Topics
Networking Devices (Layer1,2)
Networking Devices (Layer 3)
Different types of network layer attacks
Firewall- ACL
Packet Filtering
DMZ, Alerts
Audit Trials
IDS
Advantages and Disadvantages of IDS(Need of IPS)
Advantages of IPS over IDS
IPS
IPS Types- Signature based
Anomaly based, Policy based
IPS Types - Honeypot based
Applications
Malicious Software

NETWORK DEVICES

Network Interface Card (NIC)

NIC stands on first place. Without this device, networking cannot be done.

This is also known as network adapter card, Ethernet Card and LAN card

A PC uses parallel data transmission technology to transmit data between its internal parts while the media that connects this PC with other PCs uses serial data transmission technology

A NIC converts parallel data stream into serial data stream and vice versa serial data stream is get converted in parallel data stream.

Types of NICs

There are two types of NICs

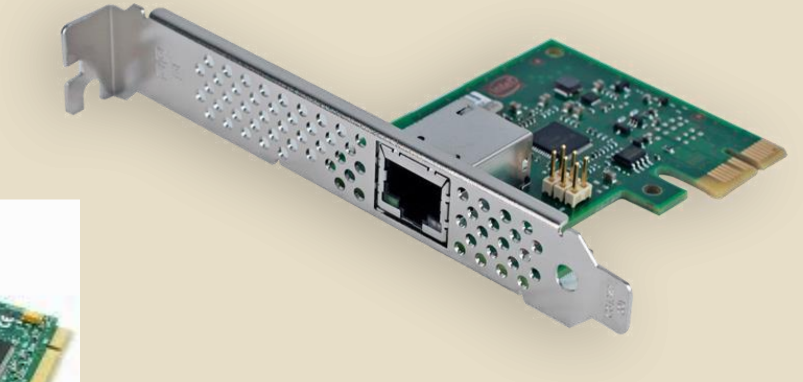
Media Specific :- Different types of NICs are required to connect with different types of media. For example we cannot connect wired media with wireless NIC card. Just like this, we cannot connect coaxial cable with Ethernet LAN card. We have to use the LAN card that is particularly built for the media type which we have.

Network Design Specific :- A specific network design needs a specific LAN card. For example FDDI, Token Ring and Ethernet have their own distinctive type of NICs card. They cannot use other's NIC card.

1 BNC and 1 RJ45 NIC

4 RJ45 NIC

PCMCIA for Laptops



Single RJ45 NIC

Token Ring NIC

Repeater

Repeater – A repeater operates at the physical layer.

Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

An important point to be noted about repeaters is that they do not amplify the signal.

When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

HUB

HUB operated at Physical Layer is used to connect multiple computers in a single workgroup LAN network. Typically HUBs are available with 4,8,12,24,48 ports.

Based on port type, there are two types of HUB:-

Ethernet HUB :- In this type of HUB all ports have RJ-45 connectors.

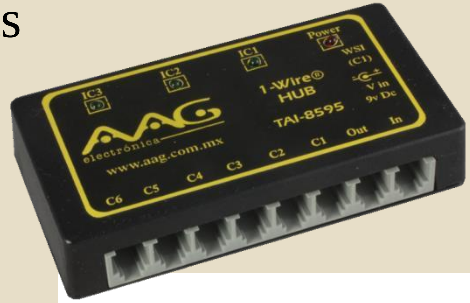
Combo HUB :- In this type of HUB ports have several different types of connectors such RJ-45, BNC, and AUI.

For Example a HUB which has four ports. Ports share everything. One port received data signal from its connected device. It will make three copies of data signal from HUB and give one copy to each port. Receiver port doesn’t need a copy of data signal for itself as it has it the original version.

When a hub receives signal on its port, it repeats the signal and forwards that signal from all ports except the port on which the signal arrived

There are two types of HUB

Passive HUB:- It forwards the data signal from all ports except the port on which signal arrived.
It doesn’t interfere in data signal.



Active HUB:- It also forwards the data signal from all ports except the port on which signal arrived. But before forwarding, it improves quality of data signal by amplifying it. Due to this added features active HUB
 is also known as repeaters.

Bridge

Bridge operates at data link layer

It is used to divide a large network in smaller segments.

For example a network has 70 nodes.

Without segmentation all these nodes will share same collision domain that will bring down overall network performance.

To run a network smoothly we should not place more than 20 nodes in a collision domain.

To deal with this situation we can use Bridge.

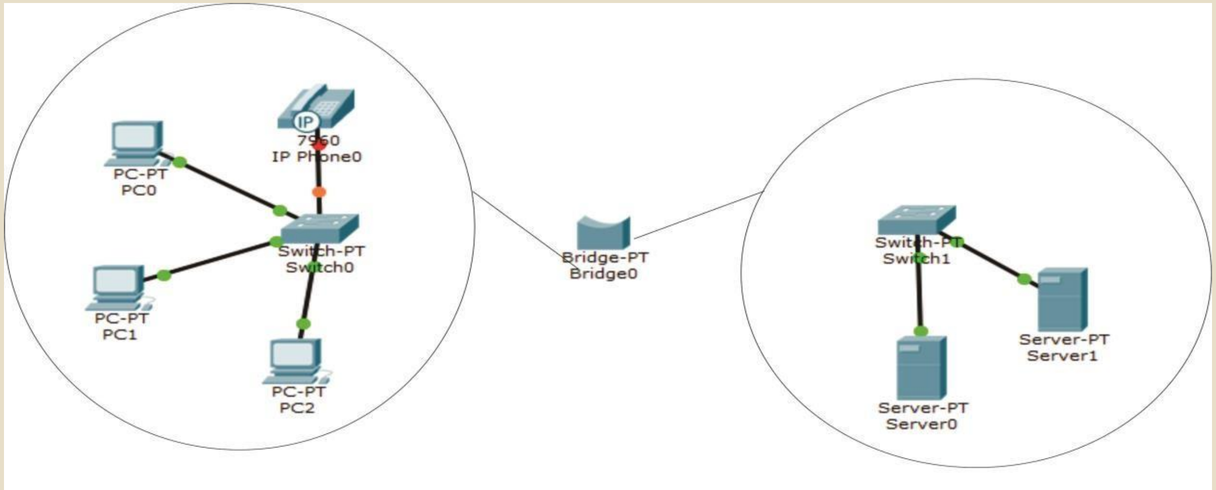
Bridge has per port collision domain which means if a port faces collision, other ports will not effect from this collision.

Basic function of Bridge are following :-

- Break a large network in smaller segments.
- Join different media types such as UTP with fiber optic.
- Join different network architectures such as Ethernet with Token Ring.

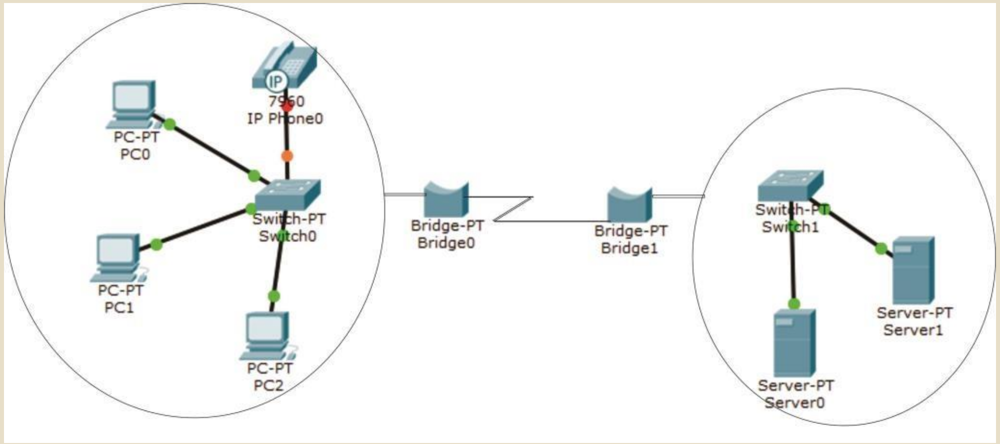
There are three types of bridge:-

Local Bridge :- This bridge connects two LAN segments directly. In Ethernet Implementation it is known as **Transparent** bridge. In Token Ring network it is called **Source-Routed** bridge

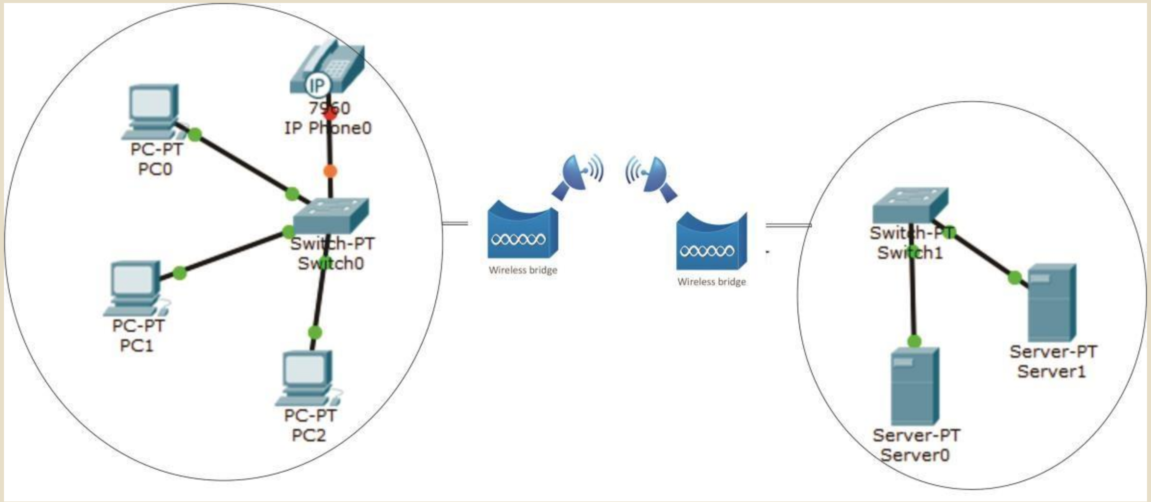


Remote Bridge :-

This bridge connects with another bridge over the WAN link.



Wireless Bridge :- This bridge connects with another bridge without wiring between them.



In OSI Layer model Bridge works at physical layer and data link layer.

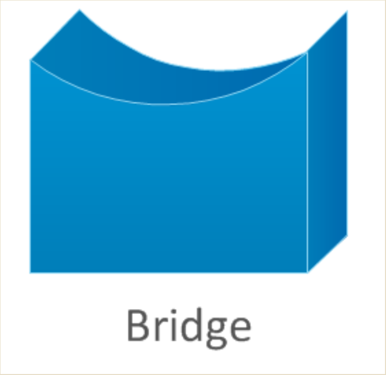
Bridges have following issues :-

•Bridges have limited ports

•In bridge forward decision are made through the software which slow down overall performance of network

•Bridges use age old technology which is not capable to fulfill the requirement of modern networks effectively

Switch and Router solves these issues



Switch

Just like Hub and Bridge, switch is also used to connect multiple computers together in a LAN segment.

Switch operates at data link layer

Switches available with 4,8,12,24,48,64 ports.

Each switch port has a separate collision domain.

At layer two data signals are formatted in frames.

When a switch receives frame, it checks FCS (Frame checksum sequence) field in it.

Switch process the frame only if it is valid.

All invalided frames are automatically dropped.

All valid frames are processed and forwarded to their destination MAC address.

Switches support three methods of switching

- Store and Forward
- Cut and Through
- Fragment Free

Store and Forward

This is the basic mode of switching. In this mode Switch buffers entire frame into the memory and run FCS (Frame Check Sequence) to ensure that frame is valid and not corrupted.

A frame less than 64bytes and higher than 1518bytes is invalid.

Only valid frames are processed and all invalid frames are automatically dropped.

Among these three methods, this method has highest latency.

Latency is the time taken by device in passing frame from it.

Cut and Through

Cut and Through method has lowest latency.

In this method Switch only read first six bytes from frame after the preamble. These six bytes are the destination address of frame.

This is the fastest method of switching.

This method also process invalid frames.

Only advantage of this method is speed.

Fragment Free

This is a hybrid version of ***Store and Forward method*** and *Cut and Through method*.

It takes goodies from both methods and makes a perfect method for switching.

It checks first 64 bytes of frame for error. It processes only those frames that have first 64bytes valid.

Any frame less than 64 bytes is known as **runt**. Runt is an invalid frame type.

This method filters **runt** while maintaining the speed.

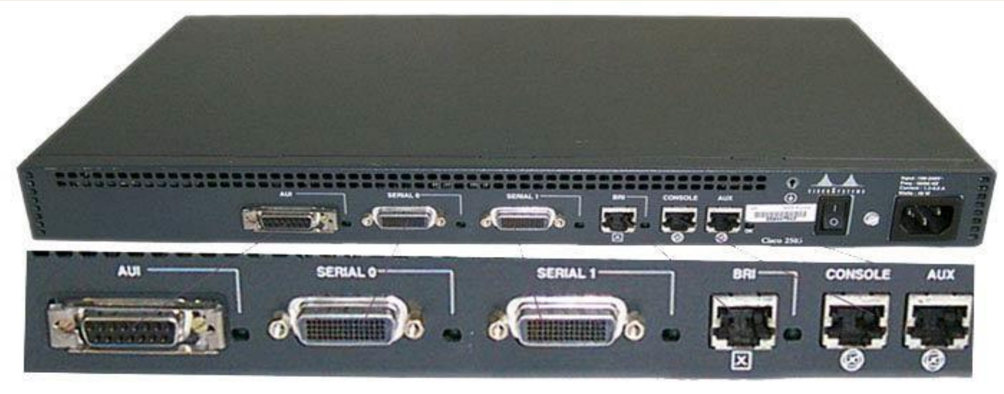
Routers

Router is a layer three device operates at Network Layer which forwards data packet from one logical network segment to another.

Router forwards packets on the bases of their destination address. For this router keeps record of the path that packets can use as they move across the network.

These records are maintained in a database table known as routing table.

Routing table can be built statically or dynamically



Basically routers are used :-

To connect different network segments.

To connect different network protocols such as IP and IPX.

To connect several smaller networks into a large network (known as internetwork)

To break a large network in smaller networks (Known as subnet usually created to improve the performance or manageability)

To connect two different media types such as UTP and fiber optical.

To connect two different network architectures such as token ring and Ethernet.

To connect LAN network with Telco company’s office (Known as DTE device).

To access DSL services (known as DSL Router).

Gateway and Brouter

Gateway –

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.

They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Brouter –

It is also known as bridging router is a device which combines features of both bridge and router.

It can work either at data link layer or at network layer.

Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

Definition of Computer Networks

A **Computer networks** is a collection of

nodes or computers or systems

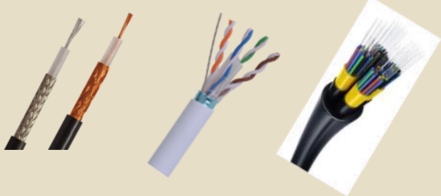
and **devices**

connected together through

communication devices

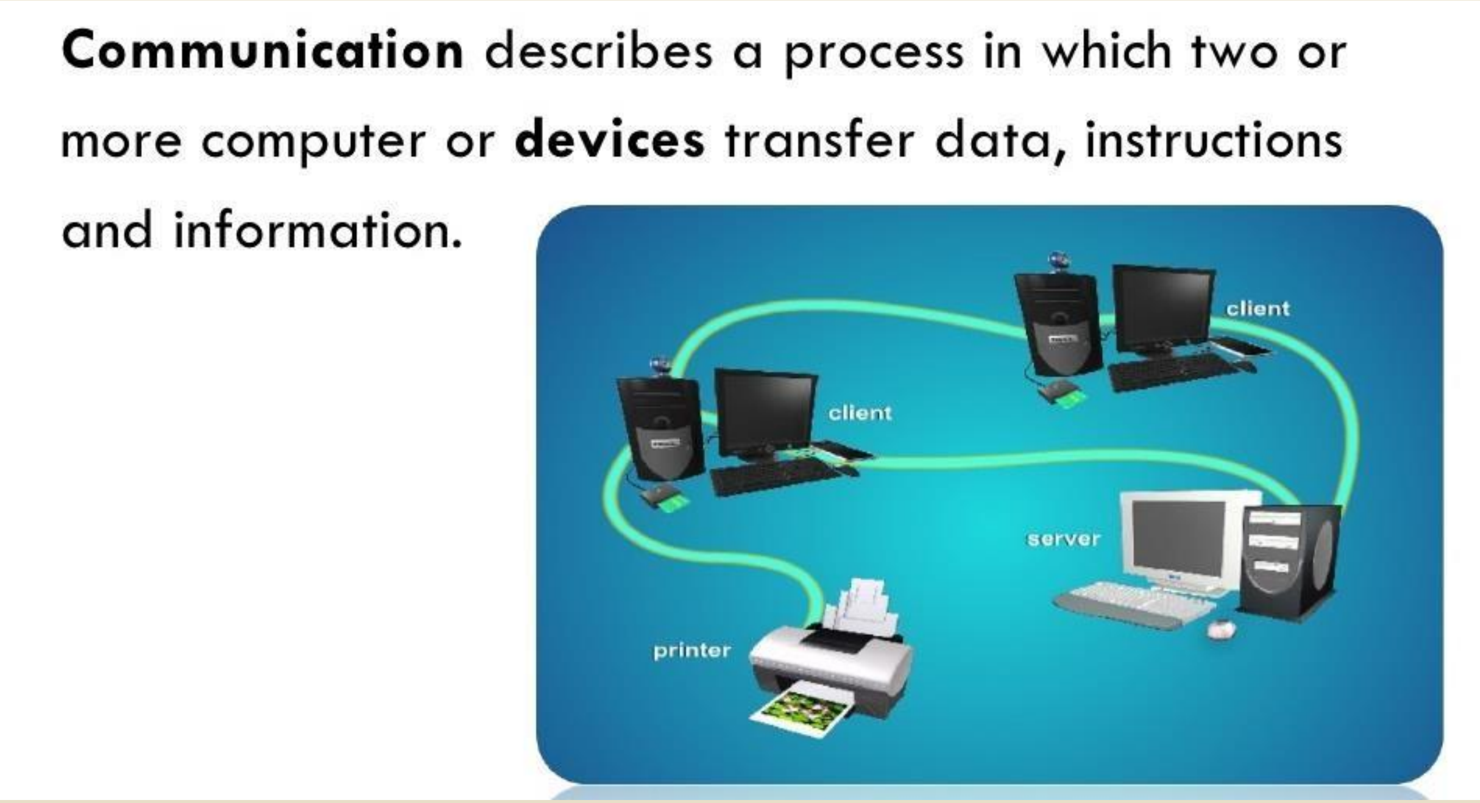
and **transmission media**

Guided Media



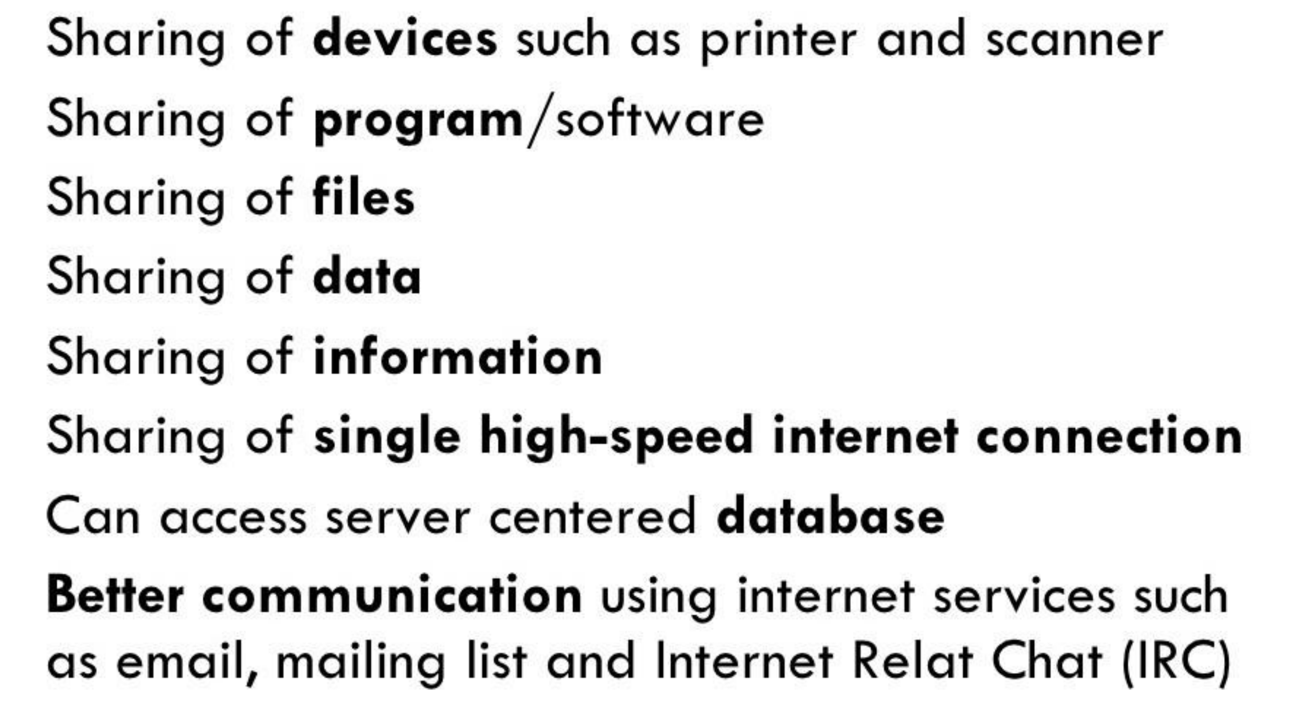
Wireless Media

Computer Communications



Communication describes a process in which two or more computer or **devices** transfer data, instructions and information.

Advantages of Networks



Sharing of **devices** such as printer and scanner

Sharing of **program**/software

Sharing of **files**

Sharing of **data**

Sharing of **information**

Sharing of **single high-speed internet connection**

Can access server centered **database**

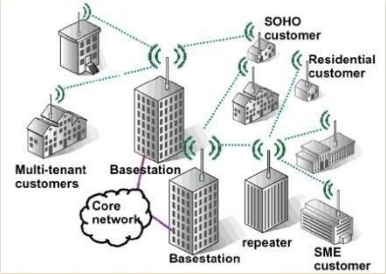
Better communication using internet services such as email, mailing list and Internet Relat Chat (IRC)

Different Types of Networks

Depending upon the geographical area covered by a network, it is classified as :

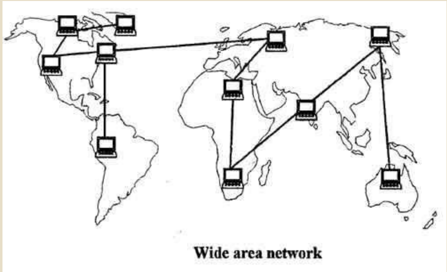
Local Area Network (LAN)

LAN
TechTerms.com



Metropolitan Area Network (MAN)

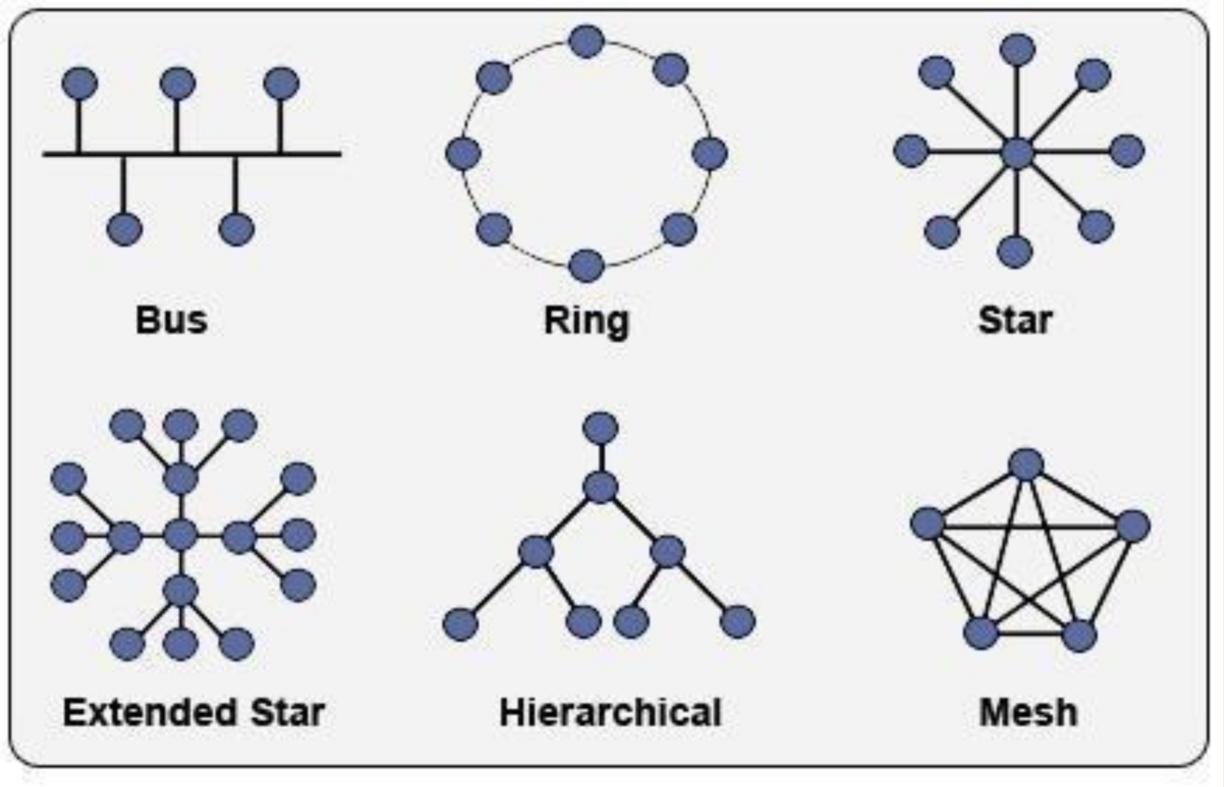
Wide Area Network (WAN)



PERSONAL AREA NETWORK(PAN)

Personal Area Network (PAN)

Networks



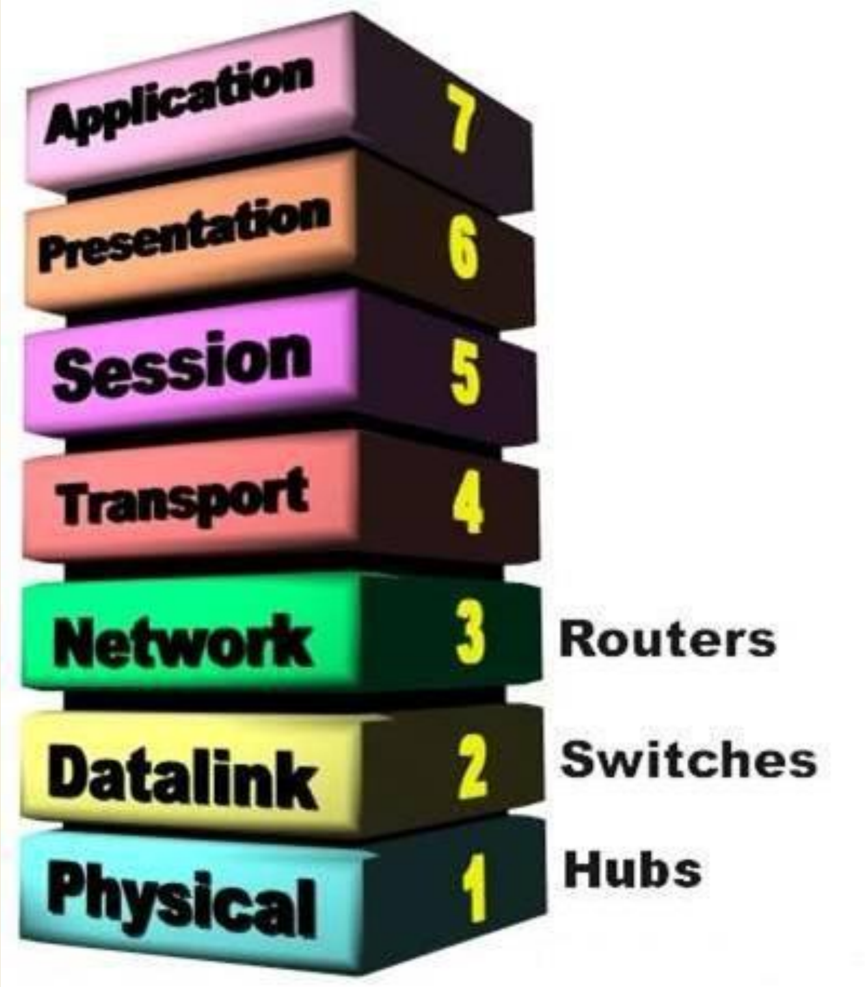
Topologies

Physical

The geometric arrangement of components that make up the LAN

Logical

The possible connections between pairs of networked end-points that can communicate


Application
7
Presentation
6
Session
5
Transport
4
Network
3
Routers
Datalink
2
Switches
Physical
1
Hubs

OSI Layers

Seven Layers of OSI

File Transfer, Email, Remote Login ❼

ASCII Text, Sound (syntax layer) ❼

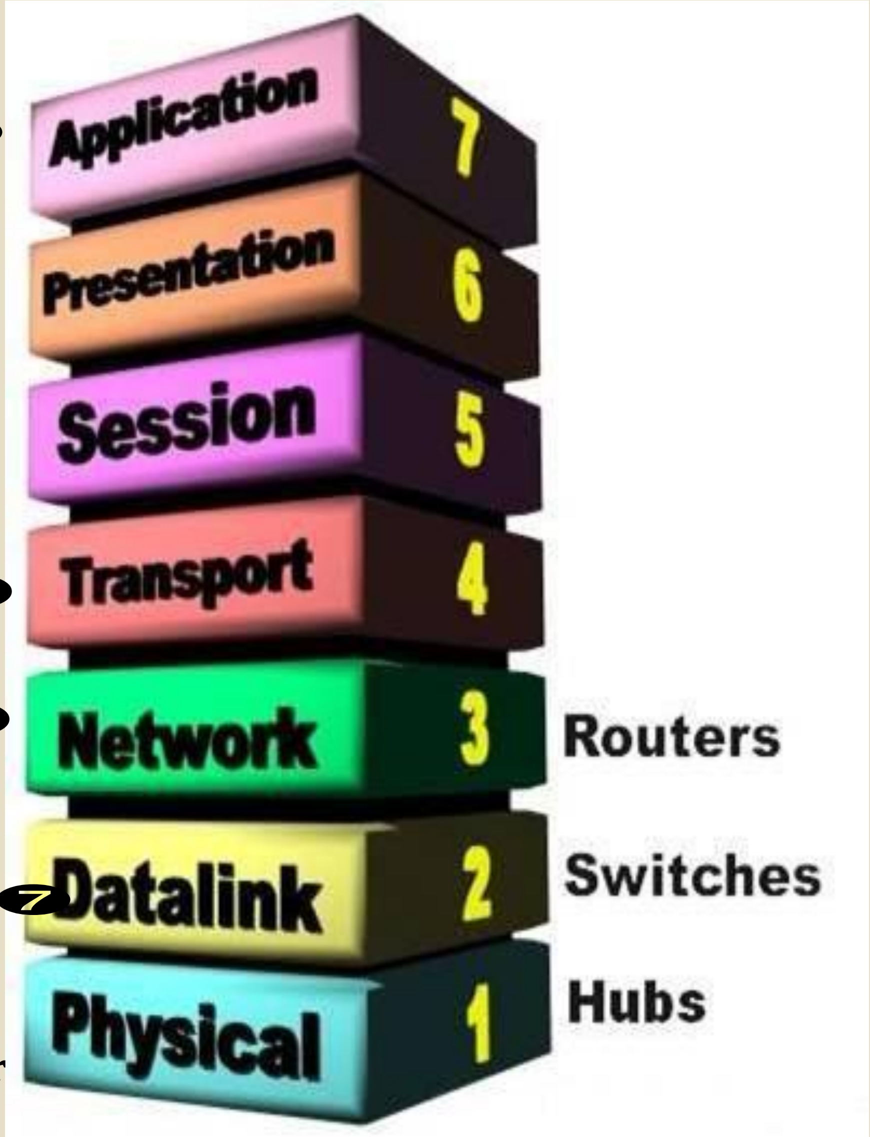
Establish/manage connection ❼

End-to-end control & error checking
(ensure complete data transfer): TCP ❼

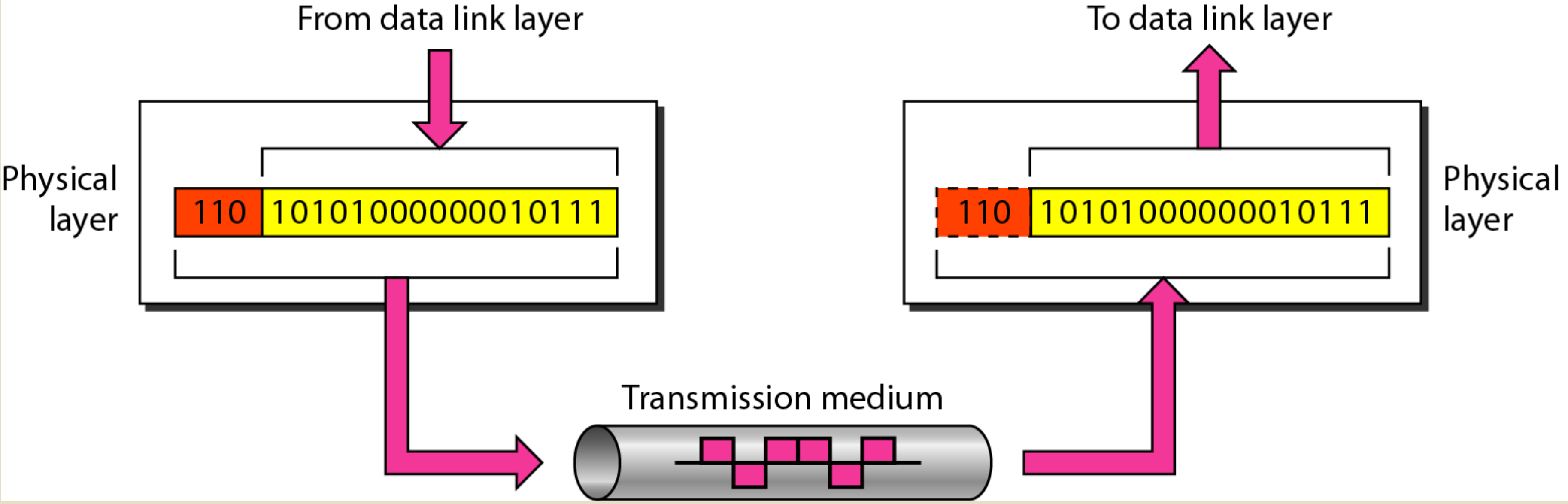
Routing and Forwarding Address: IP ❼

Two party communication: Ethernet ❼

How to transmit signal; coding Hardware
means of sending an receiving data on a carrier

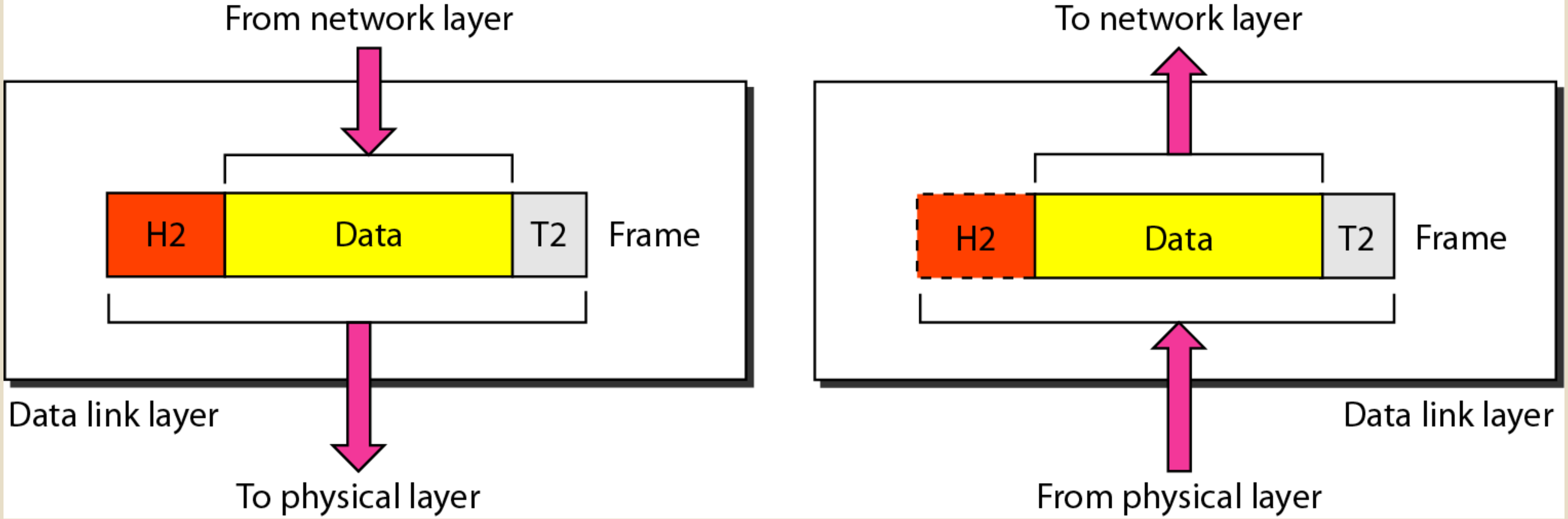


Physical layer



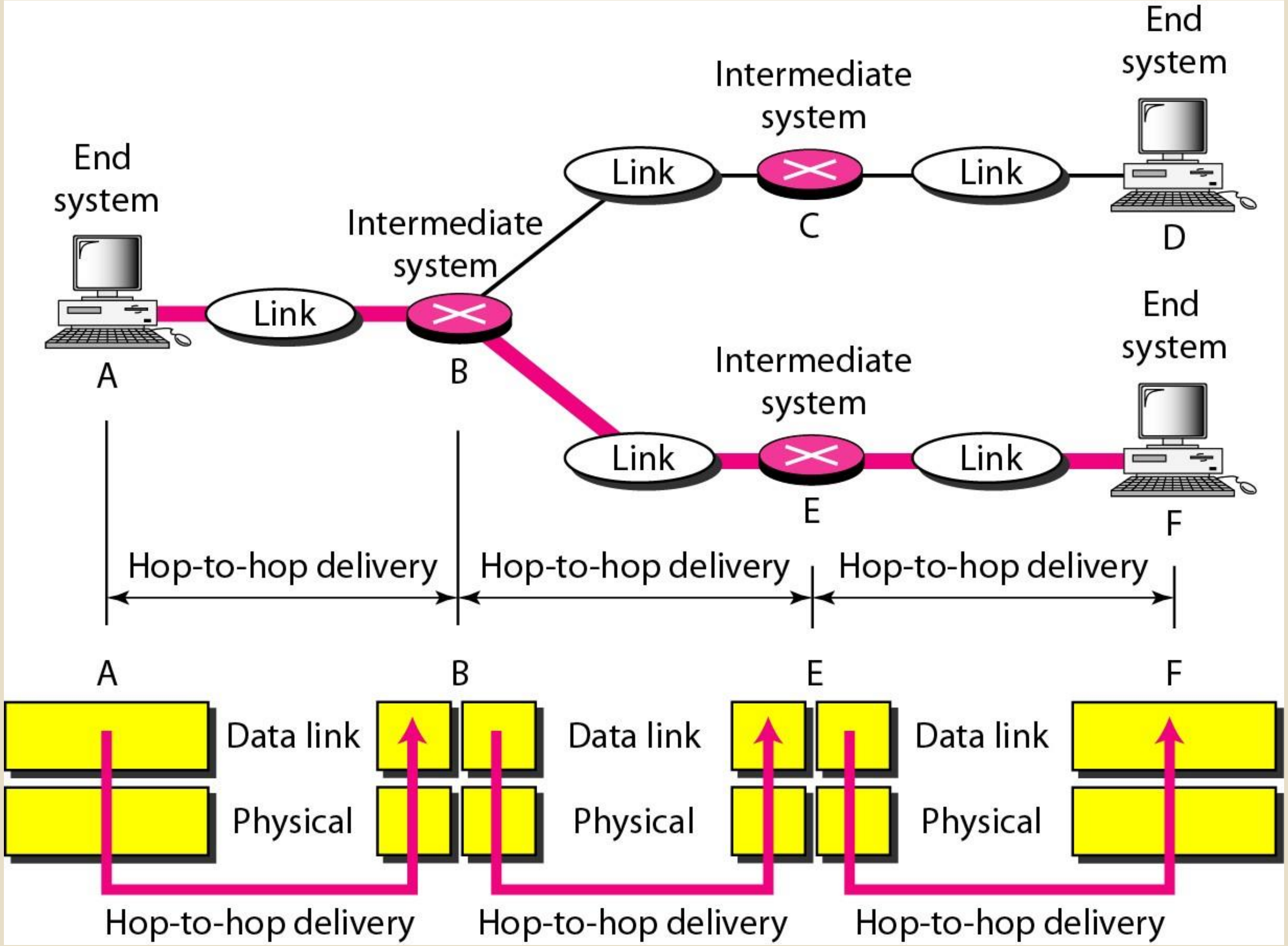
The physical layer is responsible for movements of

Data link layer

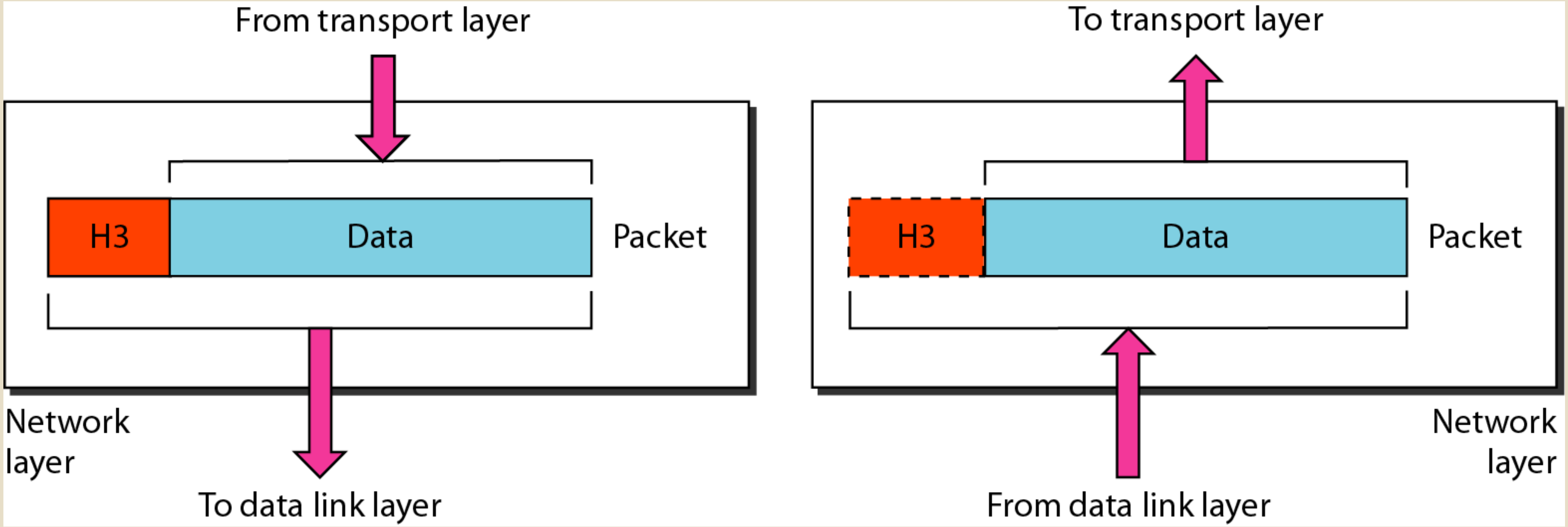


The data link layer is responsible for moving frames from one hop (node) to the next.

Hop-to-hop delivery

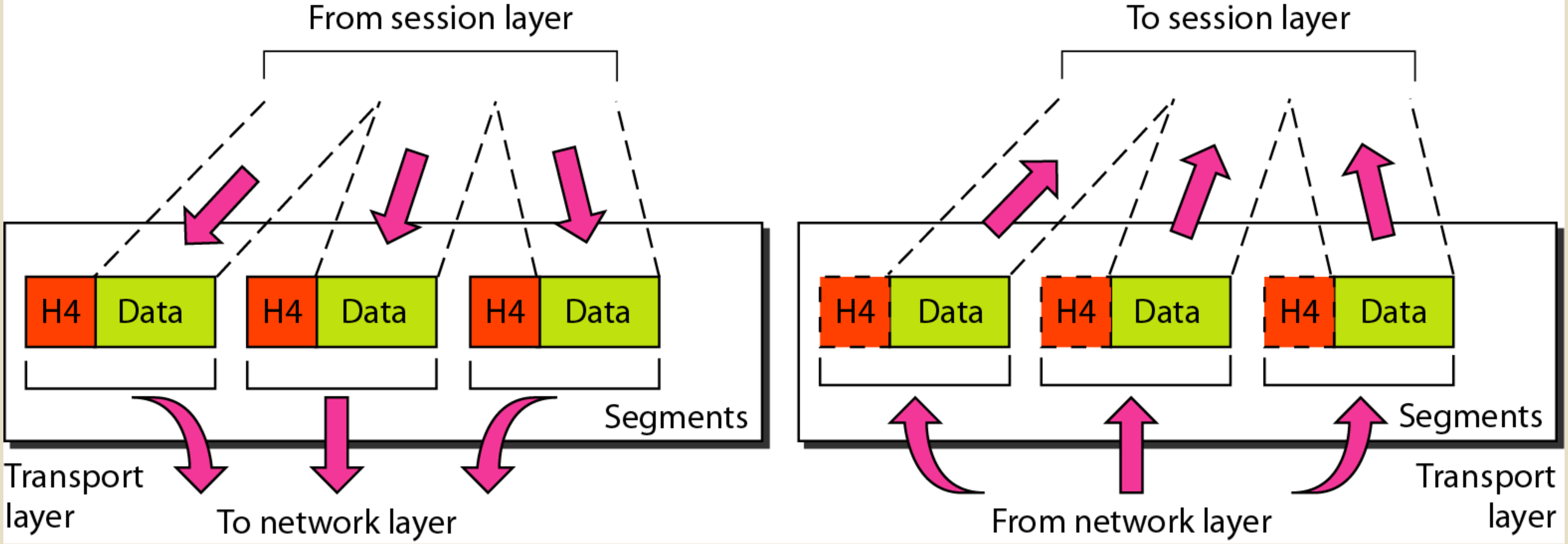


Network layer



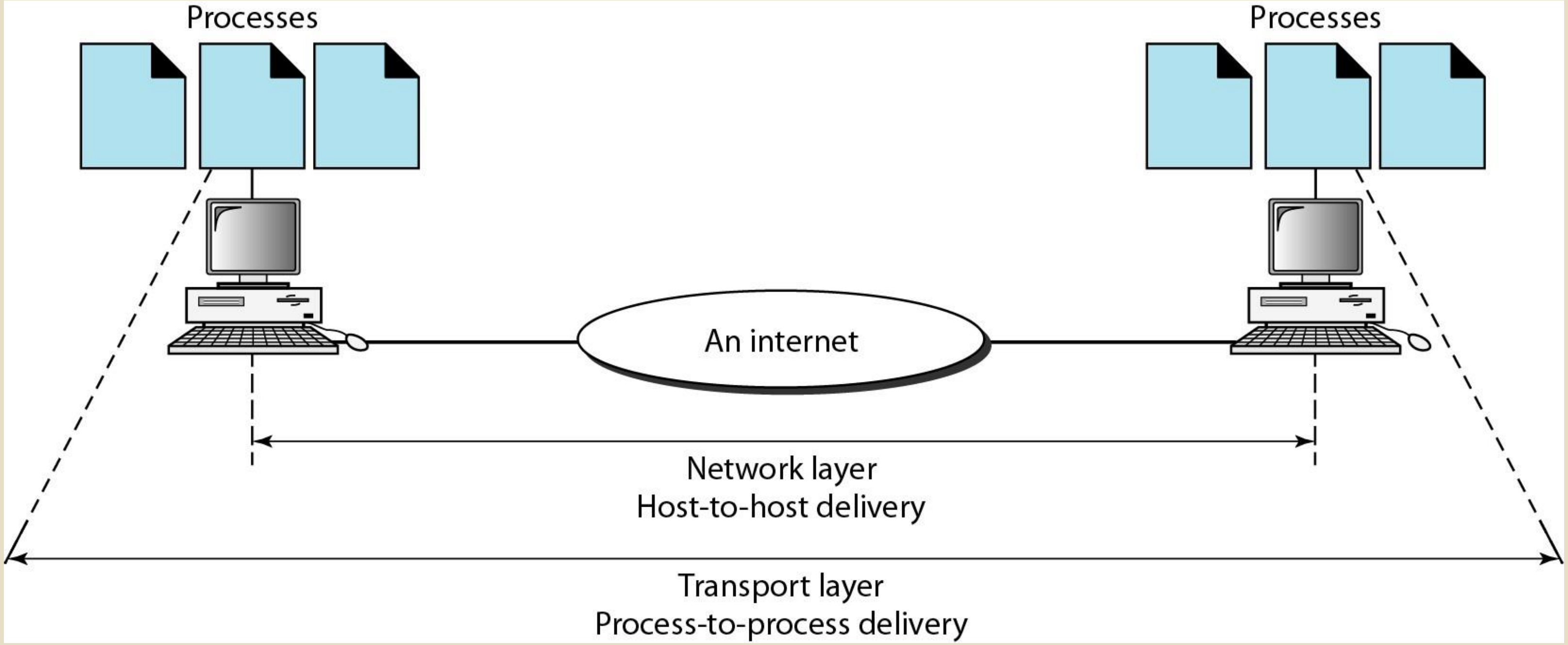
The network layer is responsible for the delivery of individual packets from the source host to the destination

Transport layer

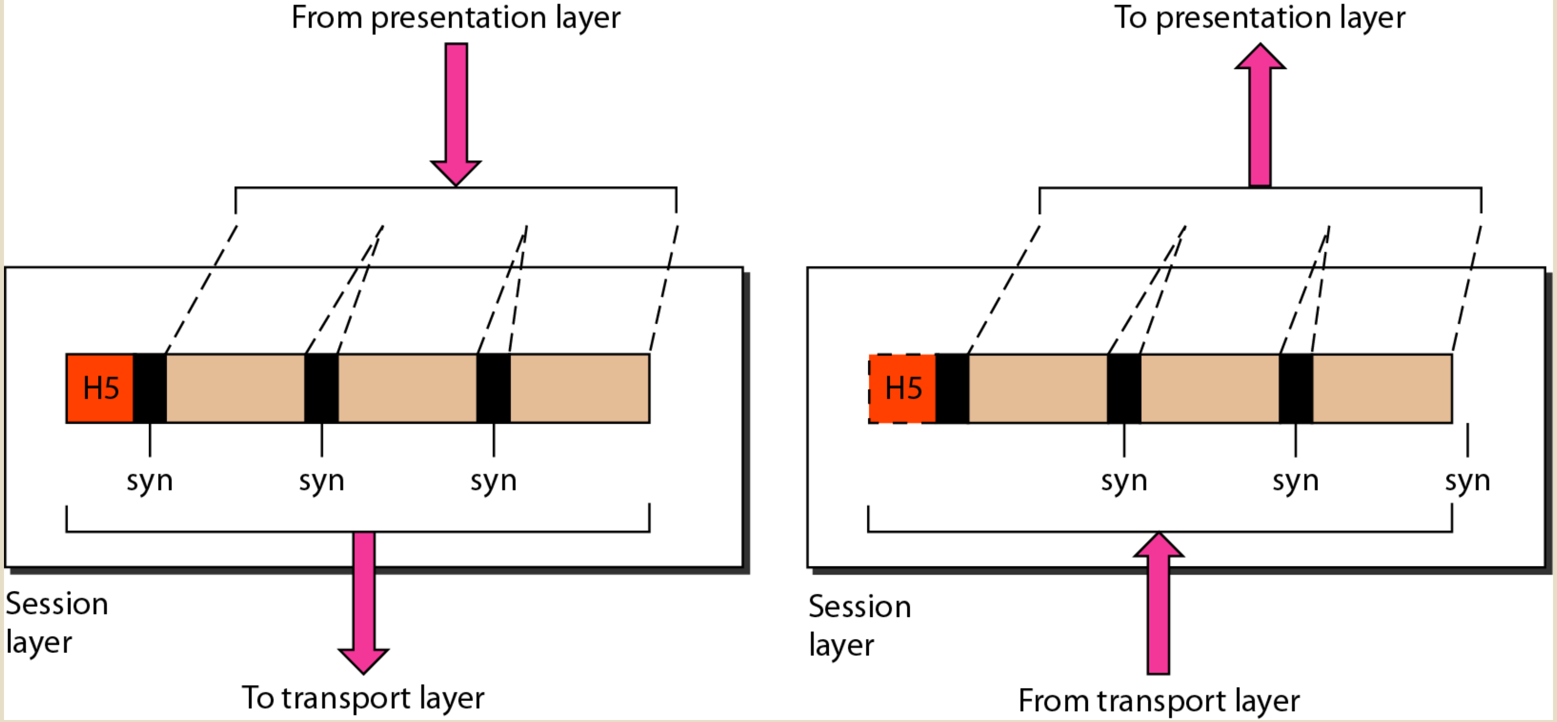


The transport layer is responsible for the delivery of a message from one process to

Reliable process-to-process delivery of a message

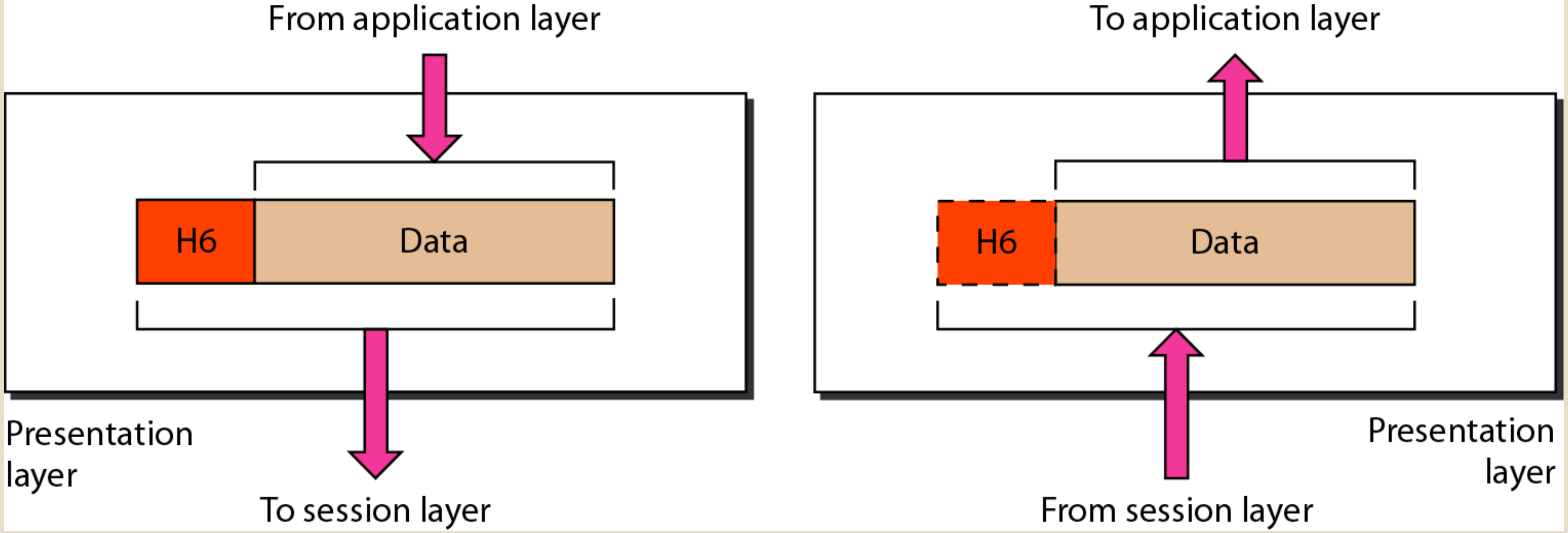


Session layer



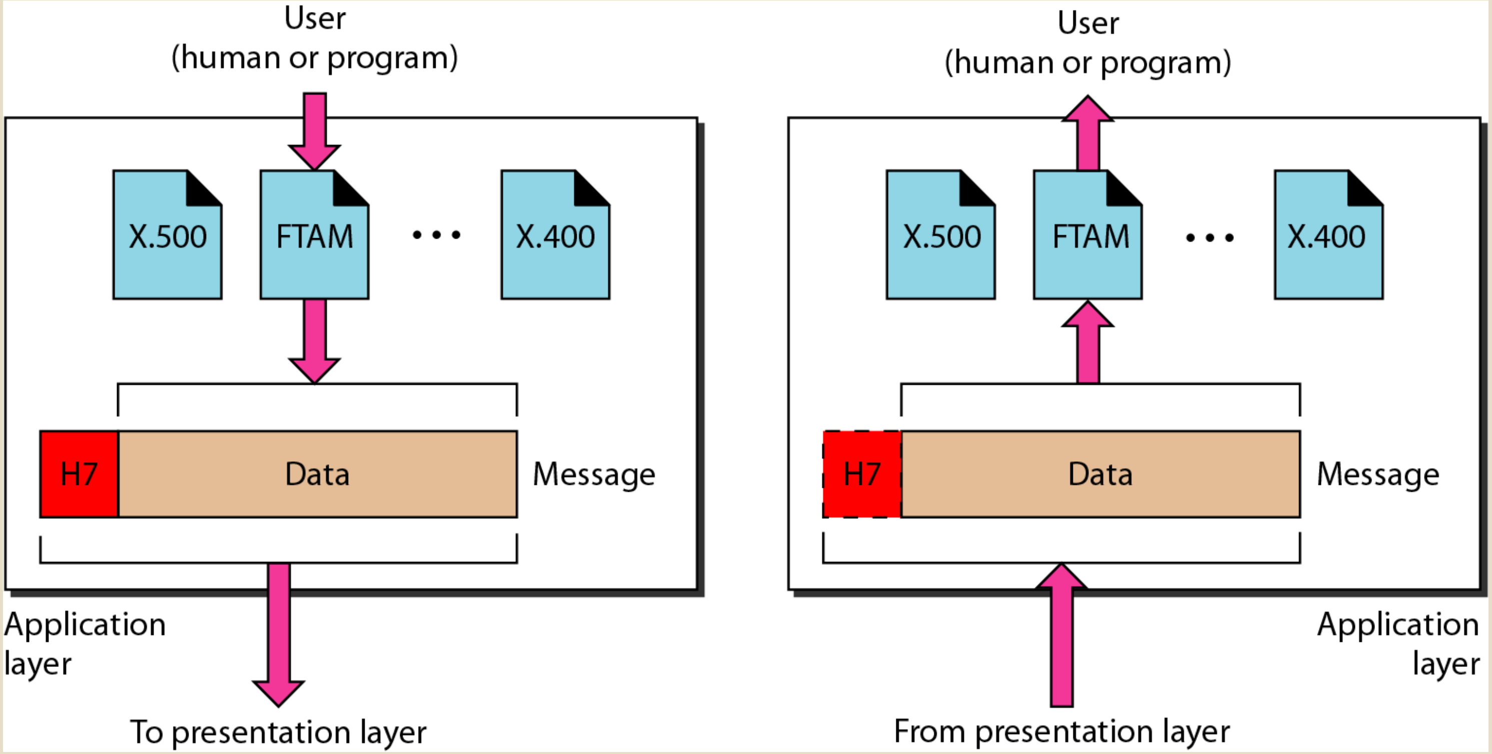
The session layer is responsible for dialog control and synchronization.

Presentation layer



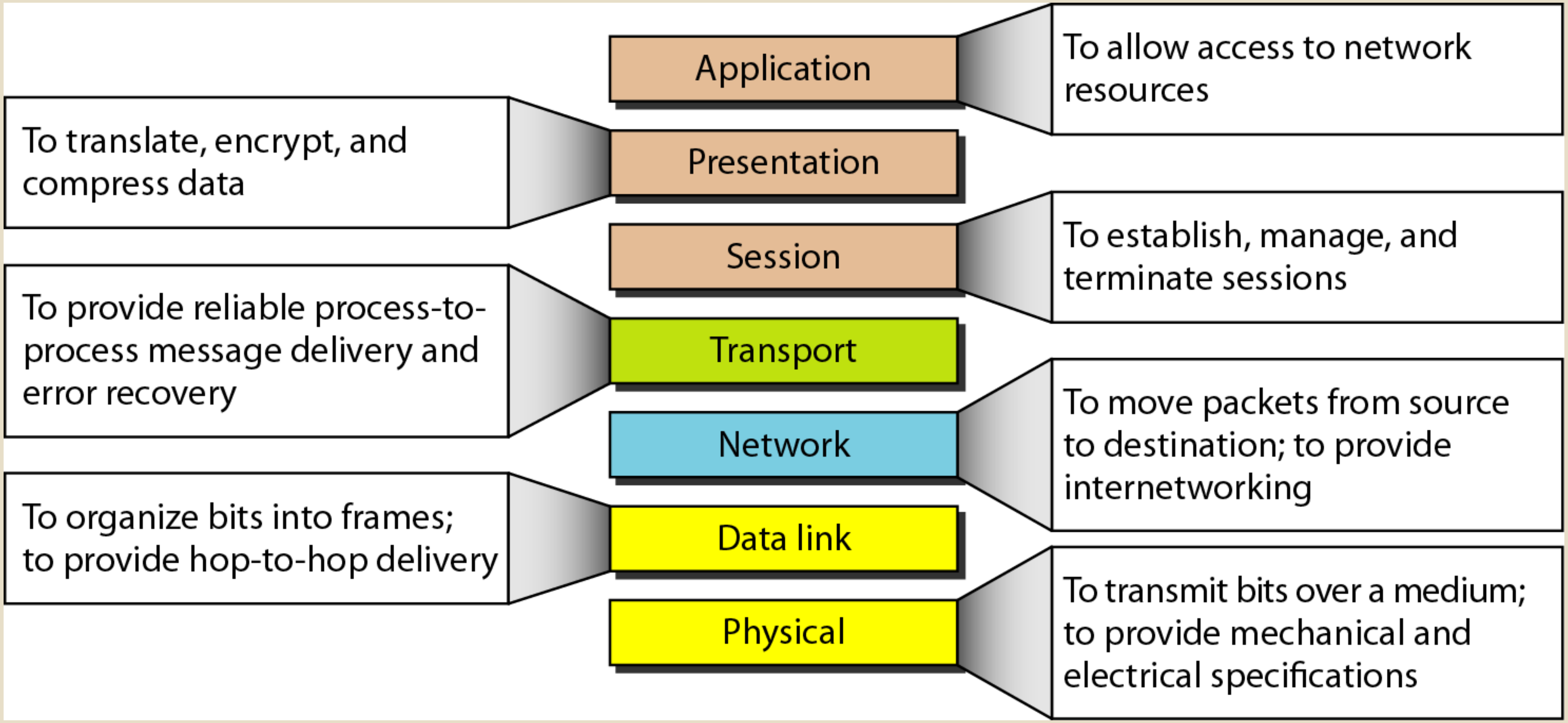
The presentation layer is responsible for translation, compression, and

Application layer



The application layer is responsible
for providing services to the

Summary of layers



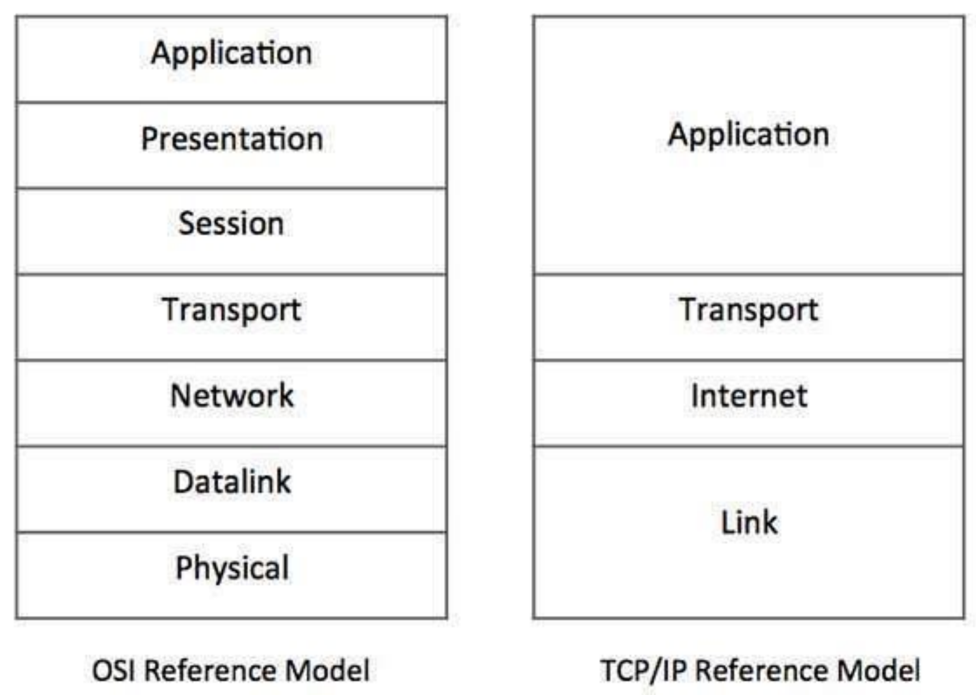
Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

Networks

TCP/IP Protocol Model

TCP/IP Protocol Model

The layers in the **TCP/IP protocol suite** do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.



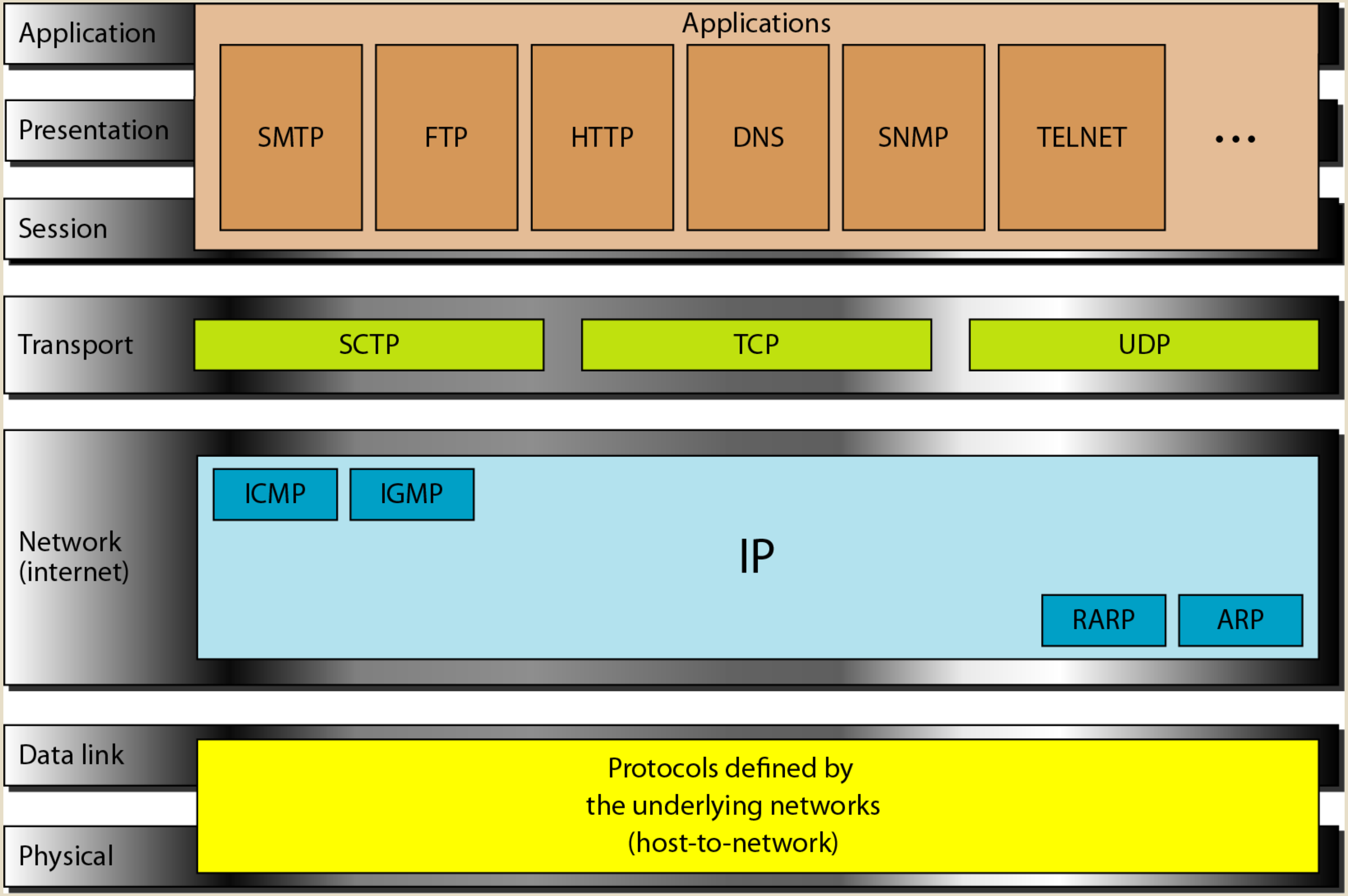
Application
Presentation
Session
Transport
Network
Datalink
Physical

OSI Reference Model

Application
Transport
Internet
Link

TCP/IP Reference Model

TCP/IP and OSI model

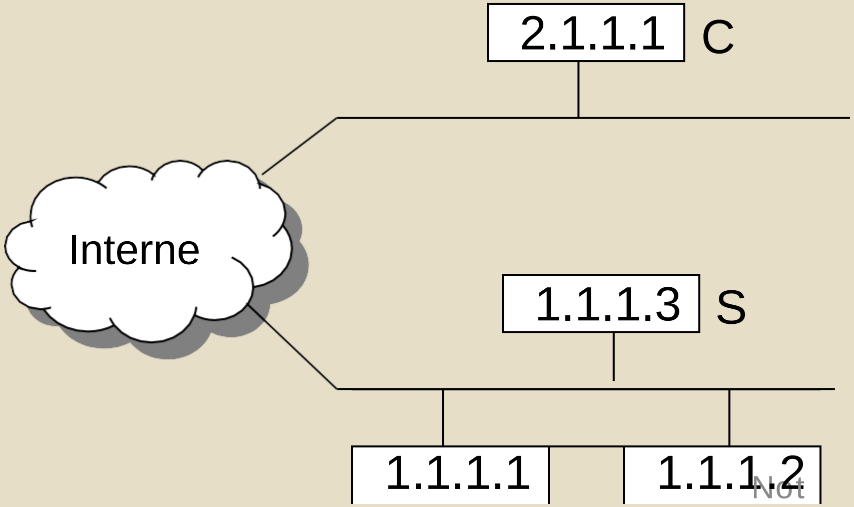


Different Types of Network Layer

- Attacks on Different Layers
  - IP Attacks
  - ICMP Attacks
  - Routing Attacks
  - TCP Attacks
  - Application Layer Attacks

Security Flaws in IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, rhosts etc..)

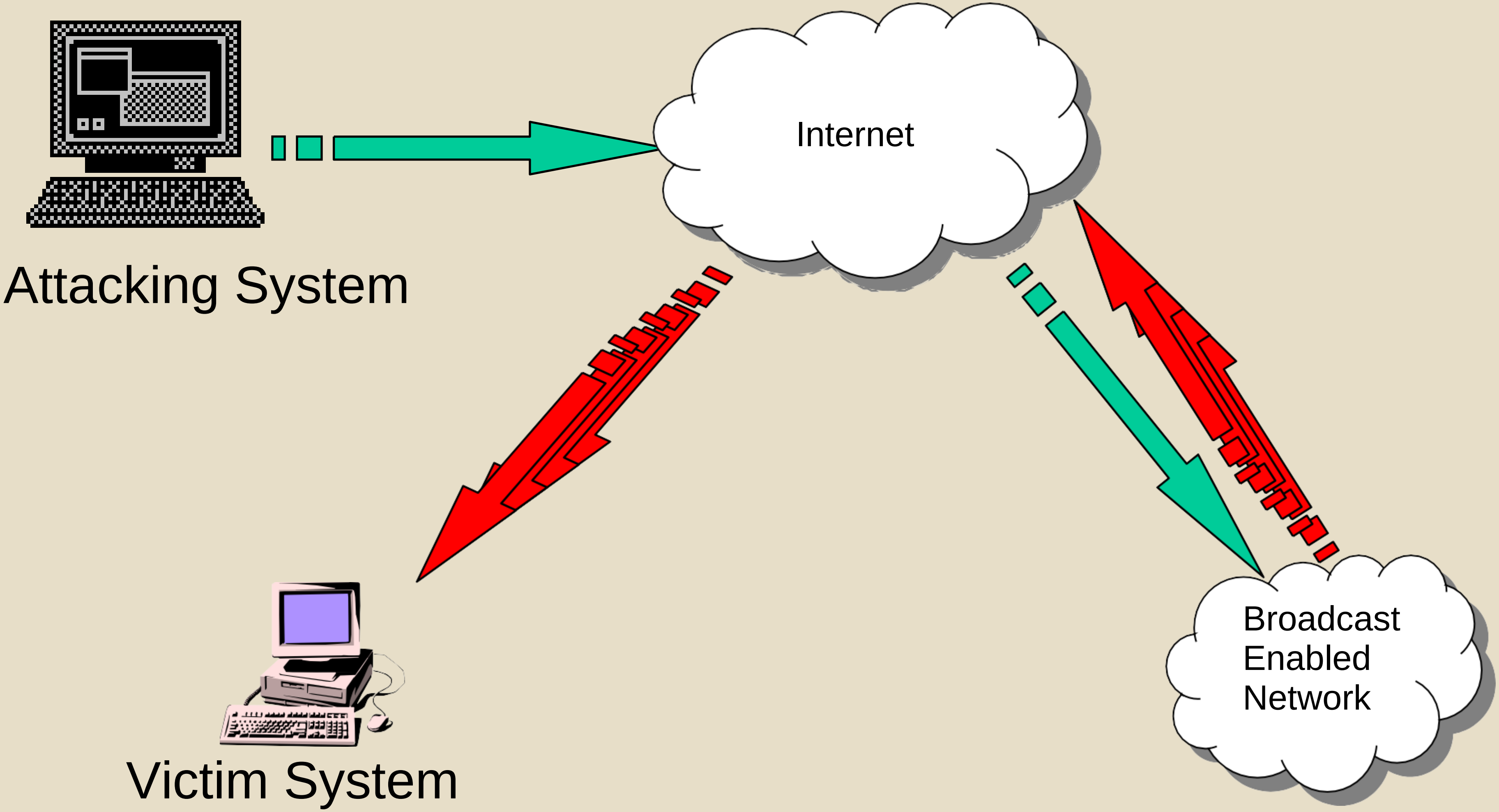


- Can A claim it is B to the server S?
  - ARP Spoofing
- Can C claim it is B to the server S?
  - Source Routing

Security Flaws

- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive
- Traffic amplification attack
  - IP allows broadcast destination
  - Problems?
- Divert traffic to malicious nodes
  - Black-hole attack
  - Eavesdropping
- How to implement routing attacks?
  - Distance-Vector
    - Announce low-cost routes
- BGP vulnerabilities
  - Prefix hijacking
  - Path alteration
- Protocol-level vulnerabilities
  - Implicit trust assumptions in design
- Implementation vulnerabilities
  - Both on routers and end-hosts
- Incomplete specifications
  - Often left to the imagination of programmers

Ping Flood

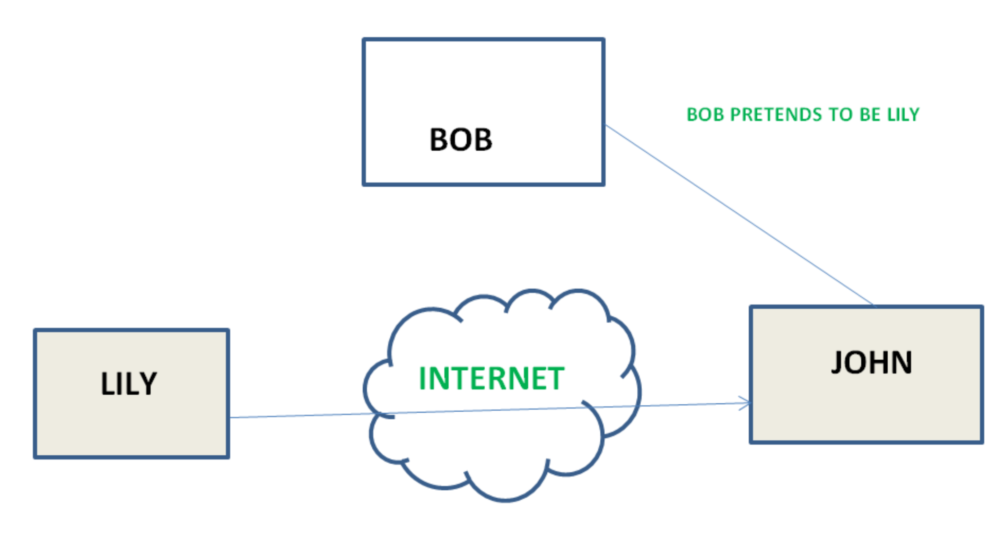

Internet
Attacking System
Victim System
Broadcast
Enabled
Network

Types of Attacks

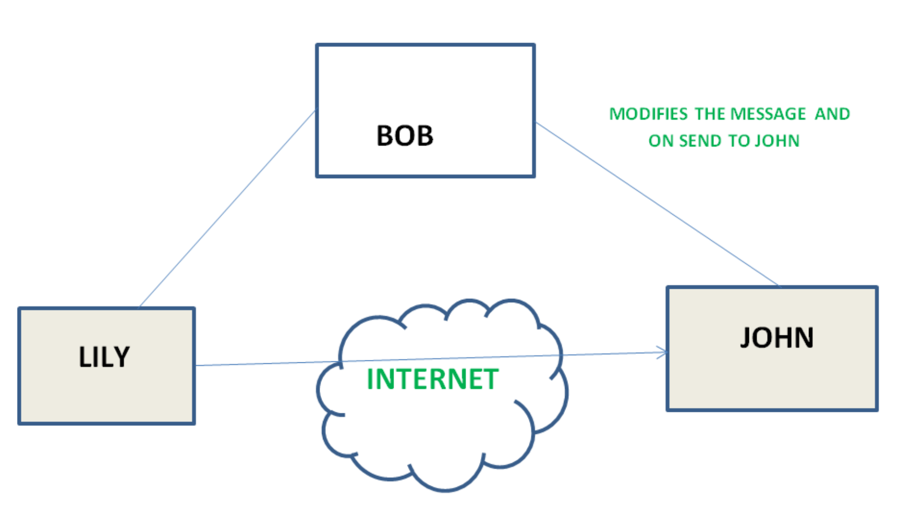
Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

1. **Masquerade**
2. **Modification of messages**
3. **Repudiation**
4. **Replay**
5. **Denial of Service**

- **Masquerade –**
  Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.

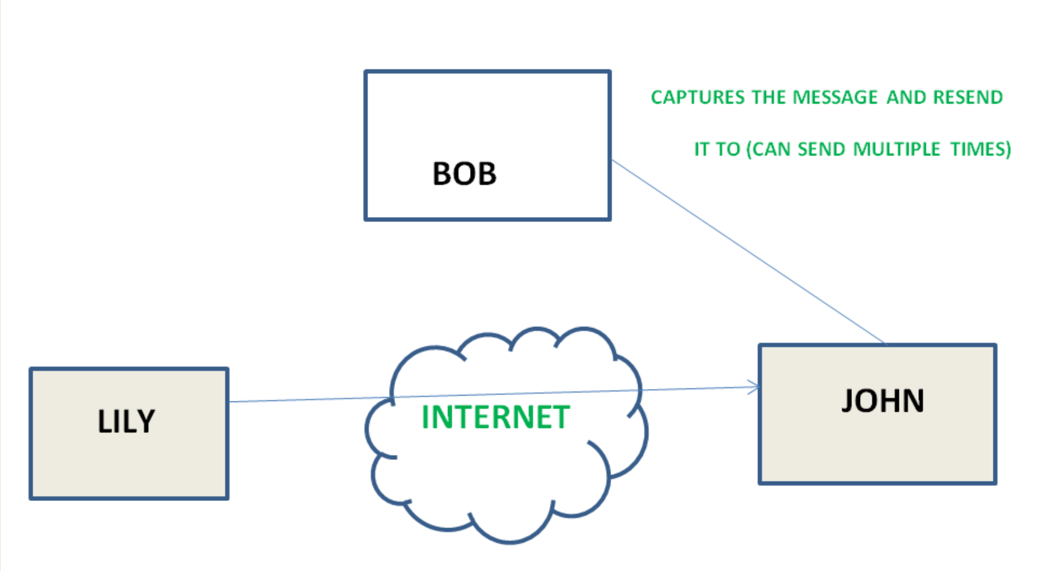


- **Modification of messages –**
  It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as
  “Allow Smith to read confidential file X”.

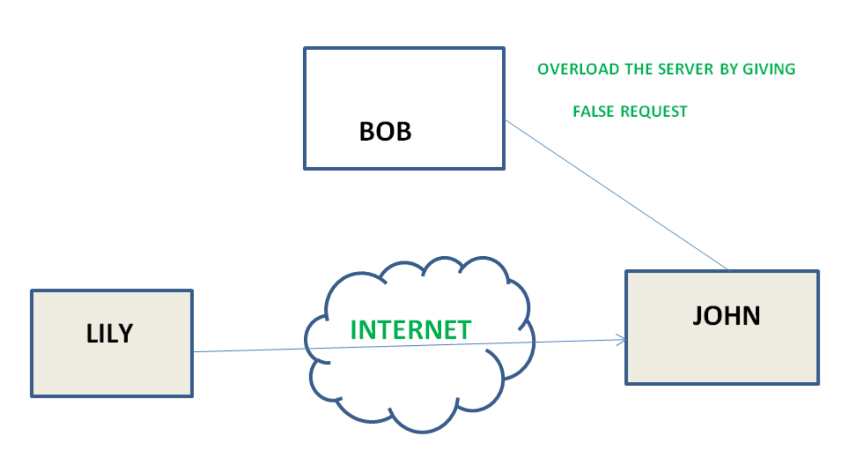


- **Repudiation –**
  This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message.
  For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.

- **Replay –**
  It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.


BOB
CAPTURES THE MESSAGE AND RESEND
IT TO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

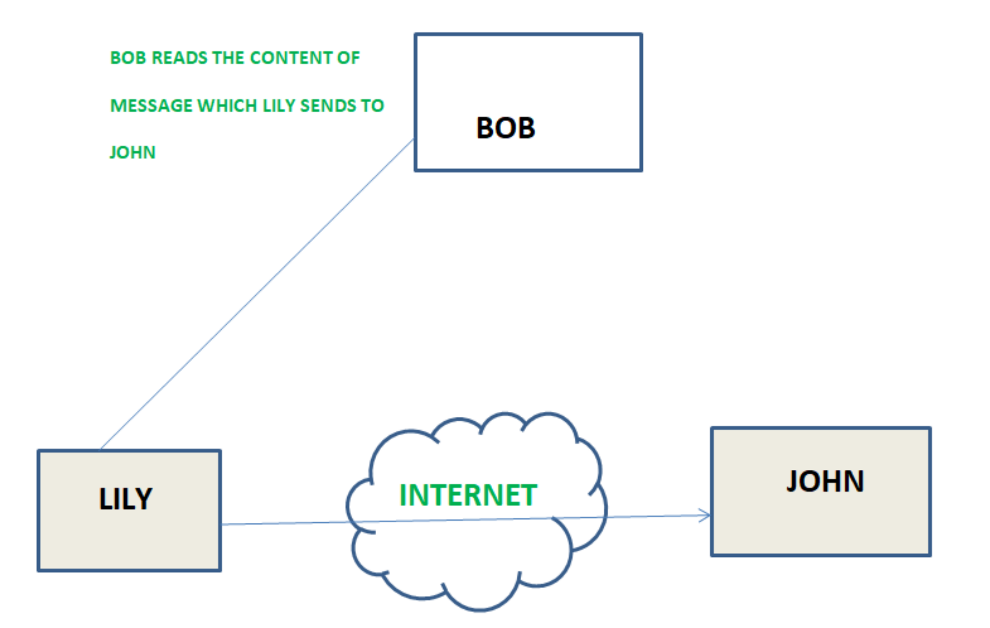
- **Denial of Service –**
  It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



- **Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content**
2. **Traffic analysis**

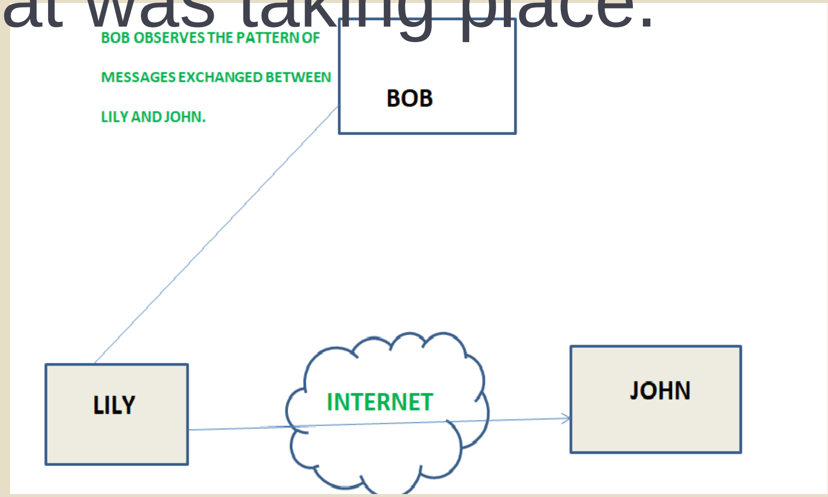
- **The release of message content –** Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions



- **Traffic analysis –**

  Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

  The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



Types of network layer attacks

Eavesdropping

- communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic.
  - When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping.
  - Eavesdropping is the biggest security problem that administrators face in an enterprise. Improved With strong encryption services that are based on cryptography.

Data Modification

- After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver.
- Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

Identity Spoofing (IP Address Spoofing)

- Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.
- After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data.

Password-Based Attacks

- password-based access control. user name ,password.
- Older applications do not always protect identity information as it is passed through the network for validation.
- Eavesdropper gain access to the network by posing as a valid user.
- When an attacker finds a valid user account, the attacker has the same rights as the real user..
- After gaining access to your network with a valid account, an attacker can do any of the following:
  - Obtain lists of valid user and computer names and network information.
  - Modify server and network configurations, including access controls and routing tables.
  - Modify, reroute, or delete your data.

Compromised-Key Attack

- A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.
- An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Man-in-the-Middle Attack

- occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange.
- When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.
- Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information.

Sniffer Attack/ Packet Sniffer

- A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.
- Using a sniffer, an attacker can do any of the following:
- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Phishing

- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

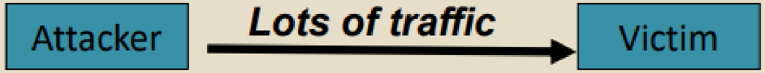
DNS spoofing

- Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver’s cache, causing the name server to return an incorrect IP address.

Denial-of-Service Attack

- Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.
- Objective ❼ make a service unusable, usually by overloading the server or network
- After gaining access to your network, the attacker can do any of the following:
  - Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
  - Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
  - Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
  - Block traffic, which results in a loss of access to network resources by authorized users.

- Attacker usually spoofs source address to hide origin
- Disrupt service by taking down hosts
  - E.g., ping-of-death
- Consume host resources
  - TCP SYN floods
  - ICMP ECHO (ping) floods
- Consume network resources
  - E.g., UDP/ICMP floods
- Consume bandwidth
  - UDP floods
  - ICMP floods

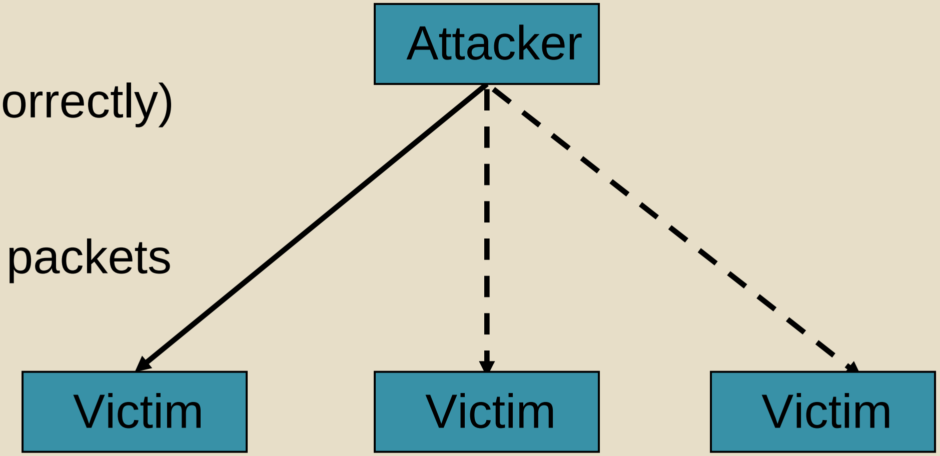


Simple DoS

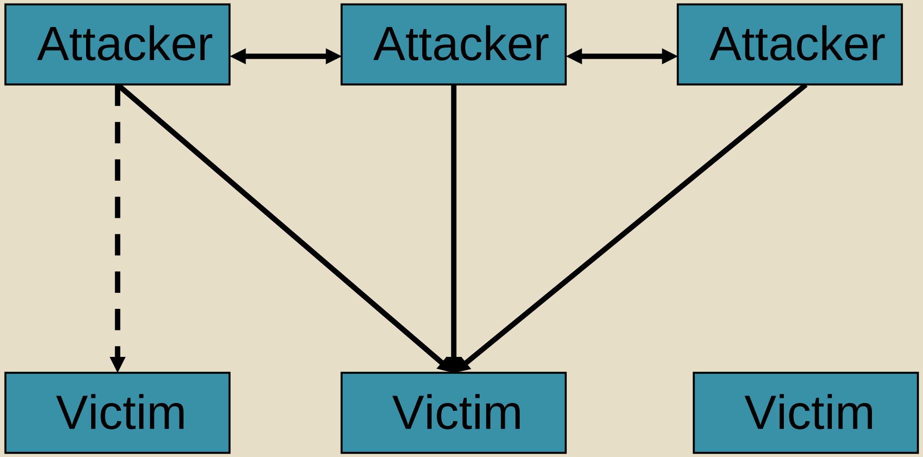
- The Attacker usually spoofed source address to hide origin
- Easy to block

Crashing the victim
    Ping-of-Death
    TCP options (unused, or used incorrectly)

Forcing more computation
    Taking long path in processing of packets



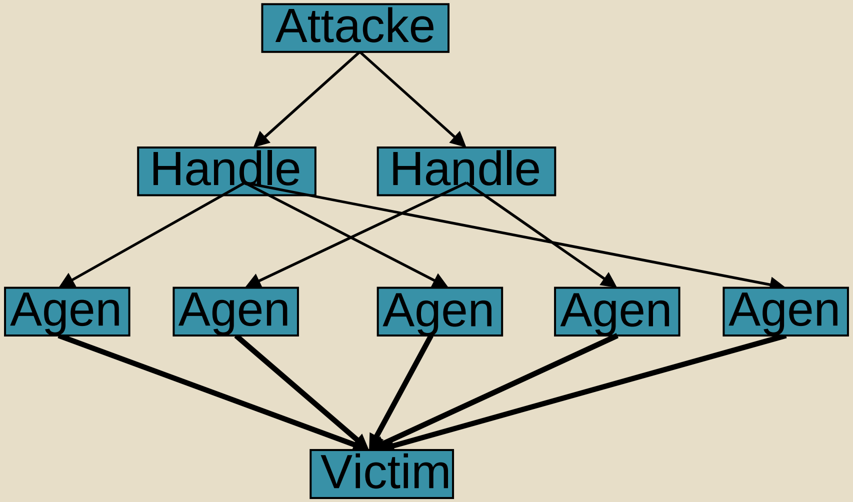
Coordinated DoS



- The first attacker attacks a different victim to cover up the real attack
- The Attacker usually spoofed source address to hide origin
- Harder to deal with

Distributed DoS

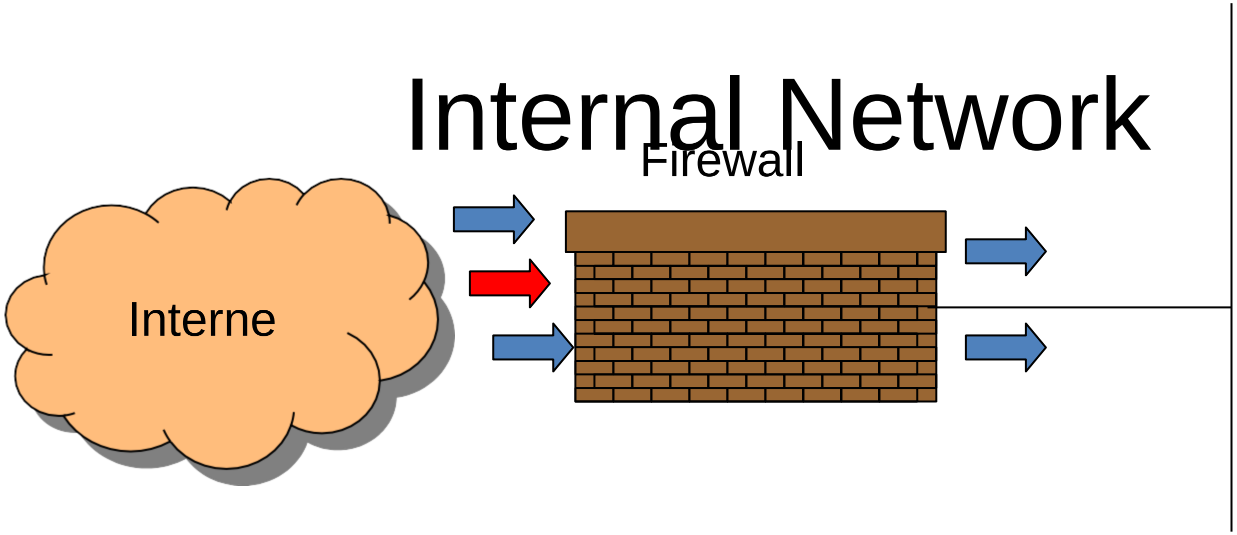
- The handlers are usually very high volume servers
  - Easy to hide the attack packets
- The agents are usually home users with DSL/Cable
  - Already infected and the agent installed
- Very difficult to track down the attacker
- How to differentiate between DDoS and Flash Crowd?
  - Flash Crowd ➐ Many clients using a service legitimately
    - Slashdot Effect
    - Victoria Secret Webcast
  - Generally the flash crowd disappears when the network is flooded
  - Sources in flash crowd are clustered



Firewall

Firewall

- A firewall is a device that filters traffic between a “protected” or inside network and a “less trustworthy” or outside network.
- A firewall is basically an executable code run on a dedicated computer.
- As all traffic should pass through the firewall, it is not a point of bottleneck for system performance and hence non-firewall functions are not performed on that machine running the firewall.
- Also, since non-firewall code does not exist in the computer, it is hard for an attacker to make use of any vulnerability to compromise the firewall.



Firewalls

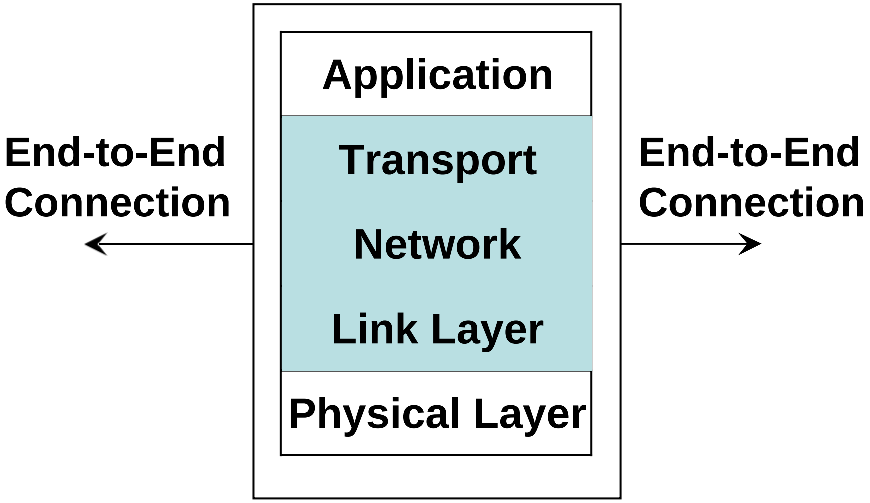
- Design idea:
  - Firewalls implement a security policy that is specifically designed to address what bad things that should not happen in a "protected environment"
  - Security policies that dictate what to allow: Standard security practices dictate a "default-deny" ruleset for firewalls, implying that the only network connections allowed are the ones that have been explicitly stated to be allowed.
  - Security policies that dictate what not to allow: Users and business community who lack such a detailed understanding to explicitly state what should be allowed in prefer a "default-allow" ruleset, in which all traffic is allowed unless it has been specifically blocked.
    - Even though this configuration is relatively more prone to inadvertent network connections and system compromise, it is more commonly used because of mere lack of knowledge and new applications that come into existence.

Firewalls

- Not all firewalls need to have the same capability.
- One cannot compare the “goodness” of two firewalls based on the security policies they are configured with.
  - **The key factor that drives the selection of a security policy for a firewall is the threats that an installation (network) needs to avoid happening.**
- **Packet Filters**
- A packet filtering firewall controls access to packets on the basis of packet address (source or destination) or specific transport protocol type (such as HTTP, Telnet, etc)
  - **Egress filtering:** Packets would be sent out (or not to be sent out) only to specific networks and/ or belonging to specific transport layer protocols.
  - **Ingress filtering:** Packets belonging to (not belonging to) only certain source networks and/ or specific transport layer protocols could be let in.
- A common strategy to avoid IP spoofing attacks is to have the packet filter configured not to let in packets having a source address that corresponds to the internal network.
  - In other words, the attacker has spoofed the source IP address to be the IP address of a machine belonging to the network being protected by the firewall.
- The code for packet filters will become lengthy as we want to block traffic belonging to specific networks, IP addresses and transport layer protocols.

Attacks Prevented using Packet Filter Firewalls

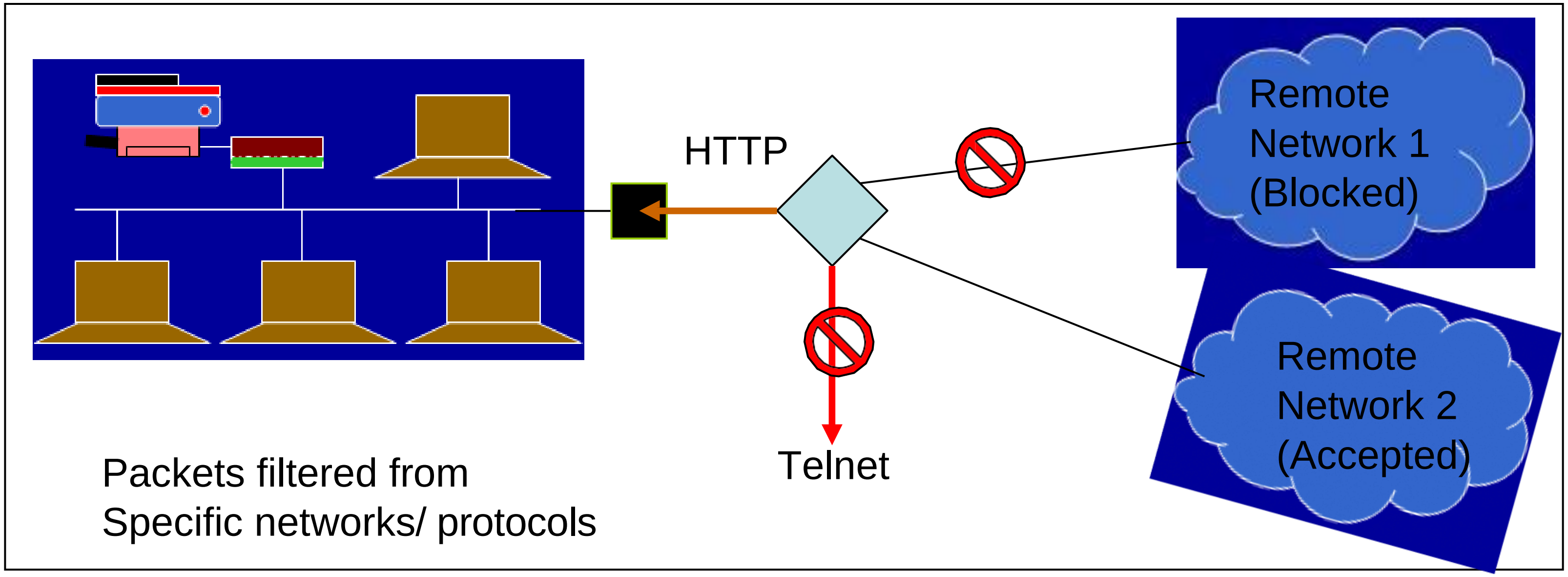
- In addition to IP spoofing attacks, packet filter firewalls could also be configured to avoid source routing and tiny fragmentation attacks.
- Source routing attacks: where source specifies the route that a packet should take to bypass security measures, should discard all source routed packets
- Tiny fragment attacks: intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into fewer separate fragments to circumvent filtering rules needing full header info; can enforce minimum fragment size to include full header.



Layers supported by Packet Filter and Stateful Firewalls

Source (adapted from): Figure 22.1(b) from William Stallings – Cryptography and Network Security, 5th Edition

Packet Filters



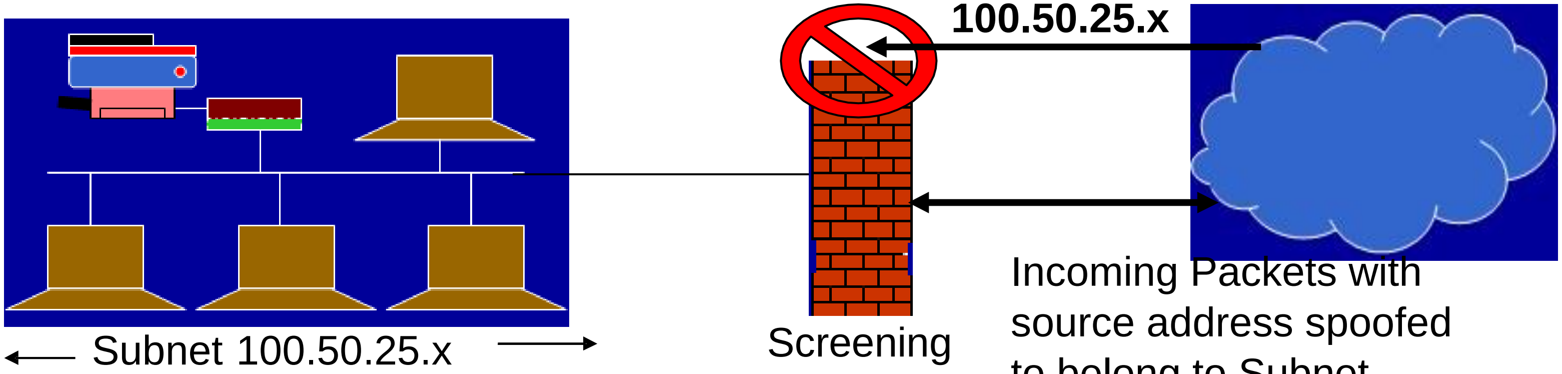
HTTP

Remote Network 1 (Blocked)

Remote Network 2 (Accepted)

Telnet

Packets filtered from
Specific networks/ protocols



100.50.25.x

Subnet 100.50.25.x

Screening
Router

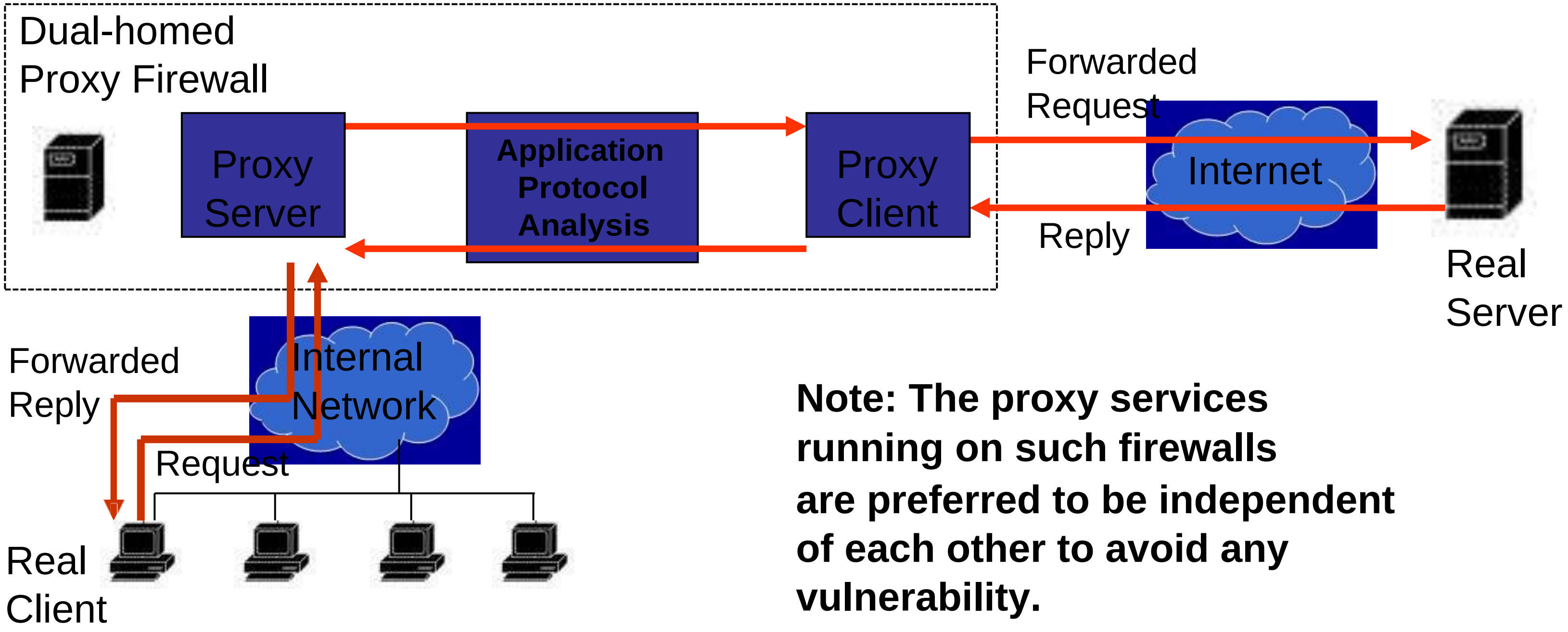
Incoming Packets with
source address spoofed
to belong to Subnet
100.50.25.x are filtered

Stateful Inspection Firewalls

- Firewalls based on packet filters operate on packets on an individual basis and do not store the state information pertaining to the action taken on a packet processed earlier.
- Stateful firewalls (also called circuit firewalls) examine the contents of each packet with regards to their placement within the packet series belonging to a specific connection.
- Stateful firewalls maintain records of all connections passing through the firewall and is able to determine whether a packet is the start of a new connection or part of an existing connection.
- Stateful firewalls can remember the sequence numbers expected on both sides as part of a TCP session and can block attempts to hijack the session, when an intruder sends several TCP segments with different sequence numbers (trial-and-error).
- The state of a connection will be a criteria to trigger specific rules of the firewall.
  - Examples:
    - Data packets for a connection cannot get in before the connection is completely established and after a connection is completely teardown.
    - Do not let more than a certain number of simultaneous TCP connections to originate per IP address.
    - Do not let more than a specific amount of data to be transferred per day from the inside network to any outside IP address.

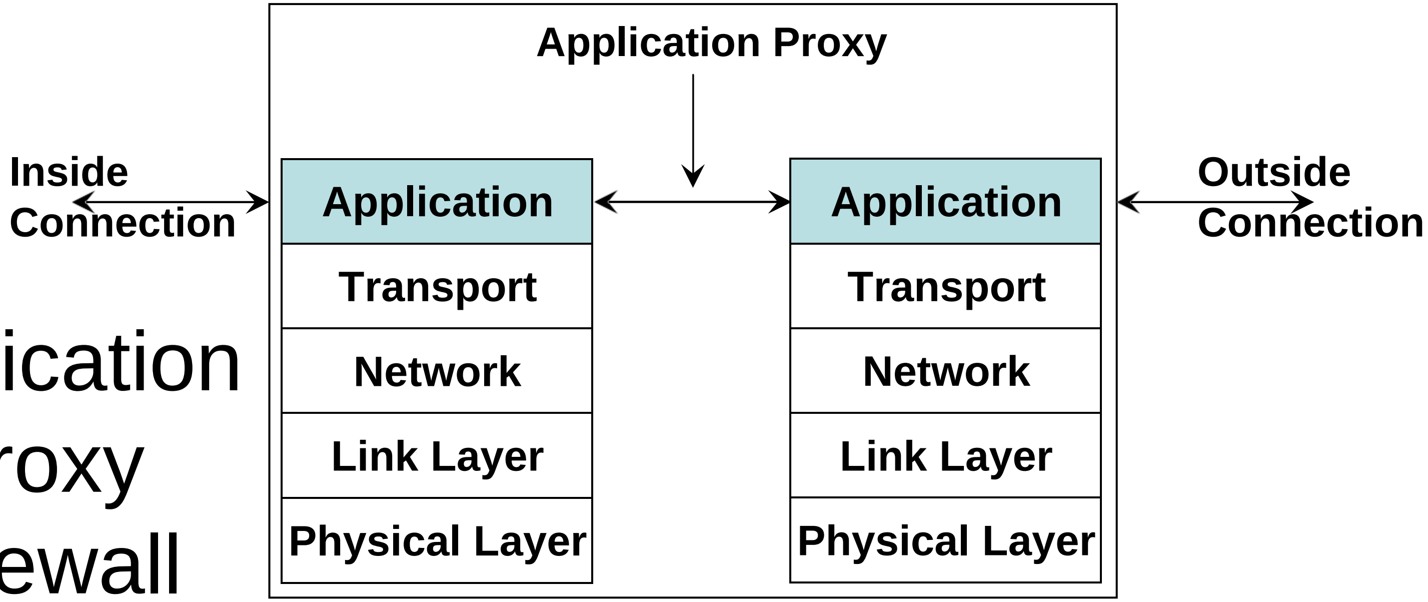
Application Proxy Firewall

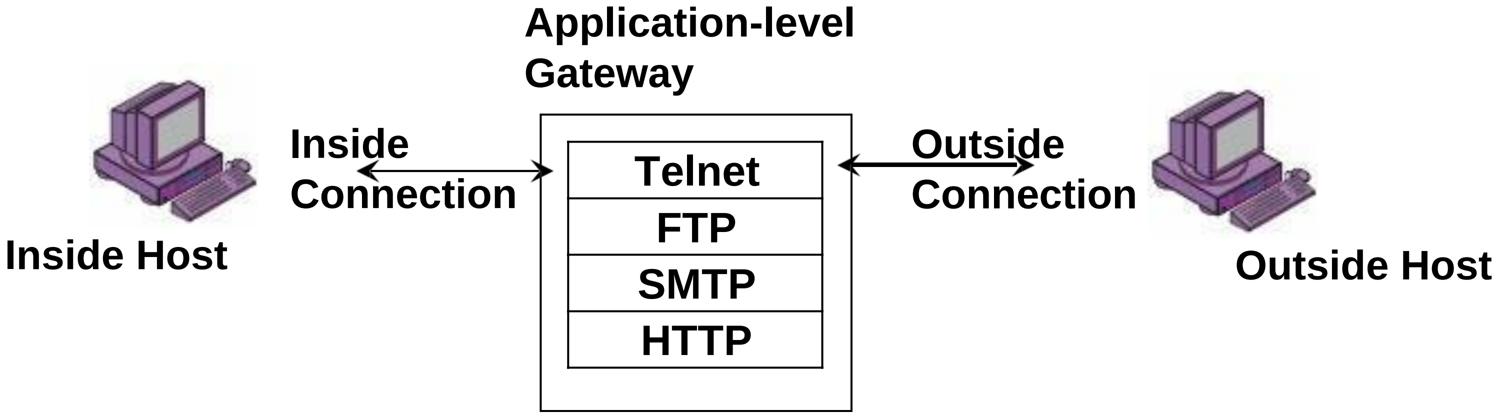
- Packet filters look only at the headers of the packets, not at the data inside the packets.
- An application layer firewall (proxy; also called as bastion) simulates the proper effects of an application so that the application receives only requests to act properly.
- A proxy gateway is a two-headed device: It looks to the inside as if it is the outside (destination) connection; while to the outside, it responds as it is from the inside.



Note: The proxy services running on such firewalls are preferred to be independent of each other to avoid any vulnerability.

Application Proxy Firewall





Source (adapted from): Figure 22.1(d) from William Stallings – Cryptography and Network Security, 5th Edition

Application Proxy Firewall

- Each application proxy in the firewall requires two components: a proxy server and a proxy client.
- All communication between internal users and the Internet passes through the proxy server rather than allowing users to directly communicate with servers on the Internet.
- An internal user (client) sends a request to connect to an external service. The request goes through the Application Proxy Firewall that runs a proxy server for that particular service being requested.
- The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service.
- Proxy servers allow only those packets that comply with the services of the application protocol.
- Proxy servers are also useful to collect audit records of session information
- If the proxy server approves the request, it forwards that request to the proxy client.
- The proxy client then contacts the real server on behalf of the real client and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server.
- The proxy server relays requests and responses between the proxy client and the real client.

- Note: The above discussion assumes the client is in the internal network and the server is in the external network. The same discussion applies for the other scenario too:
  - The real client (from the outside network) contacts the proxy server, the proxy server evaluates the request and forwards to the proxy client, the proxy client contacts the real server (running in the internal network).
  - The proxy client forwards the response from the real server to the proxy server, which forwards the response to the real client (in the outside network).

Examples of using Proxy Firewall

- Scenario 1: A company wants to allow dial-in access by its employees, without exposing its company resources to login attacks from remote non-employees. Suppose the internal network has a mixture of operating system types, none of which support strong authentication through a challenge-response system.
- Solution:
  - The requirement could be handled by a specifically written proxy that requires strong authentication such as a challenge-response, in addition to a valid username and corresponding password.
  - The proxy validates the challenge-response itself, and then pass on only the username and password in a form required by the internal host's operating system.
- Scenario 2: A company wants to set up an online price list so that outsiders can see the products and prices offered. It wants to be sure that (a) no outsider can change the prices or product list and (b) outsiders can access only the price list and not any of the more sensitive files stored inside.
- Solution:
  - The requirement could be handled by a specifically written proxy that monitors the file transfer protocol data to ensure that only the price list file was accessed, and that the file could be only read, not modified.

- Note: A proxy firewall can also function more as a guard, monitoring the amount and quality of data exchanged.
  - –It could keep track of the amount of data exchanged per user from the internal network and deny access if exceeded a pre-defined limit.
  - –A proxy firewall could also run a virus scanner to scan all the incoming files and if required outgoing files too.

Proxy Servers

- A Proxy Server is a server (a computer system or an application program) that acts as intermediary for requests from clients seeking resources and/or service from other servers.
- The proxy server typically evaluates the request according to its filtering rules (say by IP address or port number) and acts based on this evaluation.
- A proxy server has a large variety of potential purposes, including:
  - To keep machines behind it anonymous (mainly for security)
  - To speed up access to resources (using caching) – Web proxy servers
  - To apply access policy to network services or content (to block visiting undesired sites) – proxy firewall
  - To log/ audit usage – proxy firewall
  - To scan transmitted content for malware before delivery – content-filtering web proxy
- Deploying a proxy solution within a network environment is typically done either by requiring all client systems to configure their browsers to use the proxy or by deploying an intercepting proxy that actively intercepts all requests without requiring client-side configuration.
- A proxy server that passes requests and replies unmodified is usually referred to as a gateway or also sometimes, tunneling proxy.

Reverse Proxy Servers

- A reverse proxy server is an Internet-facing proxy used as a front-end to control and protect access to a server/servers on a private network, as well as to perform tasks such as load-balancing, authentication and etc.
- A reverse proxy server appears to the Internet clients as an ordinary server. Internally, it could merely forward the client requests to the original internal servers for handling. The response would be returned as if it came directly from the proxy server.
- There are several advantages in using reverse proxy servers:
  - Encryption/ SSL acceleration: A reverse proxy server could accelerate the communication sessions by serving as a single “SSL proxy” to provide SSL encryption for an arbitrary number of hosts; removing the need for a separate SSL Server Certificate for each host.
  - Load balancing: The reverse proxy server can dynamically distribute the load to several web servers.
  - Security: The reverse proxy server could be an additional layer of defense and can protect against some operating system and web server specific attacks.

Personal Firewalls

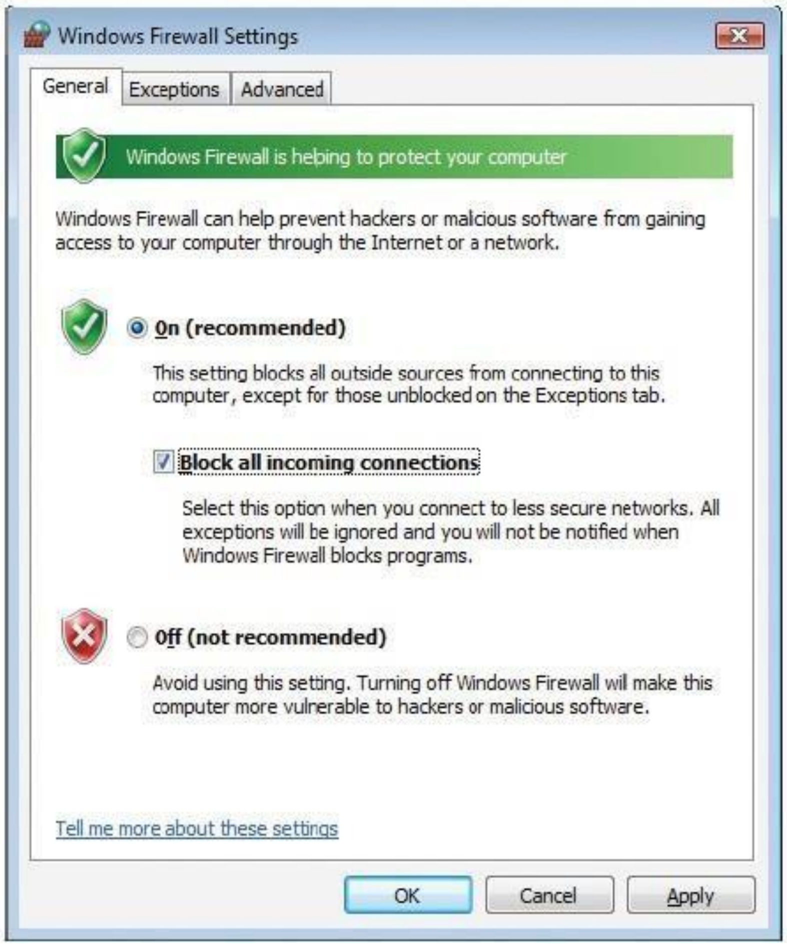
- Motivation: Home users, individual workers, and small businesses use cable modems or DSL connections with unlimited, always-on access.
- These people need a firewall, but a separate firewall computer to protect a single workstation can seem too complex and expensive.

- A workstation could be vulnerable to malicious code or malicious active agents (ActiveX controls or Java applets), leakage of personal data stored in the workstation, and vulnerability scans (like nmap) to identify potential weaknesses.
- A personal firewall is an application program that runs on a workstation to screen traffic on the workstation and block unwanted traffic leaving or entering the workstation to the network to which it is connected.
- A user could configure the personal firewall to accept traffic only from certain sites, and not from specific sites, and to generate logs of activities happened in the past
- A personal firewall could be also configured with a virus scanner which would be then automatically invoked to scan any incoming data to the workstation.

- A static machine is a vulnerable target for the attack community and adding a personal firewall can save it more secure compared to machines that are not behind such a firewall.

Examples for Personal Firewalls

- Windows Firewall
- With Windows Service Pack 2, Microsoft enabled the Windows Firewall (previously called Internet Connection Firewall) by default.
- With the introduction of the Vista Operating System, Microsoft modified Windows Firewall to make it more capable and configurable to allow more granular control of network traffic and behavior analysis of applications and services.
  - For example, if MS Outlook client suddenly attempts to connect to a remote web server, Windows Firewall can detect this as a deviation from normal behavior and block the unwanted traffic.



Windows Firewall is helping to protect your computer

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

☑ Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

○ Off (not recommended)

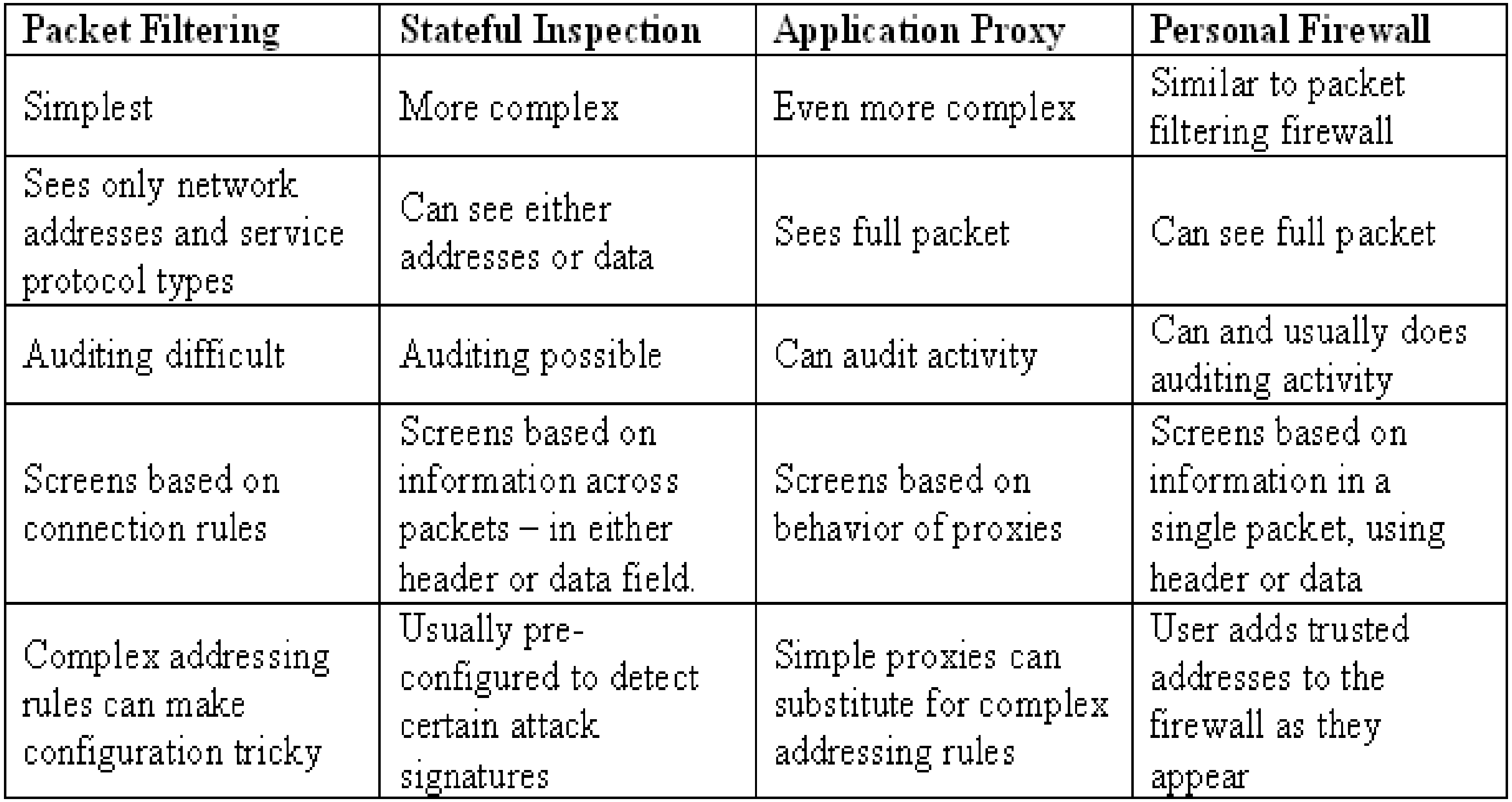
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Source: Figure 13.17 from Conklin and White – Principles of Computer Security, 2nd Edition

Examples for Personal Firewalls

- UNIX-based (Software) Firewalls
- *TCP Wrappers*: limits inbound network connections based on port number, domain, or IP address and is managed with two text files called hosts.allow and hosts.deny.
  - For example, if an inbound connection request is coming from a trusted IP address (listed in hosts.allow) and destined for a port to which it is allowed to connect, then the connection is allowed.
- *IPchains* – is a rule-based software firewall that has three configurable “chains” (set of rules) used for handling network traffic: input chain (for incoming traffic to the local system); output chain (for traffic leaving the local system) and forward chain (for traffic received by the local system; but, not destined for the local system).
  - Each packet passes all three chains for processing.
- *IPtables* – uses the same three chains for policy rules and traffic handling as IPchains; but, each packet is processed only at the appropriate chain. This allows for more granular control of network traffic and enhances performance.

Comparison of Firewall Types



Packet Filtering	Stateful Inspection	Application Proxy	Personal Firewall
Simplest	More complex	Even more complex	Similar to packet filtering firewall
Sees only network addresses and service protocol types	Can see either addresses or data	Sees full packet	Can see full packet
Auditing difficult	Auditing possible	Can audit activity	Can and usually does auditing activity
Screens based on connection rules	Screens based on information across packets – in either header or data field.	Screens based on behavior of proxies	Screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually pre-configured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	User adds trusted addresses to the firewall as they appear

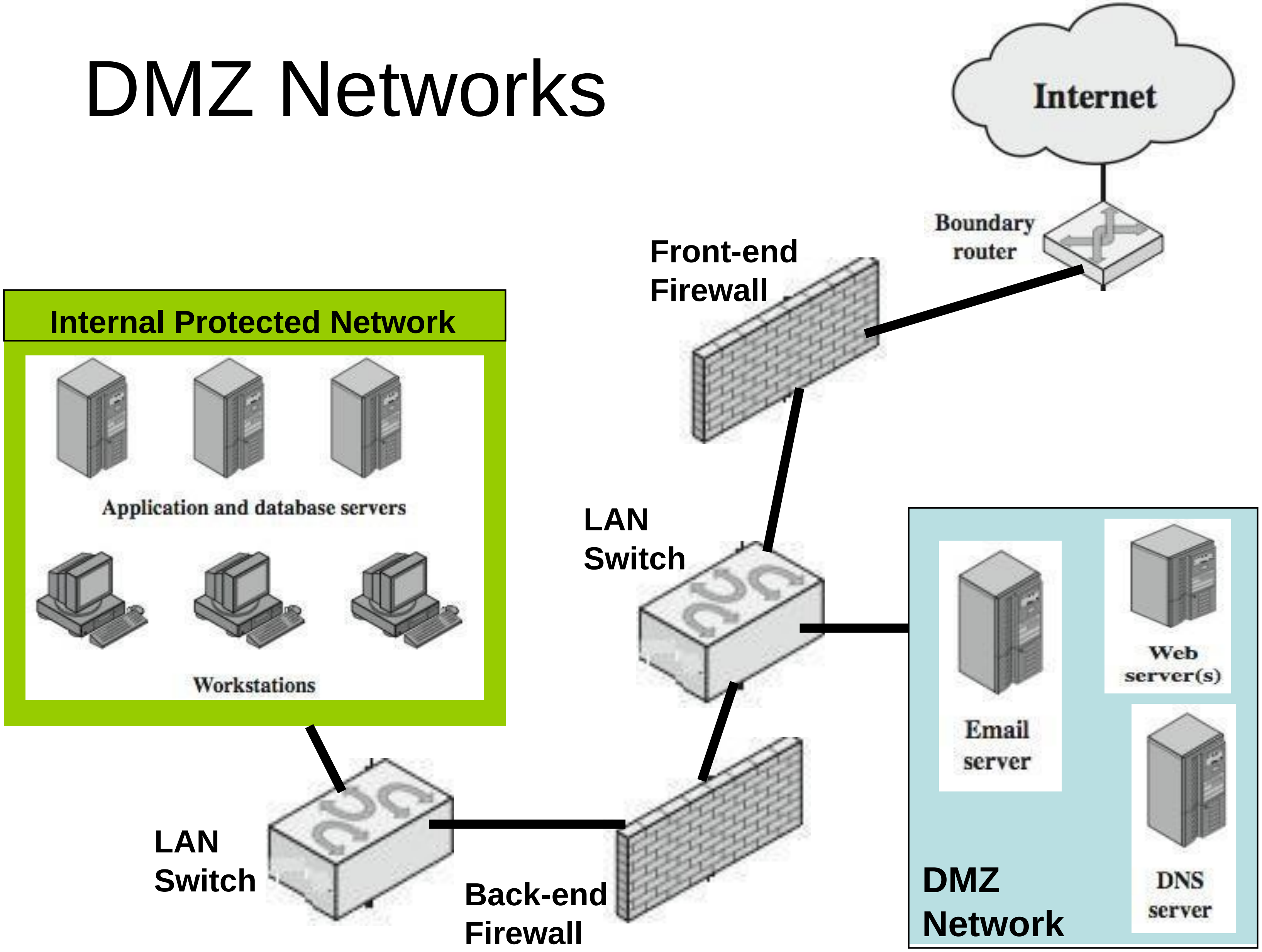
What Firewalls Can and Cannot Block

- Firewalls cannot alone secure an environment.
- A firewall protects only the perimeter of its environment against attacks from outsiders who want to execute code or access data on the machines in the protected environment.
- Firewalls cannot protect from internal threats (through disgruntled employees).
- Firewalls cannot protect against malware imported via laptop, PDA, or portable storage device infected outside the network, then attached and used internally.
- Firewalls can be held responsible for any security breach in if they are the only means to control the entire network perimeter.
  - If a host in the inside network has a connection to the outside network through a modem, the whole of the inside network is exposed to the outside network through the modem and the host. A firewall cannot be responsible for any attack
- Firewalls cannot protect data after they have left them.
- A firewall is often a single point of failure for a network.
  - A more layered approach like a screening router, followed by a proxy firewall, followed by a personal firewall may be more helpful.
- Firewalls must be frequently configured and updated to take into account the changes in the internal and external environment and based on the review of the firewall activity reports that may indicate intrusion attempts.
- The machine hosting the firewall code will not have any other software like an editor, compiler, etc. in order to reduce the chances of an attack.

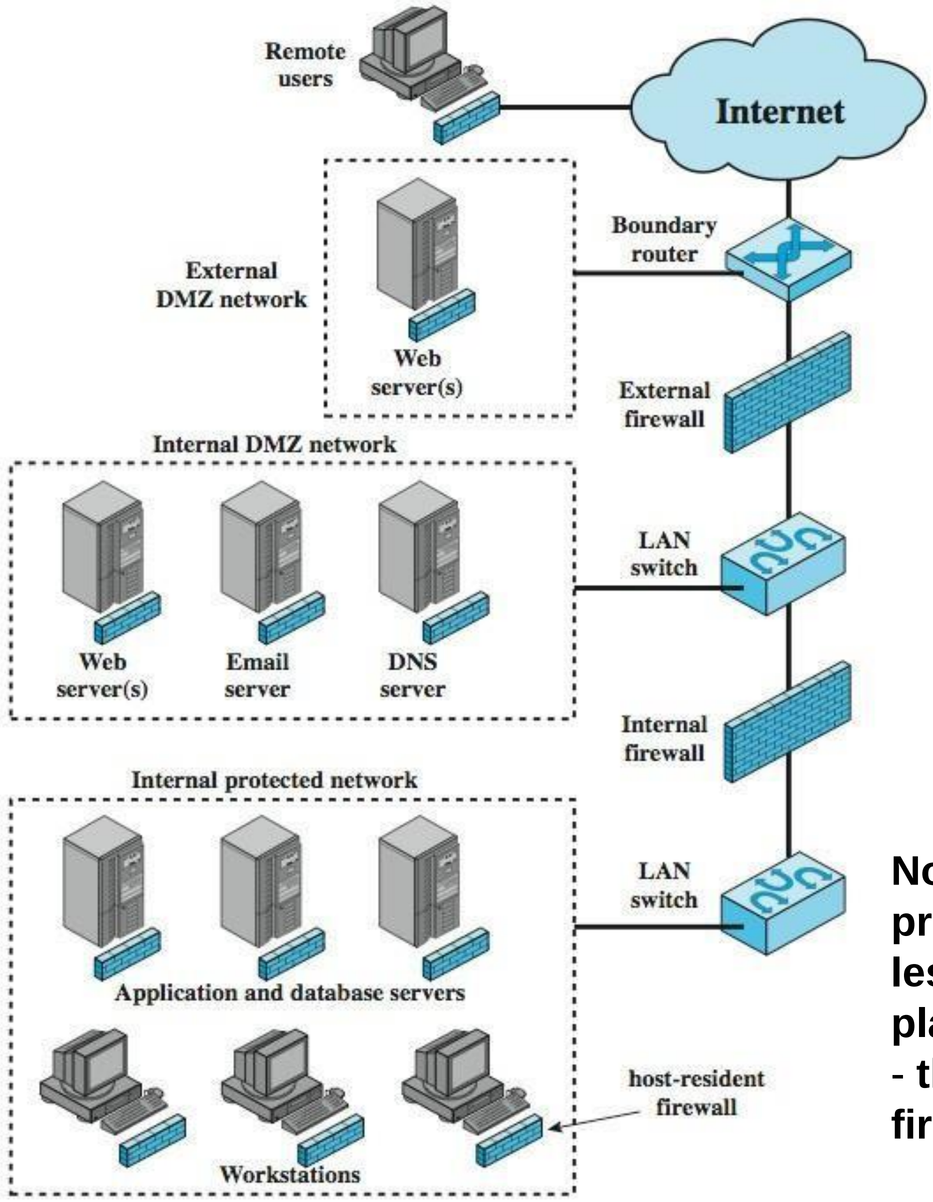
Demilitarized Zone (DMZ) Networks

- A DMZ network (also called perimeter network) is a subnet that contains an organization’s services that are exposed to a larger untrusted network (like the Internet).
- In other words, the DMZ comprises of hosts that provide services to users outside the internal LANs, such as e-mail, web, DNS servers.
- Because of the higher chances of these hosts being compromised, they are placed into their own sub-network in order to protect the rest of the network if an intruder were to succeed in attacking them.
- Thus, a DMZ network adds an additional layer of security to an organization’s LAN – an external attacker only has access to the hosts in the DMZ and not to any other internal networks.
- Hosts in the DMZ provide services to both the internal and external networks – an external (“front-end”) firewall monitors the traffic between the DMZ network and the external Internet; while, an internal (“back-end”) firewall monitors the traffic between the DMZ hosts and the internal network clients.

DMZ Networks



Distributed Firewalls



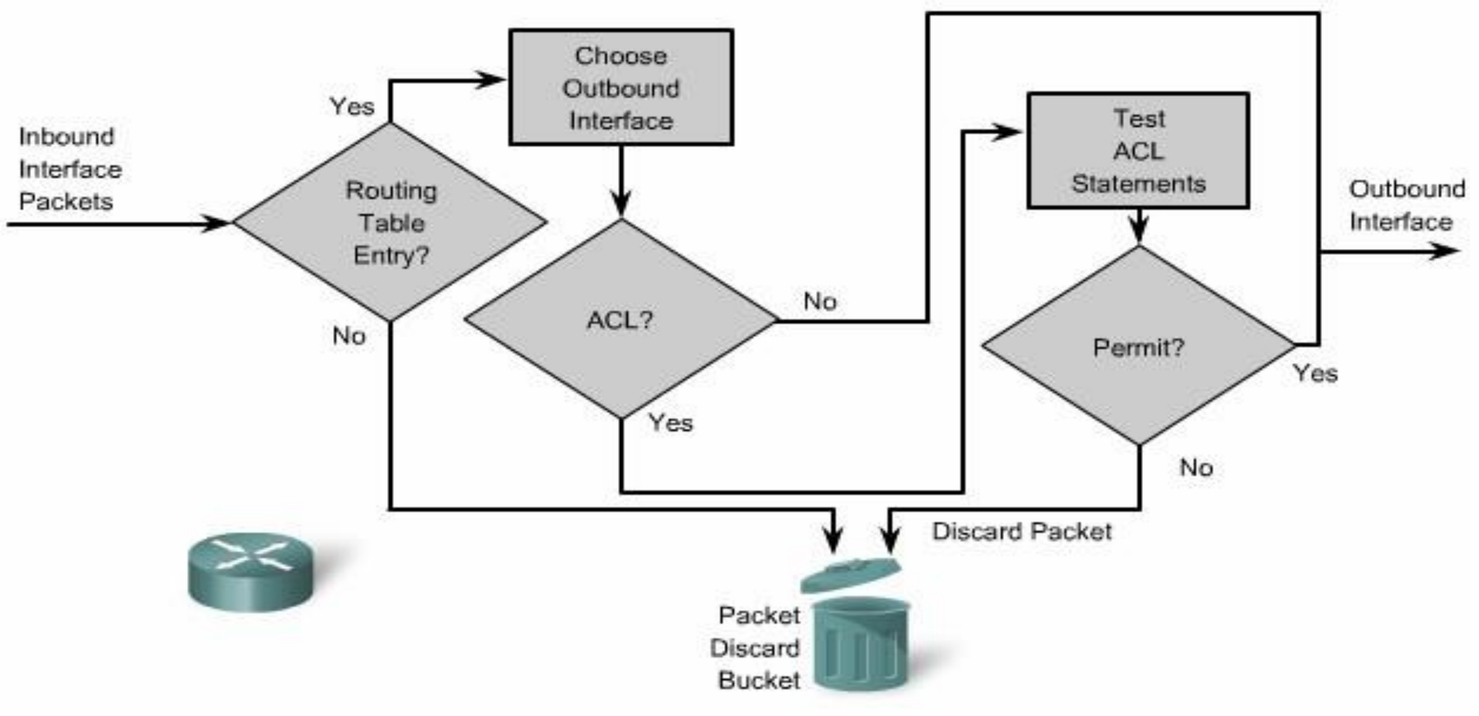
Note: Servers that need less protection, because they may have less critical information, could be placed in the external DMZ network - that is even outside the external firewall.

Access Control List

- ACLs come in two varieties: **Numbered and named**
- Each of these references to ACLs supports two types of filtering: **standard and extended.**
- Standard IP ACLs can filter only on the **source IP address** inside a packet.
- Whereas an extended IP ACLs can filter on the **source and destination IP addresses** in the packet.
- There are two actions an ACL can take: **permit or deny.**
- Statements are processed top-down.
- Once a match is found, no further statements are processed—therefore, order is important.
- If no match is found, the imaginary **implicit deny statement at the end of the ACL** drops the packet.
- An ACL should have at least one permit statement; otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.
- No matter what type of ACL you use, though, you can have only one ACL per protocol, per interface, per direction.

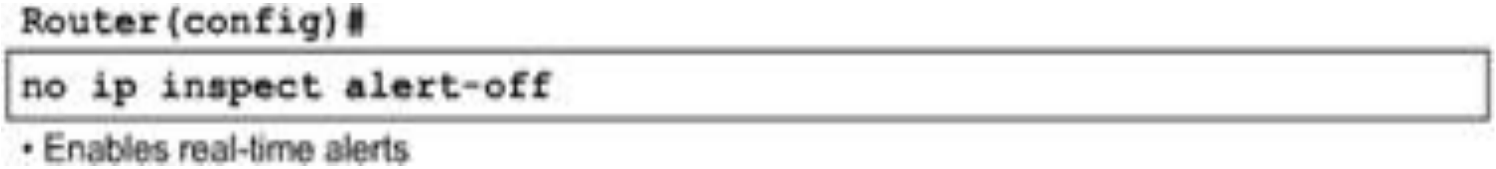
For example, you can have one IP ACL inbound on an interface and another IP ACL outbound on an interface, but you cannot have two inbound IP ACLs on the same interface

How ACLs Work



Inbound **(as the traffic comes into an interface)** **Outbound** **(before the traffic exits an interface)**

Alerts and Audits

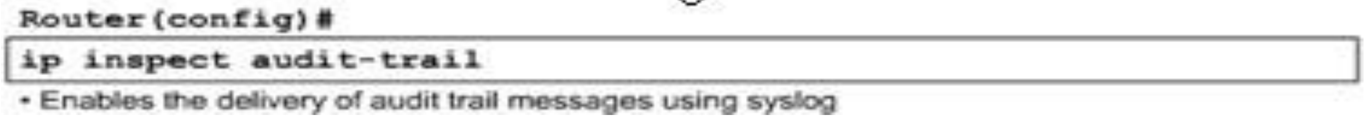


```
Router(config)#
no ip inspect alert-off
```

- Enables real-time alerts

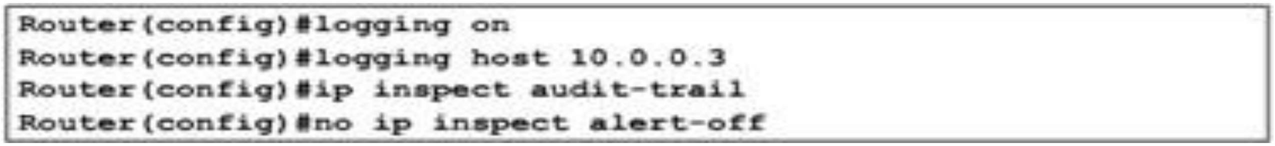
Alerts are enabled by default and automatically display on the console line of the router

If alerts have been disabled using the `ip inspect alert-off` command, the `no` form of that command, as seen above, is required to re-enable alerts.



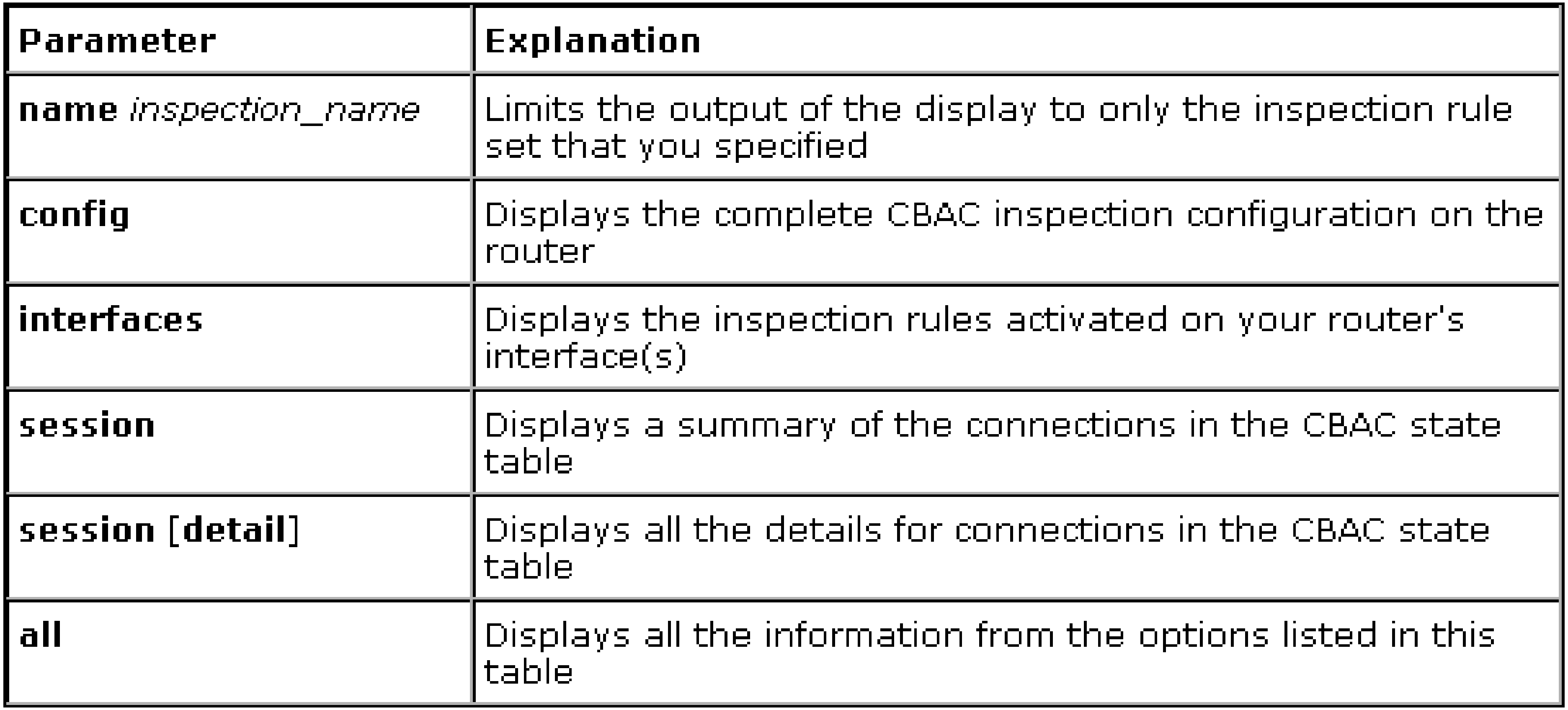
```
Router(config)#
ip inspect audit-trail
```

- Enables the delivery of audit trail messages using syslog



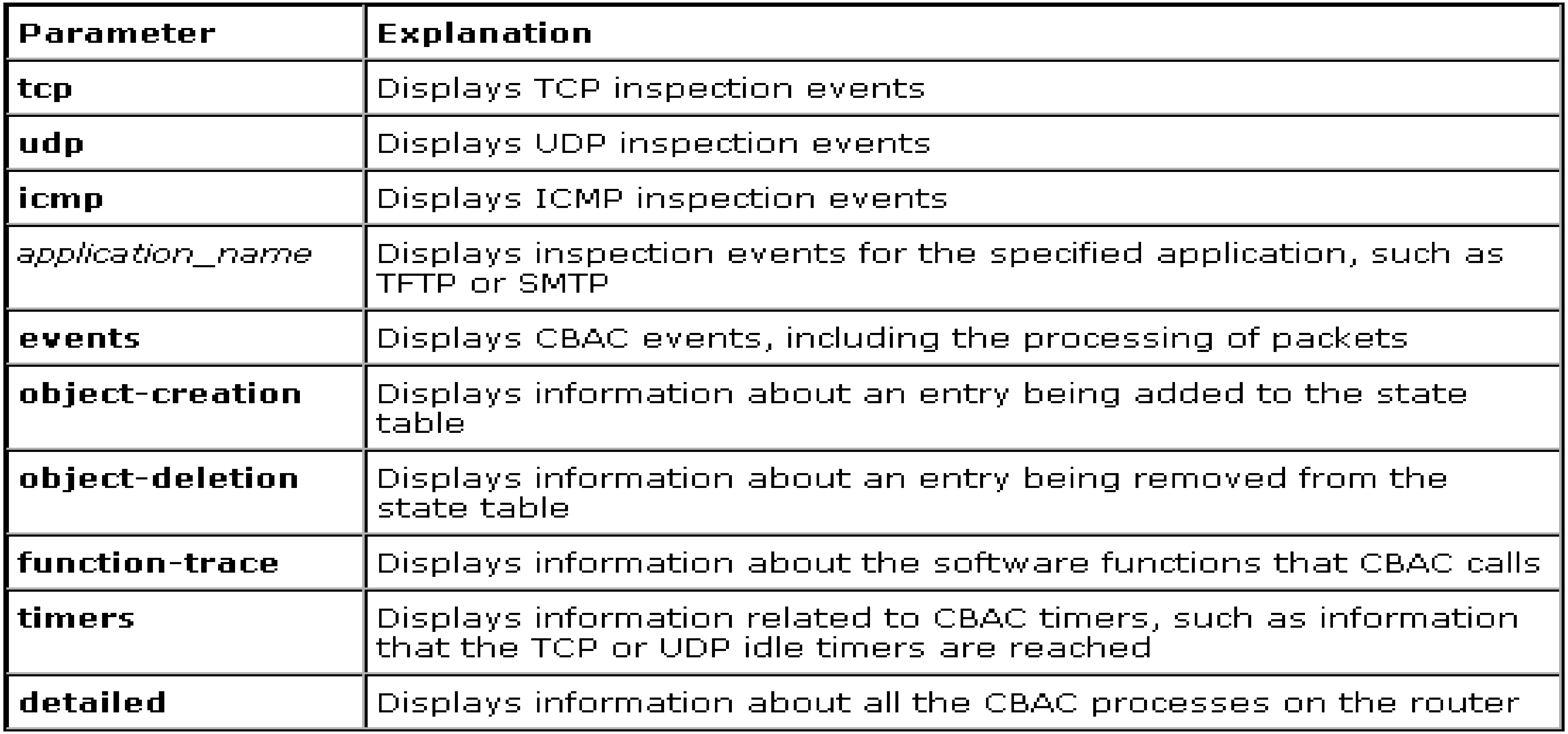
```
Router(config)#logging on
Router(config)#logging host 10.0.0.3
Router(config)#ip inspect audit-trail
Router(config)#no ip inspect alert-off
```

`show ip inspect` Parameters



Parameter	**Explanation**
name *inspection_name*	Limits the output of the display to only the inspection rule set that you specified
config	Displays the complete CBAC inspection configuration on the router
interfaces	Displays the inspection rules activated on your router's interface(s)
session	Displays a summary of the connections in the CBAC state table
session [**detail**]	Displays all the details for connections in the CBAC state table
all	Displays all the information from the options listed in this table

debug ip inspect Parameters

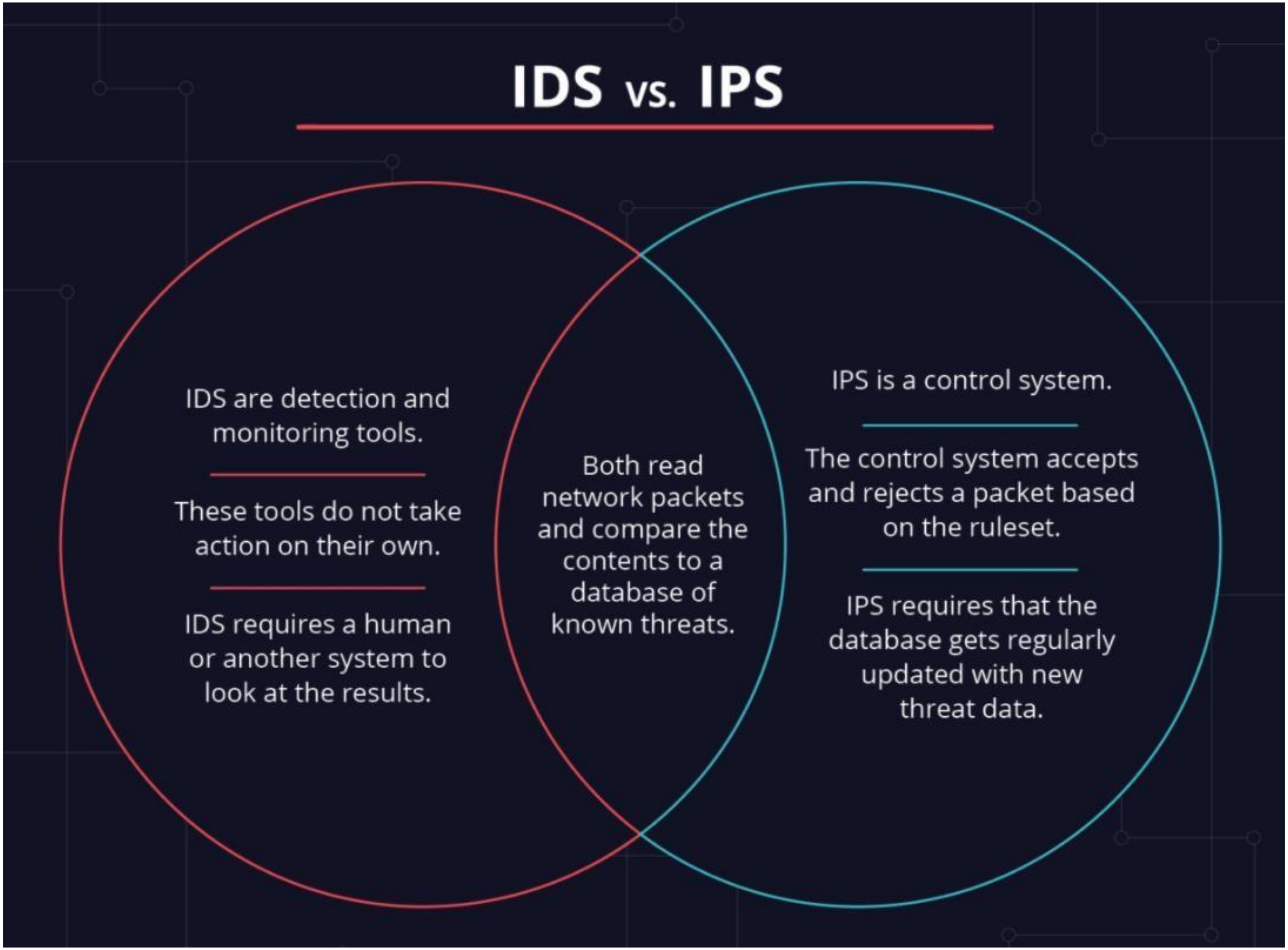


Parameter	Explanation
tcp	Displays TCP inspection events
udp	Displays UDP inspection events
icmp	Displays ICMP inspection events
application_name	Displays inspection events for the specified application, such as TFTP or SMTP
events	Displays CBAC events, including the processing of packets
object-creation	Displays information about an entry being added to the state table
object-deletion	Displays information about an entry being removed from the state table
function-trace	Displays information about the software functions that CBAC calls
timers	Displays information related to CBAC timers, such as information that the TCP or UDP idle timers are reached
detailed	Displays information about all the CBAC processes on the router

Intrusion Detection System

FIREWALL VS IDS

- Firewall cannot detect security breaches associated with traffic that does not pass through it. Only IDS is aware of traffic in the internal network
- Not all access to the Internet occurs through the firewall.
- Firewall does not inspect the content of the permitted traffic
- Firewall is more likely to be attacked more often than IDS
- IDS is capable of monitoring messages from other pieces of security infrastructure
- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks
- CodeReds on IIS
- Solution? - **Intrusion Detection Systems**



IDS vs. IPS

IDS are detection and monitoring tools.

These tools do not take action on their own.

IDS requires a human or another system to look at the results.

Both read network packets and compare the contents to a database of known threats.

IPS is a control system.

The control system accepts and rejects a packet based on the ruleset.

IPS requires that the database gets regularly updated with new threat data.

Comparing IDS and IPS

	Advantages	Disadvantages
IDS	▪ No impact on network (latency, jitter) ▪ No network impact if there is a sensor failure ▪ No network impact if there is sensor overload	▪ Response action cannot stop trigger packets ▪ Correct tuning required for response actions ▪ Must have a well thought-out security policy ▪ More vulnerable to network evasion techniques

	Advantages	Disadvantages
IPS	▪ Stops trigger packets ▪ Can use stream normalization techniques	▪ Sensor issues might affect network traffic ▪ Sensor overloading impacts the network ▪ Must have a well thought-out security policy ▪ Some impact on network (latency, jitter)

Intruders

- unknown/unwanted trespass
  - from benign to serious
- user trespass
  - unauthorized logon, privilege abuse
- software trespass
  - virus, worm, or trojan horse

Examples of Intrusion

- Remote root compromise
- Web server defacement(attack on a website that changes the visual appearance of the site or a webpage.)
- Guessing / cracking passwords
- Copying viewing sensitive data / databases
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access net
- Impersonating a user to reset password
- Using an unattended workstation.

Intrusion Detection

A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

IDS Requirement

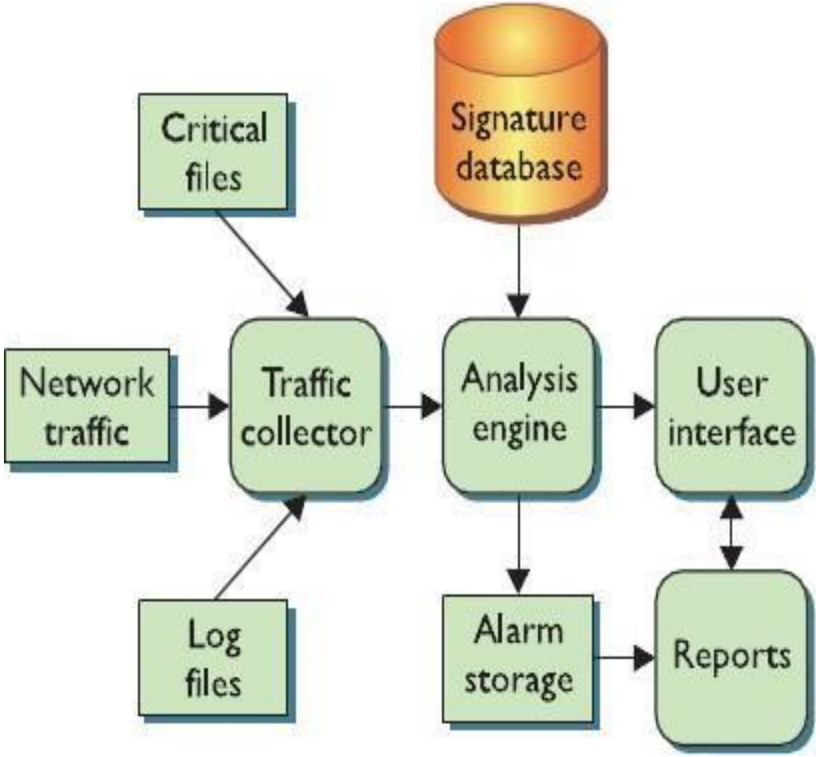
- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

IDPS Types and Options

Criteria	Type	Description
Approaches to Identifying Malicious Traffic	Signature-based	A vendor provides a customizable signature database.
	Anomaly-based	“Normal” and “abnormal” traffic is defined.
	Policy-based	Policy definition and description is created
	Honeypot-based	Sacrificial host is set up to lure the attacker.
Deployment Options	Network-based	Network sensors scan traffic that is destined to many hosts.
	Host-based	Host agent monitors all operations within an operating system.

Intrusion Detection Systems (IDS)

- An IDS to the networking world is like a burglar alarm to the physical world.
- The main purpose of an IDS is to identify suspicious or malicious activity, note activities that deviate from normal behavior, catalog and classify the activity, and, if possible, respond to the activity.
- Host-based IDS (HIDS): It examines activities on an individual system and not concerned with other systems or the network.
- Network-based IDS (NIDS): It examines activity (traffic) crossing the network it is monitoring and not concerned about individual systems.



Logical Depiction of IDS Components

Source: Figure 13.2 from Conklin and White – Principles of Computer Security, 2nd Edition

Logical Components of an IDS

- An intrusion detection system (IDS) is a device, typically a separate computer, that monitors activity to identify malicious or suspicious events.
- An IDS typically consists of several special components (often logical and software-based rather than physical) working together on the device in which it is installed.
- Traffic Collector – Collects activity/events for the IDS to examine. For a HIDS, these could be log files, audit logs, or traffic coming to or leaving a specific system. For a NIDS, these could be network traffic captured through a sniffer.
- Analysis Engine – Examines the collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database. It is often referred to as “brain” of the IDS.
- Signature Database: A collection of patterns and definitions of known suspicious or malicious activity.
- User Interface and Reporting: Interfaces with the human element, providing alerts when appropriate and giving the user a means to interact with and operate the IDS.

Signature and Anomaly-based IDS

- Based on the approach adopted to detect suspicious or malicious traffic, IDS could be categorized into Signature-based and Anomaly-based IDS.
- *Signature-based IDS*: Relies heavily on a pre-defined set of attack and traffic patterns called signatures.
- A signature-based IDS (like an anti-virus software) can only match against known patterns – if a new attack comes in that the signature-based IDS has never seen before, it would not be able to identify it as suspicious or malicious – a primary weakness of signature-based IDS.
- *Anomaly-based IDS*: Monitors activities and attempts to classify them as either "normal" or "anomalous" (suspicious and unknown) based on self-created rule sets.
- An anomaly-based IDS uses heuristic techniques to categorize and classify traffic while developing and refining their internal rule sets.
- An advantage with anomaly-based IDS is that it can potentially detect new attacks or variant of old attacks.
- A drawback of anomaly-based IDS is that it could generate a potentially high number of false positives while the system is learning what "normal" is. Hence, such IDS should be programmed to dynamically adapt to changes.

Signature-based IDS

- Example for detecting an attack using signature-based IDS:
  - Detecting the TCP SYN flood attack using a port scan
    - An IDS would probably find nothing unusual in the first SYN (say to port 80) and then another SYN (from the same source address) to port 25.
    - But as more and more ports (especially closed ports) receive SYN packets, the pattern will reflect a possible port scan that happened already

- A problem with the signature-based IDS is the signature itself: An attacker will try to modify a basic attack in such a way that it will not match the known pattern of the attack.
  - For example, an attacker may convert lowercase to uppercase characters, characters by the ASCII equivalents and etc.
- An IDS has to learn more signature patterns to catch an attack with different patterns.
- Statistical analyses are nowadays used to detect attacks with patterns that match with the stored signatures within a certain probability of error.

Anomaly/ Heuristic-based IDS

- Like the signature-based IDS, heuristic-based IDS is limited by the amount of information the system has seen (to classify actions into the right category) and how well the current actions fit into one of the categories.
- Activities could be classified into three categories: Good/ Benign, Suspicious and Unknown.
  - Over time, specific kinds of actions can move from one category to another depending on whether the IDS learnt in due course that certain actions are acceptable or not
- Model-based IDS: Develop standard models for certain activities. If the activities violated the model, raise an alarm.
  - Example: A normal behavior of an employee to start his day in the work environment would be to read emails, write many documents using a word processor, and occasionally backup files, etc. If an employee accesses system sensitive management utilities immediately after login, it could raise an alarm.
- State-based IDS: Monitor the system as it goes through different state changes. If the rate of state change is faster than a threshold or the system has entered into previously unseen state, or the system has veered into an unsafe mode, it could raise an alarm.
- Misuse-based IDS: Identify activities that could be easily misused.
  - Example: An attempt to access a password file is suspect, except for few utilities like login, password change, create user.

Policy Based IDS

Policy-Based - This approach requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators

Policy-based techniques establish boundaries between the allowed and not allowed events by imposing a set of rules.

It solves two major problems: (1) detection of unknown attacks, (2) classification of normal unseen behavior into attack class. This approach is flexible.

Drawback

First, a security specialist is required to design effective policies.

Second, defined policies should be consistent and in a logically correct state throughout the system to avoid any adverse circumstances.

Policies are interrelated through their associated conditions, and, therefore, there may exist inter or intrapolicy conflicts as an incoming event may trigger more than one rule either within a policy or between two policies.

Moreover, these policies are usually implemented sequentially, and improper ordering can cause a feedback loop or deadlock situation.

However, ontology-based systems can be used to simplify the policy specification and management tasks.

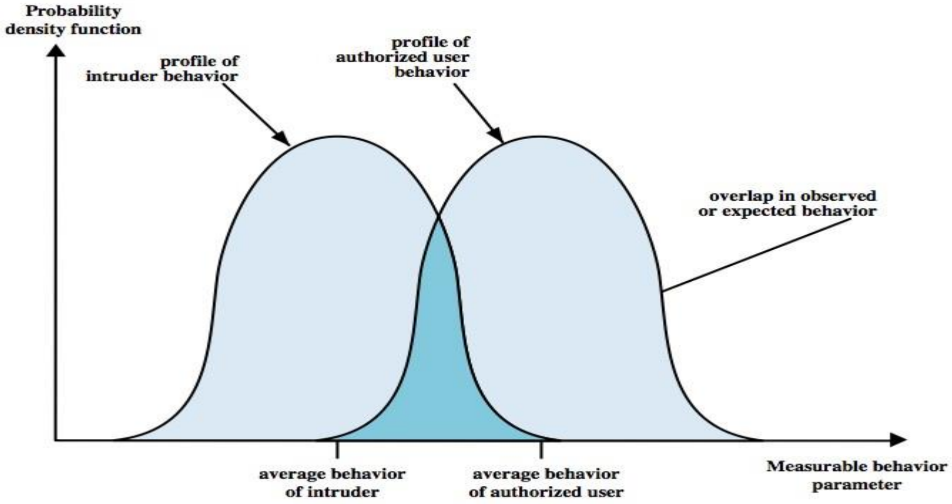
Honeypot

- A honeypot is a trap to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. –
- A honeypot is usually a computer, and sometimes data or an unused IP address space that appears to be part of a network but which is actually isolated, unprotected and monitored, and which seems to contain information or a resource that would be of value to attackers.
- Honeypots have no production value and hence should not see any legitimate traffic or activity. Whatever they capture can be surmised as malicious or unauthorized.
- A honeynet is a network of honeypots. A honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient.
- A honeypot/ honeynet is more of a preventative approach of detecting potential attackers existing in the Internet who may target the organization network in the near future.
- Honeypots could be used to fake as open relays to attract spam emails and determine the source e-mail address and destination e-mail addresses used by the spammers.
  - An open relay is an e-mail server that allows anyone on the Internet to send email through it.
  - Once they find an open relay, spammers keep sending the span email to the open relay and expect it to spread the spam.
- Note that no ordinary e-mail will come to a honeypot. All it receives could be categorized as spam.

Approaches to Identifying Malicious Traffic	Advantages	Disadvantages
Signature-based Detection	• Easy configuration • Fewer false positives • Good signature design	• No detection of unknown signatures • Initially a lot of false positives • Signatures must be created, updated, and tuned
Anomaly-based Detection	• Simple and reliable • Customized policies • Can detect unknown attacks	• Generic output • Policy must be created
Policy-based Detection	• Easy configuration • Can detect unknown attacks	• Difficult to profile typical activity in large networks • Traffic profile must be constant
Honey Pot-Based Detection	• Window to view attacks • Distract and confuse attackers • Slow down and avert attacks • Collect information about attack	• Dedicated honey pot server • Honey pot server must not be trusted

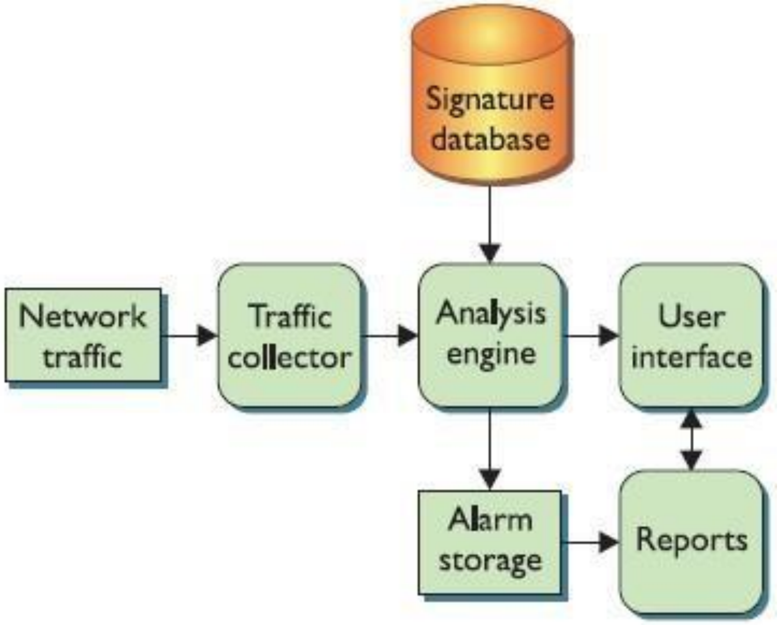
False Positives and False Negatives

- When an IDS matches an activity to a specific pattern and generates an alarm for a non-malicious traffic that is not a threat, it is called a false positive.
- Technically, the IDS is functioning correctly by matching the pattern and has no ability to determine the intent behind the activity; but, from a human standpoint, this is not an information the analyst needed to see, as it does not constitute a threat and does not require intervention.
- Hostile activity that does not match an IDS signature and goes undetected is called a false negative.
- Note that an IDS is limited by its signature set – it can match only activity for which it has stored patterns.


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

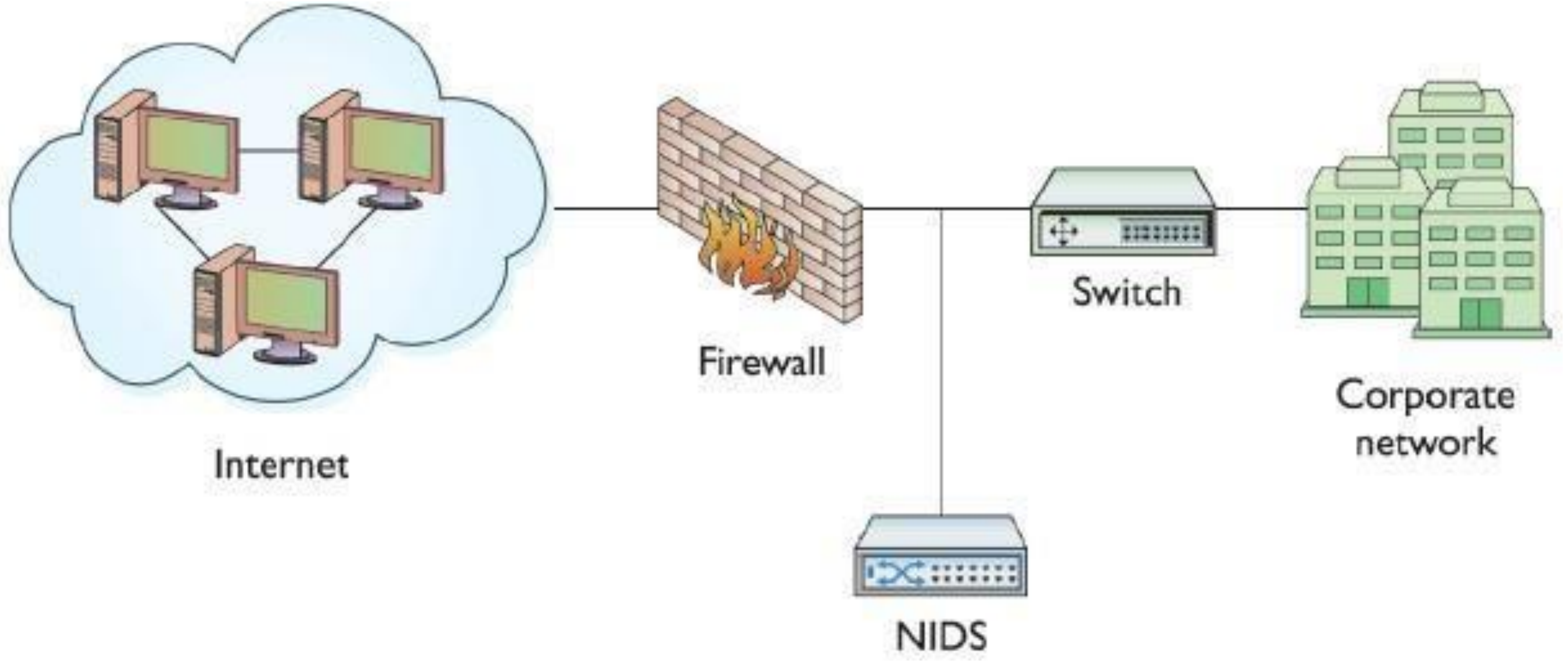
Network-based IDS (NIDS)

- NIDS are placed next to the firewall on the network perimeter and analyze the traffic as it passe by for the protocols, source, destination, content, traffic already seen and etc.
- A NIDS typically looks for traffic that typify hostile actions or misuse, such as the following:
    - Denial-of-service attacks, Port scans or sweeps, Malicious content in the data payload of a packet or packets, Vulnerability scanning, Trojans, Viruses, Worms, Tunneling and Brute-force attacks.
- The traffic collector of a NIDS logically attaches itself to a Network Interface Card (NIC) that operates in promiscuous mode (stealth mode) and sniffs the passing traffic.



Source: Figure 13.4 from Conklin and White – Principles of Computer Security, 2nd Edition

NIDS Placed behind Firewall



Source: Figure 13.7 from Conklin and White – Principles of Computer Security, 2nd Edition

NIDS: Advantages and Disadvantages

- Advantages of a NIDS
- Less Overhead: With a few well-placed NIDSs, one can monitor the entire network traffic going in and out of the organization. Also, upgrading and maintaining a fewer number of NIDSs is usually much cheaper than upgrading and maintaining hundreds of host-based IDSs.
- Big Picture: The collection of the few NIDSs can have visibility into all the network traffic and can correlate attacks (whether they are widespread or concentrated, unorganized or focused) among multiple systems.
- Disadvantages of a NIDS
- A NIDS is ineffective when traffic is encrypted.
- A NIDS cannot see traffic that does not cross it – If a NIDS is placed only in the perimeter, chances are that it could miss traffic traversing the internal network.
- A NIDS must be able to handle high volumes of traffic (even 1-Gbps is common nowadays) with the availability of networks with larger bandwidth.
- A NIDS does not know about activities on the hosts themselves.

Active vs. Passive NIDS

Passive NIDS:

- A passive NIDS simply watches the traffic, analyzes it and generates alarms.
- It does not interact with the traffic itself in any way, and it does not modify the defensive posture of the system to react to the traffic.

Active NIDS:

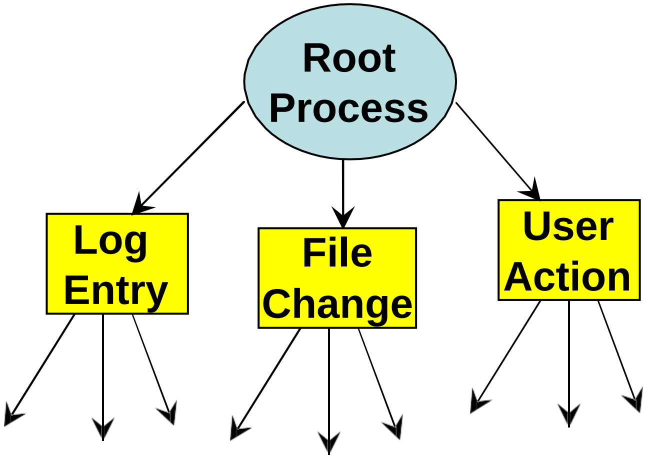
- An active NIDS contains all the same components and capabilities of the passive NIDS with one critical addition – the active NIDS can react to the traffic it is analyzing.
- The reactions of an active NIDS could range from something simple, such as sending a TCP reset message to interrupt a potential attack and disconnect a session, to something complex, such as dynamically modifying firewall rules to reject all traffic from specific source IP addresses for the next few hours or days.
- Active NIDS are also referred to as Intrusion Prevention Systems (IPSs). When configured with the private keys of the servers in the internal network, IPSs would be able to decrypt the SSH connection establishment messages between a client and server and extract the session keys that would be used during the complete session. This gives an added advantage for the IDS/IPS to handle encrypted traffic.

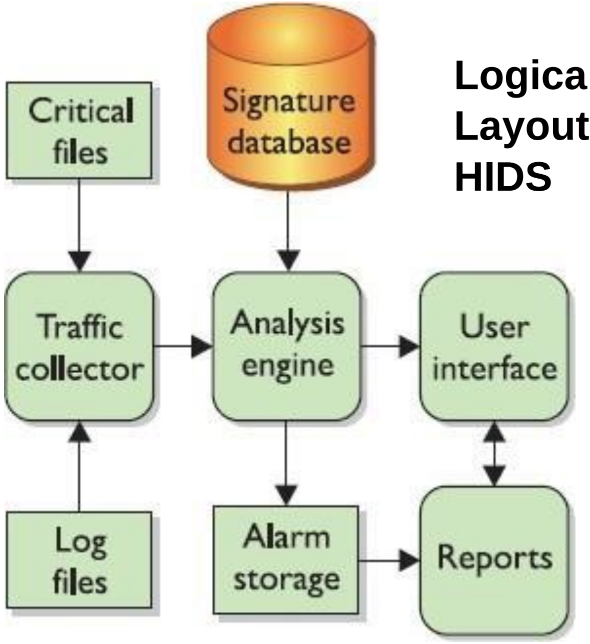
Host-based IDS (HIDS)

- A host-based IDS (HIDS) examines log files, audit trails (both generated by the local operating system), and network traffic coming into or leaving a specific host.
  - On UNIX systems, the examined logs are those created by syslog, kernel logs and error logs; On Windows systems, the examined logs are the event logs – Application, System and Security.
- Critical files are those that are vital to the system's operation or overall functionality. They may be program (or binary) files, files containing user accounts and passwords, or even scripts to start or stop system processes.
- Any unexpected modifications (for e.g., could be detected using checksum) to the critical files could mean the system has been compromised or modified by an attacker. By monitoring these critical files, the HIDS can warn users of potentially malicious activity.
- Within the log files, the HIDS is looking for certain activities that typify hostile actions or misuse, such as the following:
  - Logins at odd hours, Login authentication failures, Additions of new user accounts, Modification or access of critical system files, Modification or removal of binary files (executables), Privilege escalation

Host-based IDS (HIDS)

- HIDSs can operate in real-time, looking for activity as it occurs, or in batch mode, looking for activity on a periodic basis.
- HIDS will use up some of the local system resources (like memory and CPU cycles) to operate.
- The Analysis Engine of a HIDS could also use a decision tree to expedite pattern matching.





Logical Layout of a HIDS

Source: Figure 13.16 from Conklin and White – Principles of Computer Security, 2nd Edition

Advantages of HIDS

- A HIDS can be very operating system-specific and have more detailed signatures.
- A HIDS can reduce false-positive rates.
  - Administrators can avoid generic alarms and develop more specific, detailed signatures to identify malicious traffic much more accurately.
- A HIDS can examine data after it has been decrypted.
  - Encrypted traffic that is unreadable to a NIDS could be examined using a HIDS, when designed and implemented in the right manner.
- A HIDS can be very application specific.
  - At the host level, a HIDS can be designed, modified or tuned to work very well on specific applications without having to analyze or even hold signatures for other applications that are not running on that particular system.
- A HIDS can determine whether or not an alarm may impact that specific system.
  - Since a HIDS resides on the system, it can verify things such as patch levels, presence of certain critical files and system state while analyzing traffic. By knowing all these details, a HIDS can more accurately determine whether an activity or pattern would be potentially harmful to the system. This can significantly reduce the number of generated alarms.

Disadvantages of HIDS

- The HIDS must be installed on every system to be protected.
- The HIDS can have a high cost of ownership and maintenance. Even with a central console, with a HIDS, there will be a high number of processes to maintain, software to update, and parameters to tune.
- The HIDS uses local system resources.
  - The resources (for e.g., CPU cycles and memory) used by a HIDS are no longer available for the host system to perform its other functions.
- The HIDS has a very focused view and cannot relate to activity around it – can tell only if the system it is running on is under attack.
- The HIDS, if logged locally, could be compromised or disabled.
  - If the HIDS stores its generated alarm traffic on the local system, an attacker who is successful in breaking into the system may be able to modify or delete those alarms. Even though the presence of an empty log file could indicate that the system was attacked, it would not be possible to conduct any sort of post-incident investigation.
  - **Solution:** It would be a better security practice to store or make a copy of the log information (at least security-related) on a separate system.

Malicious Software

Packet Sniffer (Protocol Analyzer)

- Packet Sniffer: Is a computer software (or even a computer hardware programmed to) intercept and log traffic passing over a LAN.
- A packet sniffer may be used for both beneficial and malicious purposes:
  - Analyze network problems and monitor network usage
  - Gather and report network statistics
  - Filter suspect content from network traffic
  - Spy on other network users and collect sensitive information such as passwords
  - Reverse engineer (study using the structure of the different packet headers) the protocols used over the network
  - Detect network intrusion attempts
  - Gather information for effecting a network intrusion
- In order to capture all the network traffic, the Network Interface Card (NIC) on the IDS hosting the packet sniffer should run in promiscuous mode and analyze every packet crossing the wire.
- Most switches come with SPAN (Switched Port Analyzer) port – a mirrored port that will see all the traffic passing through the switch or through specific virtual LANs. Packet sniffers can be run on the SPAN port of a switch.

Malware

Malware, is software designed to break into or damage a computer system without the owner’s consent. Hostile or intrusive code is malware

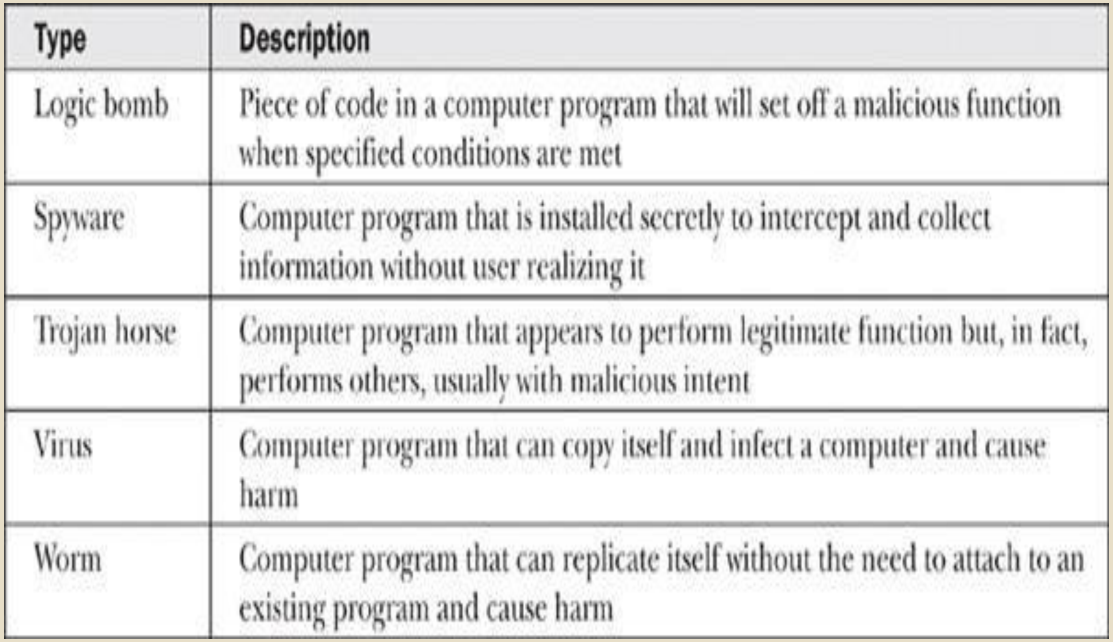
It is a malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.

Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts.

In this manner, self-replicating malware can spread exponentially fast.

Types of Malware

- **Virus** – A malware which requires some form of user’s interaction to infect the user’s device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.
- **Worm** – A malware which can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept the malware from the Internet and run it, creating a worm.
- **Botnet** – A network of private computers infected with malicious software and controlled as a group without the owners’ knowledge, e.g. to send spam.



Type	Description
Logic bomb	Piece of code in a computer program that will set off a malicious function when specified conditions are met
Spyware	Computer program that is installed secretly to intercept and collect information without user realizing it
Trojan horse	Computer program that appears to perform legitimate function but, in fact, performs others, usually with malicious intent
Virus	Computer program that can copy itself and infect a computer and cause harm
Worm	Computer program that can replicate itself without the need to attach to an existing program and cause harm

THREE METHODS TO DETECT MALWARE-

Signature Detection
Change Detection
State Detection

Signature Detection

- It detects the patterns or signatures in a particular program that may be malware.
- When malware is suspected, it is verified against the database of known bad code fragments.
- ADVANTAGE

Users and administrators can perform a simple precautionary measure keeping signature files up to date and periodically scanning for viruses.

- DISADVANTAGE

The signature files may be quite large, which makes scanning slow

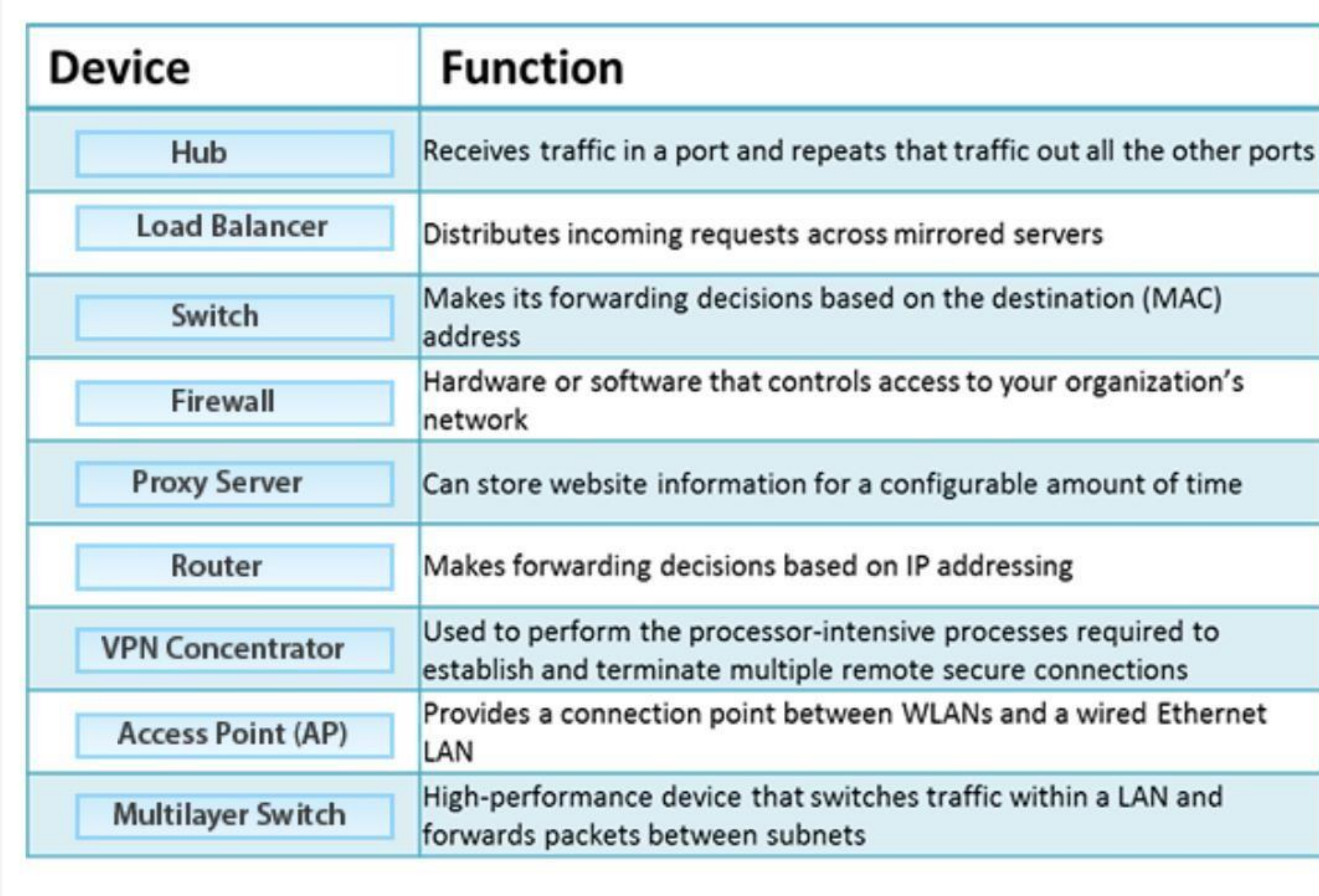
Change Detection

- Finding files that have been changed is called *change detection.*
- A file that changes unexpectedly may be due to a virus infection.
- Advantages:

If a file has been infected, a change can be detected. An unknown malware, one not previously identified (zero-day), can be detected through change detection.

State Detection

- *State detection* aims to detect unusual/ anomalous behavior.
- It relies on an expert system that determines if a state change is anomalous.
- These state changes includes malicious behavior; by extension, anomaly detection is the ability to identify potentially malicious activity.
- To determine what is normal and what is unusual and to be able to distinguish between the two.



Device	Function
Hub	Receives traffic in a port and repeats that traffic out all the other ports
Load Balancer	Distributes incoming requests across mirrored servers
Switch	Makes its forwarding decisions based on the destination (MAC) address
Firewall	Hardware or software that controls access to your organization's network
Proxy Server	Can store website information for a configurable amount of time
Router	Makes forwarding decisions based on IP addressing
VPN Concentrator	Used to perform the processor-intensive processes required to establish and terminate multiple remote secure connections
Access Point (AP)	Provides a connection point between WLANs and a wired Ethernet LAN
Multilayer Switch	High-performance device that switches traffic within a LAN and forwards packets between subnets