COMPUTER NETWORKS

MODULE V

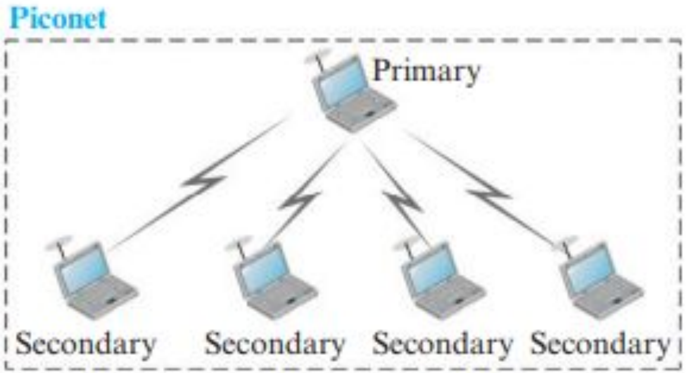
BLUETOOTH (IEEE 802.15 std)

- It is a wireless LAN technology designed to connect different types of devices which are at a shorter distance.
- It is a wireless personal-area network (PAN)
- It is an adhoc network, which means that the network is formed spontaneously.
- Two types of bluetooth networks: piconet, scatternet

Piconets:

- It is a bluetooth network
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- Secondary stations cannot communicate with each other directly.
- It also have 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

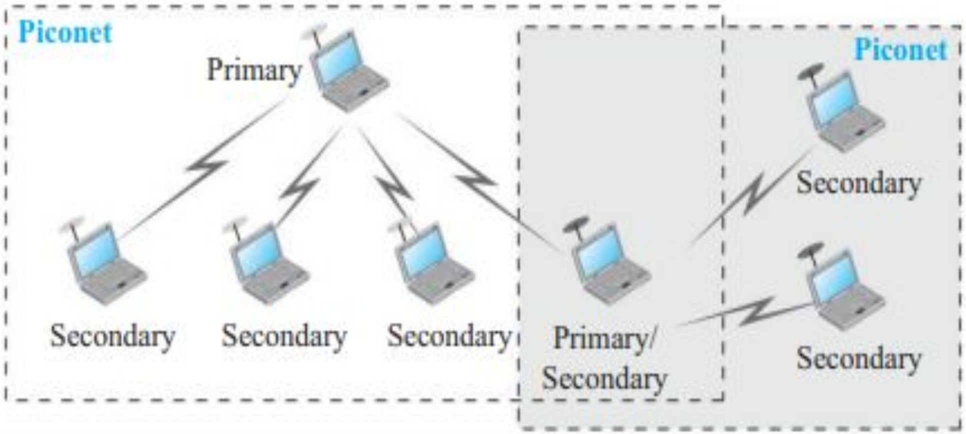
Figure *Piconet*



Scatternet:

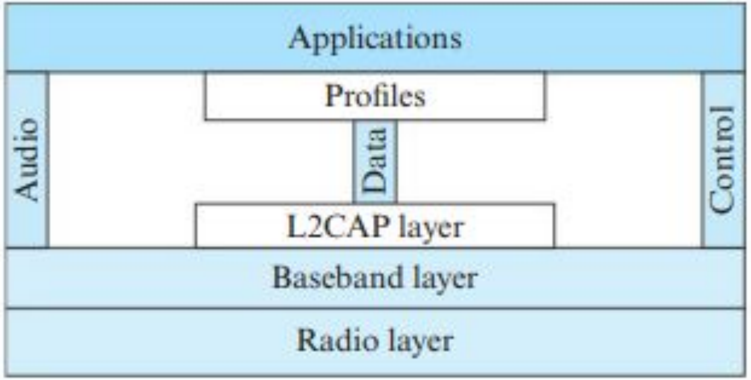
- It is a combination of piconets.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.

Figure *Scatternet*



Bluetooth Protocol Architecture:

Figure *Bluetooth layers*



- **Radio Layer:**
  - It corresponds to the physical layer of OSI model.
  - It deals with ratio transmission and modulation.
  - It uses 2.4 GHz ISM band in a range of 10 meters.
  - Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method.
- **Baseband Layer:**
  - is equivalent to the MAC sublayer in LANs.
  - uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA)
  - Master and slave stations communicate with each other using time slots of 625 µsec.
  - In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
  - **Single-Secondary Communication:**
    - The primary uses even-numbered slots (0, 2, 4, …); the secondary uses odd-numbered slots (1, 3, 5, …)
    - In slot 0, the primary sends and the secondary receives; in slot 1, the secondary sends and the primary receives. The cycle is repeated.
  - **Multiple-Secondary Communication:**
    - the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.
    - All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

- In Baseband layer, two types of links can be created between a primary and a secondary. These are:
    - **Asynchronous Connection-less (ACL):**
        - is used when data integrity is more important than avoiding latency
        - If the data gets corrupted, it will be retransmitted.
    - **Synchronous Connection-Oriented (SCO):**
        - It is used when fast delivery is needed.
        - No retransmissions even if data gets corrupted
        - used for real-time audio where avoiding delay is all-important

- **Logical Link, Control Adaptation Protocol Layer (L2CAP):**
    - is equivalent to logical link control sub-layer of LAN.
    - The ACL link uses L2CAP for data exchange but sco channel does not use it.
    - The various functions of L2CAP are:

i) Segmentation and reassembly:

- L2CAP receives the packets of up to 64 KB from upper layers and divides them into frames for transmission.
- It adds extra information to define the location of frame in the original packet.
- The L2CAP reassembles the frame into packets again at the destination.

ii) Multiplexing:

- L2CAP performs multiplexing at sender side and de-multiplexing at receiver side.

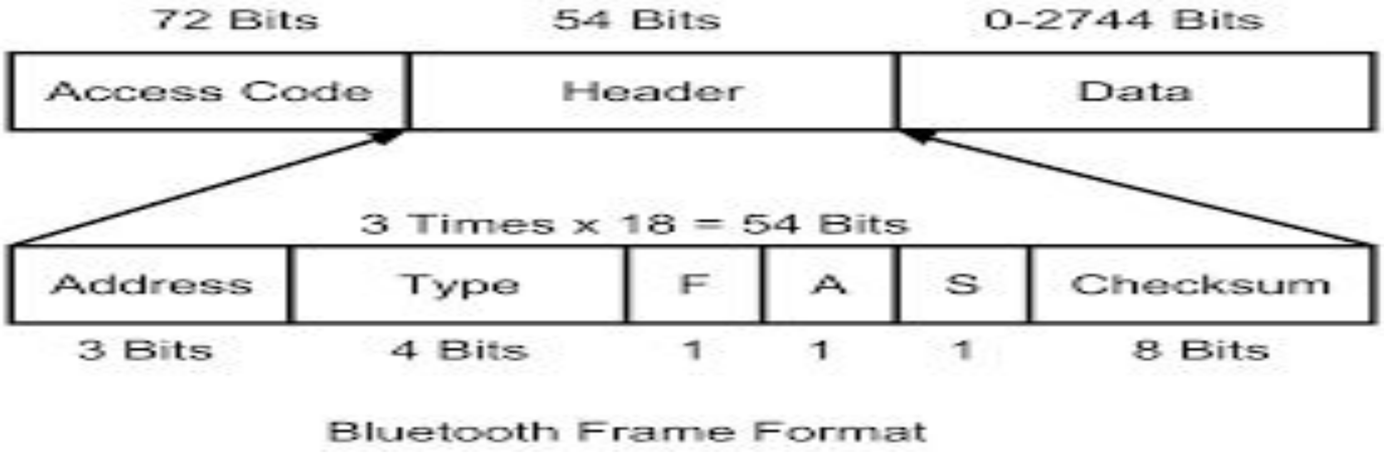
- At the sender site, it accepts data from one of the upper layer protocols, frames them and deliver them to the Baseband layer.
- At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol 1ayer.

iii) Quality of Service (QOS):

- L2CAP handles quality of service requirements, both when links are established and during normal operation.

iv) Group Management

Bluetooth Frame Format:



- **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.
- **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 times.

The header field contains following sub-fields:

(i) **Address**: This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) **A**: This bit is used for acknowledgement.

(v) **S**: This bit contains a sequence number of the frame to detect re-transmission. As stop and wait protocol is used, one bit is sufficient.

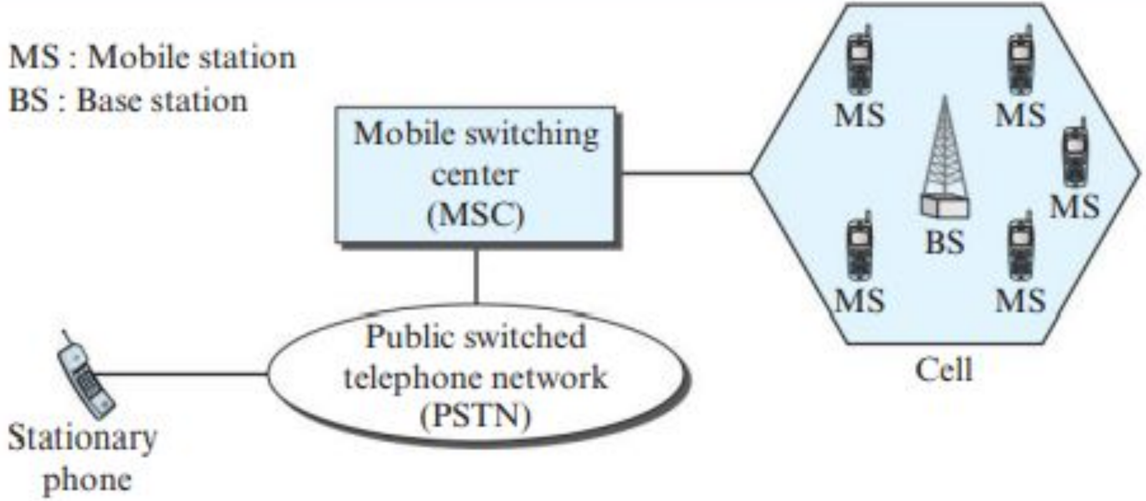
(vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.

- **Payload**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers.

CELLULAR NETWORKS

Cellular Telephony

Figure *Cellular system*

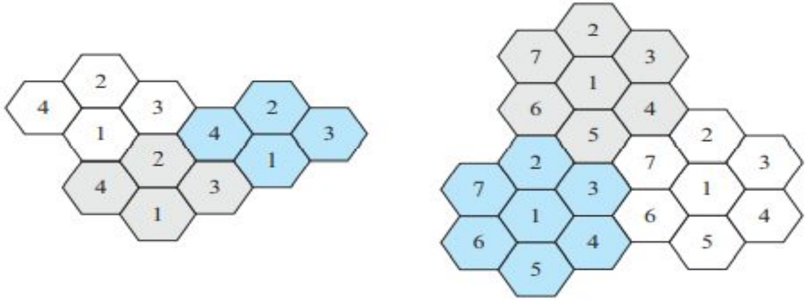

MS : Mobile station
BS : Base station
Mobile switching center (MSC)
Public switched telephone network (PSTN)
Stationary phone
MS
MS
MS
BS
MS
MS
Cell

- Cellular telephony is designed to provide communications between two moving units, called mobile stations (MSs), or between one mobile unit and one stationary unit, often called a land unit.
- A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
- Each cellular service area is divided into small regions called cells.
- Each cell contains an antenna and is controlled by a solar- or AC powered network station, called the base station (BS).
- Each base station, in turn, is controlled by a switching office, called a mobile switching center (MSC).
- The MSC coordinates communication between all the base stations and the telephone central office. It is a computerized center that is responsible for connecting calls, recording call information, and billing.
- Cell size is not fixed(radius from 1 to 30 kms).
- High-density areas require more, geographically smaller cells to meet traffic demands than do low-density areas.

Frequency-Reuse Principle:

- The frequency reuse factor is the rate at which the same frequency can be used in the
- network.
- Neighboring cells cannot use the same set of frequencies for communication because it may create interference for the users located near the cell boundaries.
- However, the set of frequencies available is limited, and frequencies need to be reused.
- A frequency reuse pattern is a configuration of N cells, N being the reuse factor, in which each cell uses a unique set of frequencies.
- When the pattern is repeated, the frequencies can be reused.
-

Figure *Frequency reuse patterns*



a. Reuse factor of 4

b. Reuse factor of 7

- The cells with the same number in a pattern can use the same set of frequencies (resuing cells).

Transmitting:

- To place a call from a mobile station, the caller enters a code 10 digits (a phone number) and presses the send button.
- The mobile station then scans the band, seeking a setup channel with a strong signal, and sends the data (phone number) to the closest base station using that channel.
- The base station relays the data to the MSC. The MSC sends the data on to the telephone central office.
- If the called party is available, a connection is made and the result is relayed back to the MSC. At this point, the MSC assigns an unused voice channel to the call, and a connection is established.
- The mobile station automatically adjusts its tuning to the new channel, and communication can begin.

Receiving:

- When a mobile phone is called, the telephone central office sends the number to the MSC.
- The MSC searches for the location of the mobile station by sending query signals to each cell in a process called paging.
- Once the mobile station is found, the MSC transmits a ringing signal and, when the mobile station answers, assigns a voice channel to the call, allowing voice communication to begin

Handoff:

- during a conversation, the mobile station may move from one cell to another.
- Thus the signal may become weak.
- So the MSC monitors the level of the signal every few seconds.
- If the strength of the signal diminishes, the MSC seeks a new cell that can better accommodate the communication.
- The MSC then changes the channel carrying the call (hands the signal off from the old channel to a new one).

Hard Handoff:

- In a hard handoff, a mobile station only communicates with one base station.
- When the MS moves from one cell to another, communication must first be broken with the previous base station before communication can be established with the new one.

Soft Handoff:

- A mobile station can communicate with two base stations at the same time.
- Thus during handoff, a mobile station may continue with the new base station before breaking off from the old one.

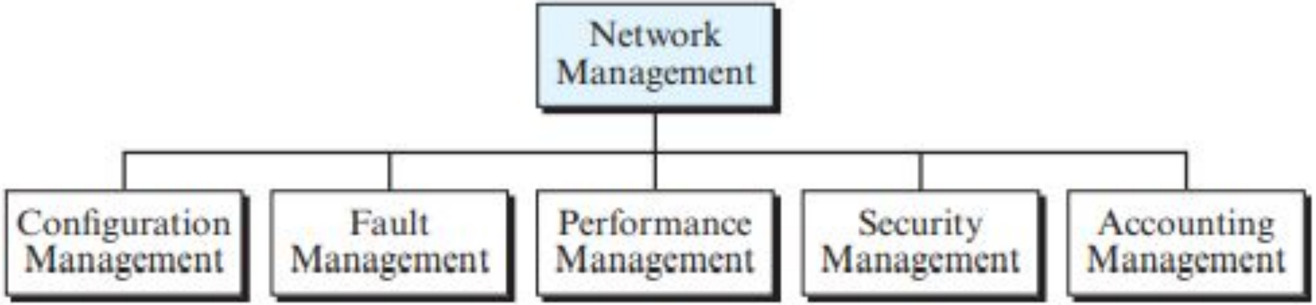
Roaming:

- A service provider usually has limited coverage. Neighboring service providers can provide extended coverage through a roaming contract.

Introduction to Network Management

- Network management includes the deployment, integration, and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

Figure *Areas of network management*



i) Configuration Management:

- Monitors the different devices in the managed network and their hardware and software configurations.
- **Reconfiguration:**
    - a daily occurrence in a large network.
    - **Hardware Reconfiguration:**
        - covers all changes to the hardware.
    - **Software Reconfiguration:**
        - covers all changes to the software.
    - **User-Account Reconfiguration:**
        - adding/removing users, creating groups, setting user-privileges etc
- **Documentation**:
    - The original network configuration and each subsequent change must be recorded.
    - **Hardware Documentation**
    - **Software Documentation**
    - **User-Account Documentation**

ii) Fault Management:

- It continuously monitors the status of each component individually and in relation to each other.
    - **Reactive Fault Management:**
        - It is responsible for detecting, isolating, correcting, and recording faults.
        - It handles short-term solutions to faults.
    - **Proactive Fault Management:**
        - It tries to prevent faults from occurring.

iii) Performance Management:

- It continuously monitors the performance of each device of the network.
- Capacity, Traffic, Throughput, Response Time

iv) Security Management:

- It is responsible for controlling access to the network based on predefined policy.

v) Accounting Management:

- is the controlling of users’ access to network resources through charges.

- There are three principal components of a network management architecture: a managing entity (the boss in our analogy above—you), the managed devices (the branch office), and a network management protocol.

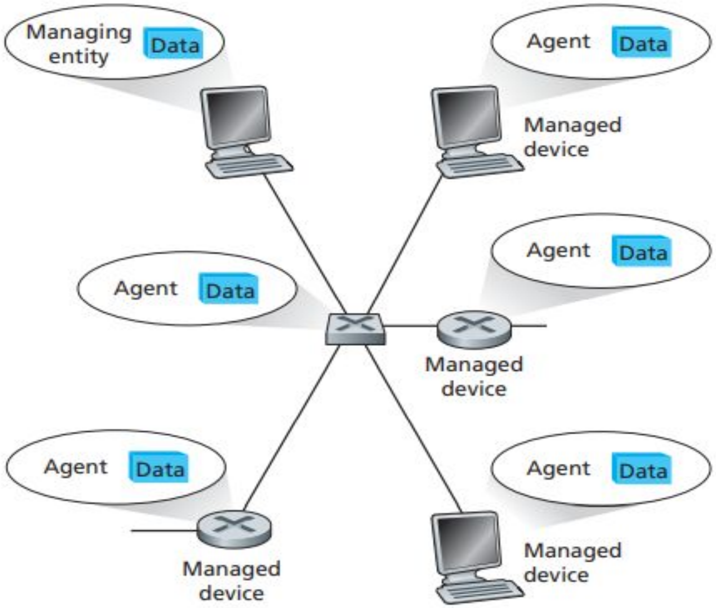


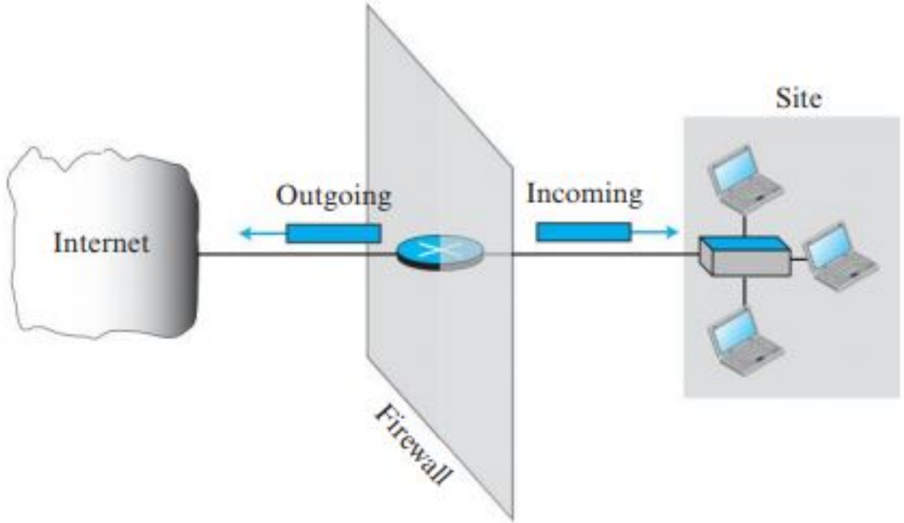
Figure ♦ Principal components of a network management architecture

FIREWALLS

- In a computer network, when traffic entering/leaving a network is security-checked, logged, dropped, or forwarded, it is done by operational devices known as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs).

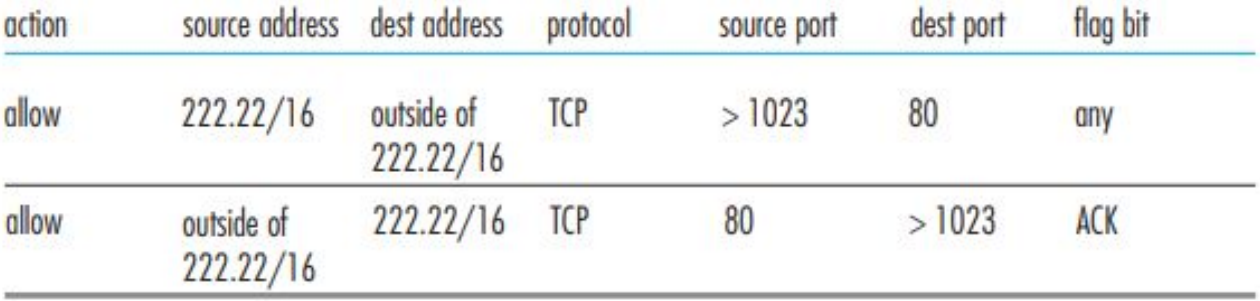
Firewalls:

- A firewall is a combination of hardware and software that isolates an organization’s internal network from the Internet at large, allowing some packets to pass and blocking others.
- It allows a network administrator to control access between the outside world and resources within the administered network by managing the traffic flow to and from these resources.
- A firewall has three goals:
    - All traffic from outside to inside, and vice versa, passes through the firewall
    - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
    - The firewall itself is immune to penetration.
- Types of firewalls:
    - traditional packet filters
    - stateful filters
    - application gateways


Site
Outgoing
Incoming
Internet
Firewall

i) Packet Filters:

- A packet filter examines each packet in isolation, determining whether the datagram should be allowed to pass or should be dropped based on administrator-specific rules.
- Packets are filtered based on
  - IP source or destination address
  - Protocol type in IP datagram field: TCP, UDP etc
  - source and destination port
- filtering is primarily done at the network layer (layer three) or the transport layer (layer four) of the OSI reference model.
- Firewall rules are implemented in routers with access control lists.

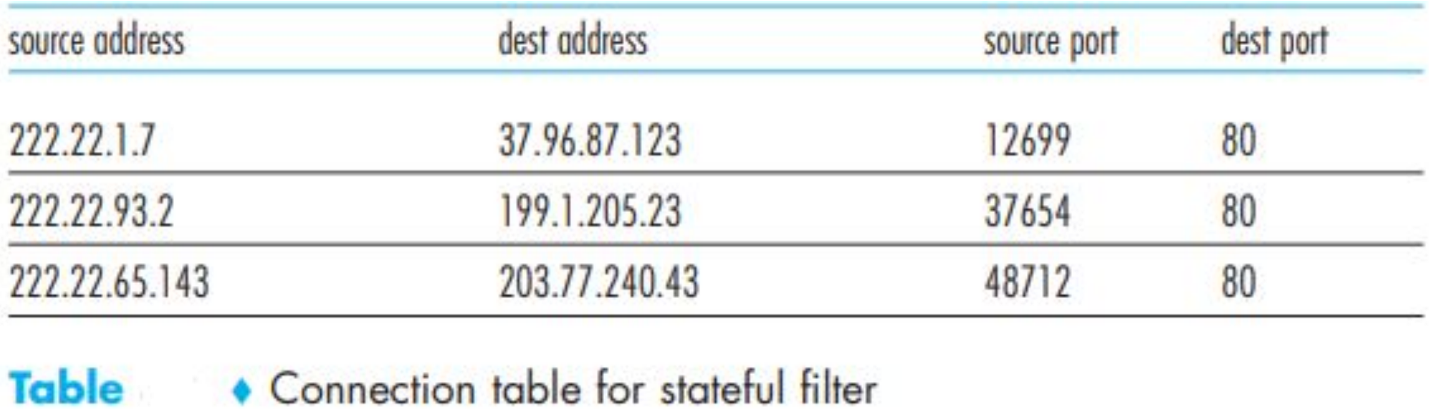


action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

Table ♦ An access control list

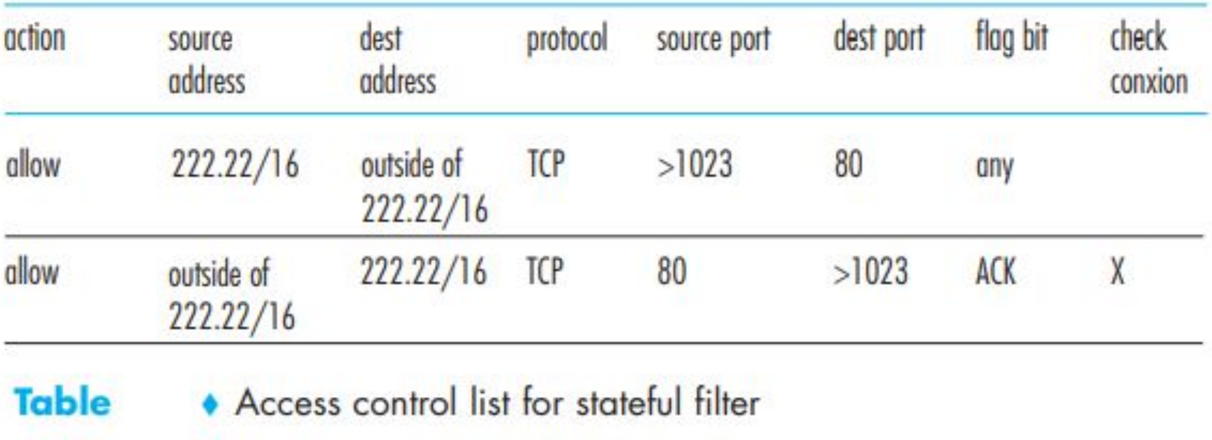
ii) Stateful Packet Filters:

- It monitors the full state of active network connections.
-



source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Table ♦ Connection table for stateful filter



action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	>1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	>1023	ACK	X

Table ♦ Access control list for stateful filter

- Suppose an attacker attempts to send a malformed packet into the organization’s network by sending a packet with TCP source port 80 and with the ACK flag set from a machine with IP address 150.23.23.155 and port number 12543.

iii) Application Gateway:

- An application gateway is an application-specific server through which all application data (inbound and outbound) must pass.
- Each gateway is a separate server with its own processes.

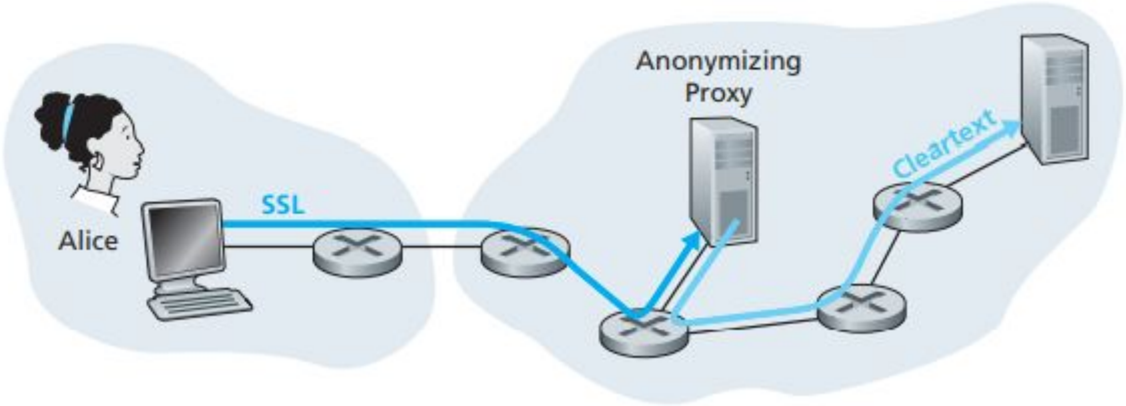


Figure ♦ Providing anonymity and privacy with a proxy

THREATS AND ATTACKS

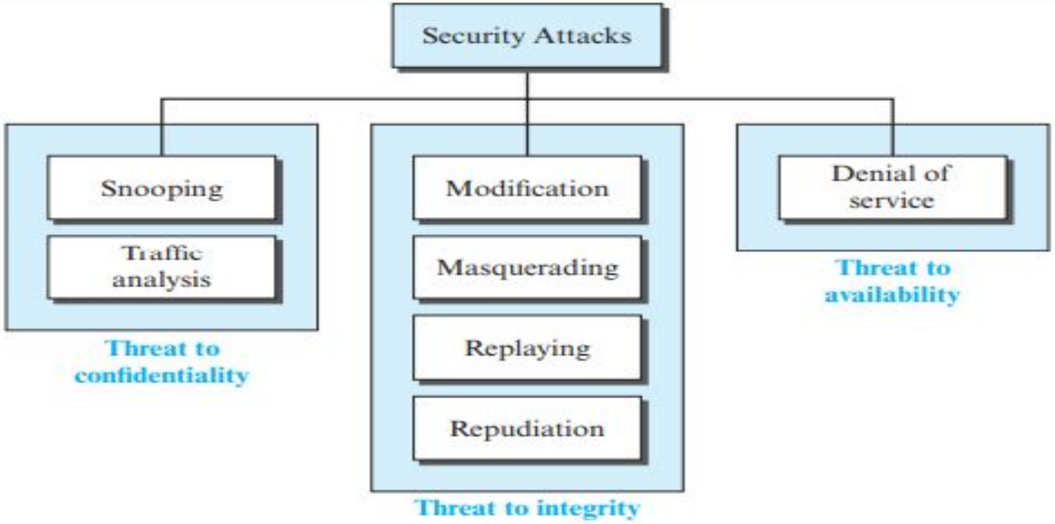
Network security

- Our three goals of security are
  - Confidentiality: for achieving this, we need to conceal it during transmission.
  - Integrity: changes need to be done only by authorized entities and through authorized mechanisms.
  - Availability: The information created and stored by an organization needs to be available to authorized entities

Attacks

- Our three goals of security —confidentiality, integrity, and availability —can be threatened by security attacks.

Figure *Taxonomy of attacks with relation to security goals*



I) Attacks Threatening Confidentiality:

- the two types of attacks that threatens the confidentiality of information are snooping and traffic analysis.
- **Snooping:**
    - It refers to unauthorized access to or interception of data.
    - To prevent snooping, we can encrypt the data so that it is not understandable to the interceptor.
- **Traffic Analysis:**
    - by monitoring online traffic, the interceptor can find the e-mail address of the sender or the receiver. He can also collect pairs of requests and responses to help him guess the nature of the transaction.

ii) Attacks Threatening Integrity:

- The integrity of data can be threatened by several kinds of attacks: modification, masquerading, replaying, and repudiation.
- **Modification:**
  - After accessing information, the attacker modifies the information like deleting or delaying the message to harm the system or to benefit from it.
- **Masquerading:**
  - Masquerading, or spoofing, happens when the attacker impersonates somebody else.
  - For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.
- **Replaying:**
  - The attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation:**
  - Such attack is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

iii) Attacks Threatening Availability:

- **Denial of Service:**
  - It may slow down or totally interrupt the service of a system.
  - The attacker might send so many bogus requests to a server that the server crashes because of the heavy load. Or
  - The attacker might intercept and delete a server’s response to a client, making the client believe that the server is not responding.

Overview of tools and troubleshooting

- Network troubleshooting tools are standalone or integrated solutions that help network administrators identify the root cause of a network issue in order to fix it.
- These network troubleshooting tools range from simple command line based troubleshooting utilities to more comprehensive and robust solutions that allows for a systematic, efficient and proactive approach to network troubleshooting.
- There are many programs and utilities available for Windows and UNIX operating systems that allow us to sniff, capture, trace, and analyze packets that are exchanged between our computer and the Internet.
- Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.
- Some of these, such as Wireshark and Ping Plotter have graphical user interface (GUI); others, such as traceroute, nslookup, dig, ipconfig, and ifconfig, are network administration command-line utilities.
- Any of these programs and utilities can be a valuable debugging tool for network administrators.

- Some of the basic network troubleshooting tools are as follows:
  - Ping
  - Tracert/ Trace Route
  - Ipconfig/ ifconfig
  - Netstat
  - Nslookup
  - Pathping/MTR
  - Route
  - PuTTY

- One of the tools that a host can use to test the liveliness of another host is the **ping** program. The **ping** program can also measure the reliability and congestion of the router. Ping can calculate the round-trip time.
- The **traceroute** program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination. It can find the IP addresses of all the routers that are visited along the path. The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- **ipconfig** is a console application program of some computer operating systems that displays all current TCP/IP network configuration values. ifconfig(interface configuration) command is used to configure the kernel resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.

- The **network statistics (netstat)** command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.
- **nslookup** is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping .
- The **PathPing** command is a command-line network utility supplied in Windows 2000 and beyond that combines the functionality of ping with that of tracert. It is used to locate spots that have network latency and network loss.
- **Route** is a command used to view and manipulate the IP routing table

- **PuTTY** is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection.
- The **echo request and the echo reply** pair of messages are used by a host or a router to test the liveliness of another host or router.
- The **timestamp request and the timestamp reply** pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.

NETWORK ANALYZERS

Network Analysis and Sniffing

- It is the process of capturing, decoding, and analyzing network traffic.
  - Why is the network slow?
  - What is the network traffic pattern?
  - How is the traffic being shared between nodes?

- Also known as traffic analysis, protocol analysis, sniffing, packet analysis etc.

Network Analyzer

- A combination of hardware and software tools that can detect, decode, and manipulate traffic on the network
- Available both free and commercially
- Mainly software-based (utilizing OS and NIC)
- Also known as sniffer
- A program that monitors the data traveling through the network passively