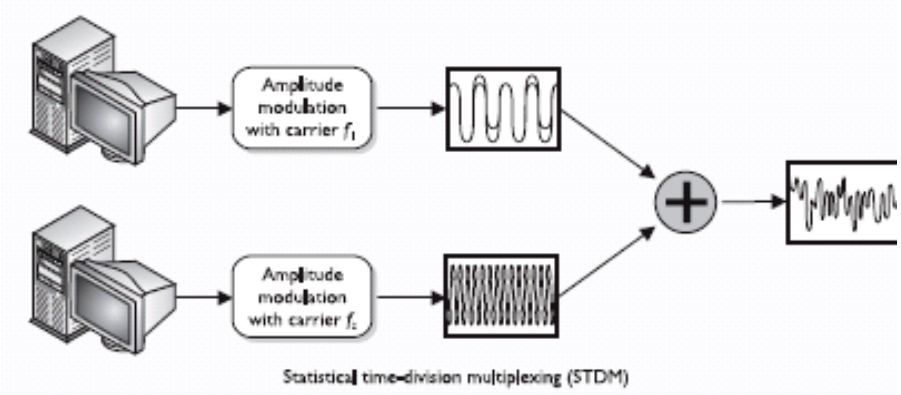


Figure 7-44 Multiplexing puts several phone calls, or data transmissions, on the same wire.

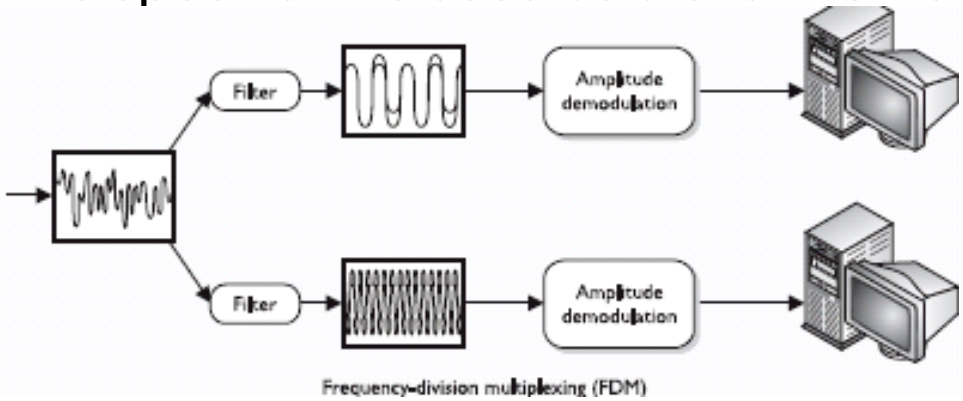
Other Multiplexing

Statistical time-division Multiplexing (STDM): Analyze typical workload and determine in real time how much time each device should be allocated for data transmission



Statistical time-division multiplexing (STDM)

Frequency-division Multiplexing: traditionally used by radio, each frequency within the spectrum is used as a channel to move data.



Frequency-division multiplexing (FDM)

Switching

- required when more than 1:1 communication
- **Circuit switching**: dynamically establish a virtual circuit, may pass thru a few switches, example: ISDN and telephone call. Fixed delay;
- **Packet switching**: address is specified in packet, use router or switch to route to the destination; example: internet, x.25, frame relay; provide high degree of redundancy; variable delay, usually carry data (not voice)

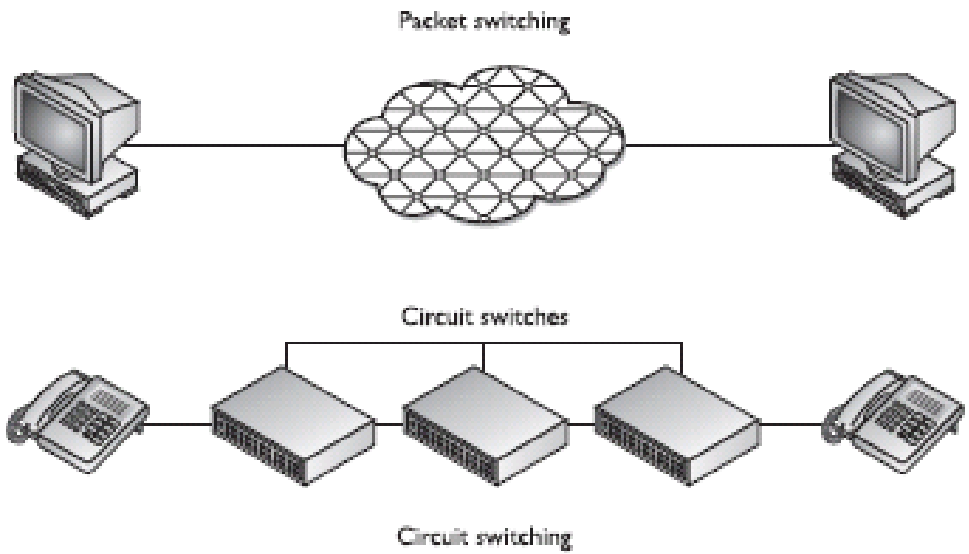


Figure 7-46 Circuit switching provides one road for a communication path, whereas packet switching provides many different possible roads.

Frame Relay

- Frame Relay is a WAN protocol at data link layer, packet switching
- Diff companies or diff sites connect to the cloud which is provided by carrier.
- Pay for Committed Information Rate (CIR) at each site
- *Two devices: **DTE** (Data Terminal Equipment) from customer (such as router, switch) and **DCE** (Data Circuit-Terminating Equipment) from provider*
- Cheaper and more flexible than dedicated line

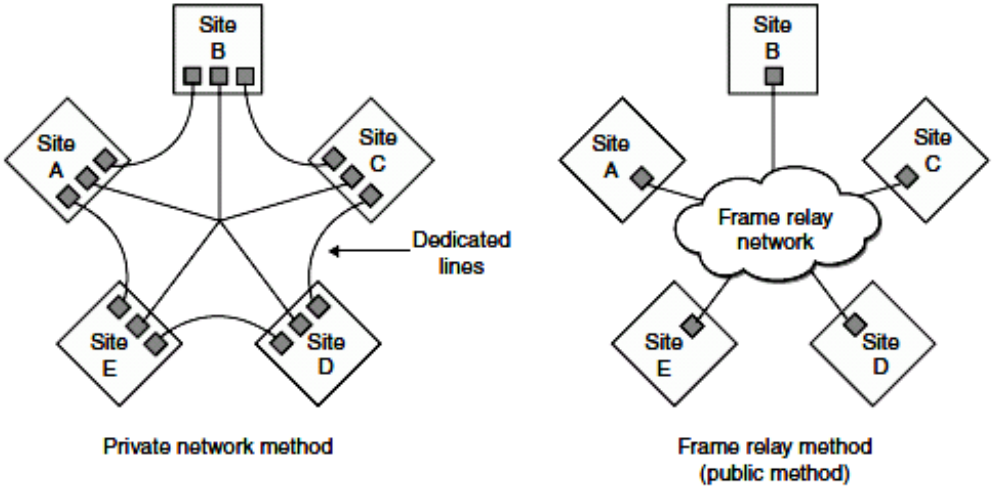


Figure 7-47 A private network connection requires several expensive dedicated links. Frame relay enables users to share a public network.

X.25 & ATM

- **X.25**
  - is older WAN protocol (1970); switching; any-to-any connection;
  - pay for bandwidth use
  - data divided into 128 bytes in High-Level Data Link control (HDLC) frame
  - weak: not advanced as frame relay; many layer error checking and correcting and fault tolerance
- **ATM (Asynchronous Transfer Mode)**
  - is cell-switching technology; high speed technology used for LAN, MAN, WAN and service provider connection
  - use 53 bytes fixed size cell provides more efficient and faster
  - ATM setup virtual circuits and guarantee bandwidth and **QoS**
  - Good for voice and video transmission
  - ATM technology is used by carrier to make up part of internet
  - Also used in company's backbone.

QoS

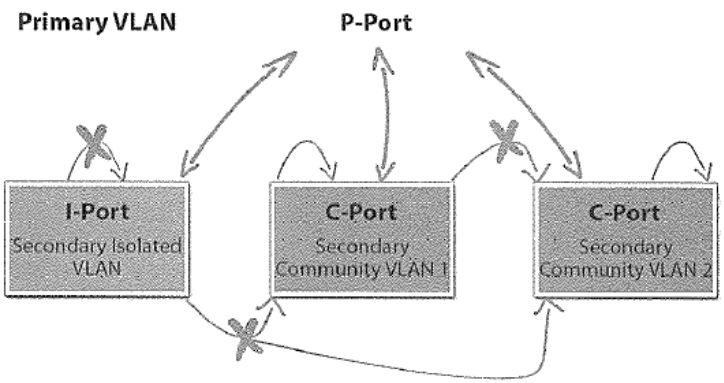
- **Quality of Service (QoS)**
  - to allow a protocol to distinguish between diff classes of message and assign priority levels.
    - **Constant bit rate (CBR)**: for time sensitive, such as voice and video
    - **Variable bit rate (VBR)**: for delay-insensitive, uneven application, customer specify high/low
    - **Unspecified bit rate (UBR)**: no guarantee
    - **Available bit rate (ABR)**: can provide more bandwidth if available after a guaranteed rate
  - First used in ATM, used in others now

C5. Virtualized Networks

- **Software Defined Network (SDN):**
  - **Decoupling** traditional **Switching/Routing** and using **Software defined** to distribute network more effectively & efficiency.
- **Software Defined Storage (SDS)**:
  - Include Intelligent Data Placement, SW-based Controller, Software RAID

Port Isolation (= Private VLAN)

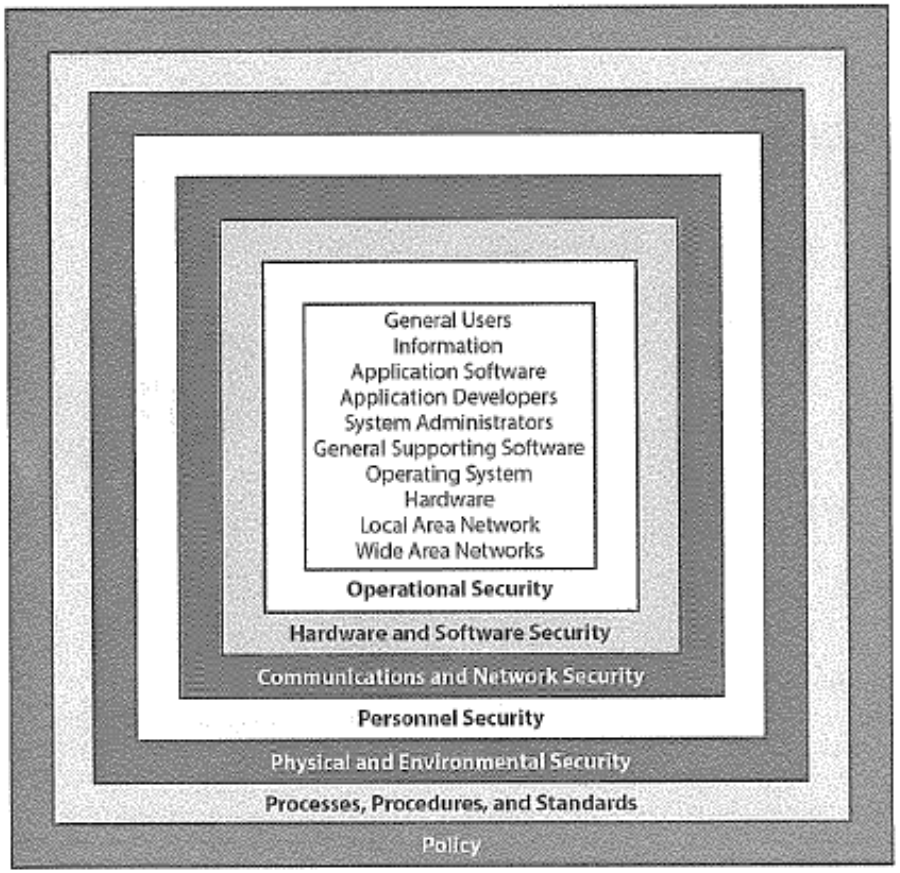
- Extending the Abilities of a VLAN
  - **Promiscuous** (P-Port): The switch port connects to a router, so it can connect to all other ports.
  - **Isolated** (I-Port), can communicate with Router only
  - **Community** (C-Port): can communicate within same community, not other community.



	I-Port	P-Port	C1-Port	C2-Port	Uplink to Switch2
I-Port	Deny	Permit	Deny	Deny	Permit
P-Port	Permit	Permit	Permit	Permit	Permit
C1-Port	Deny	Permit	Permit	Deny	Permit
C2-Port	Deny	Permit	Deny	Permit	Permit
Uplink to Switch2	Permit/Deny	Permit	Permit	Permit	Permit

D. Prevent or mitigate network attacks

- **Network can be:**
  - **Enabler**
  - **Channel of Attack**
  - **Bastion of Defense: like layer defense**



D. Prevent or mitigate network attacks

- **Network Security Objectives**
  - **Confidentiality**: Sniffing
  - **Integrity**: Modifying SMTP
  - **Availability**: Denial of Service (DoS)

Protection and tool

- **Open Mail Relay Servers:** Blacklist or Whitelist of email domain to against Spam
- **Port Scanning:** to find vulnerabilities and to fingerprinting OS by evaluating response time, detail of handshake
- **Intrusion Detection System (IDS)**
- **Security Event/Incident Management (SEIM):** Collect log and event from different devices and consolidate with sophisticated reporting
- **Vulnerability Assessment**: find out vulnerabilities by reviewing documentation, structure, functionality, code etc.
- **Penetration** Testing: Simulating attack
- **Network Taps**: device to copy all data of network traffic for the purpose of analysis, diagnostics, maintenance, forensic analysis.

D. Prevent or mitigate network attacks

- **Denial of Service (DoS)**
  - sending malformed packet to hurt bandwidth, file system quota, memory allocation and CPU utilization
- **Smurf**
  - Broadcast ICMP (Internet control message protocol) with victim's IP
  - All PC send "ECHO REPLY" to victim's PC
  - Countermeasure: disable direct broadcast; disallow internal source IP in perimeter router, allow necessary ICMP; network-based IDS; appropriate patch
- **Fraggle**
  - similar to Smurf, but use UDP (user datagram protocol)

Attacks

- **SYN Flood**
  - attacker sends SYN from invalid IP
  - victim commits connection and sends SYN/ACK, but never receive ACK
  - system will be hanged in a dozen times
  - not take a lot of bandwidth
  - will hang up 1-23 minutes
  - Countermeasure: decrease timeout; increase connection queue size; patch; network-based IDS; Firewall
- **Teardrop**
  - packet may need to be fragmented and recombined
  - network specify Maximum Transaction unit (MTU) for max packet size, but not minimum
  - attacker sends many very small and malformed fragment
  - victim can not handle and get freeze or reboot
  - Countermeasure: patch; disallow malformed fragment; use router to combines

Attacks

- **Distributed Denial of Service**
  - logical extension of DoS
  - use hundreds or thousands to computer (or zombie)
  - countermeasure: restrict unnecessary ICMP and UDP; network-based IDS; hardening; rename admin & strict password; perimeter router;

Spoofing

- **Spoofing** attack: falsifying data on a telecommunications network
  - **IP** address spoofing
  - **Caller ID** spoofing
  - **E-mail** spoofing
  - **DNS** spoofing: incorrect record sends from DNS server to another one
  - **Protocol** spoofing, a technique to increase performance in data communications
  - **SMS** spoofing
  - **Website** spoofing
  - **GPS** spoofing