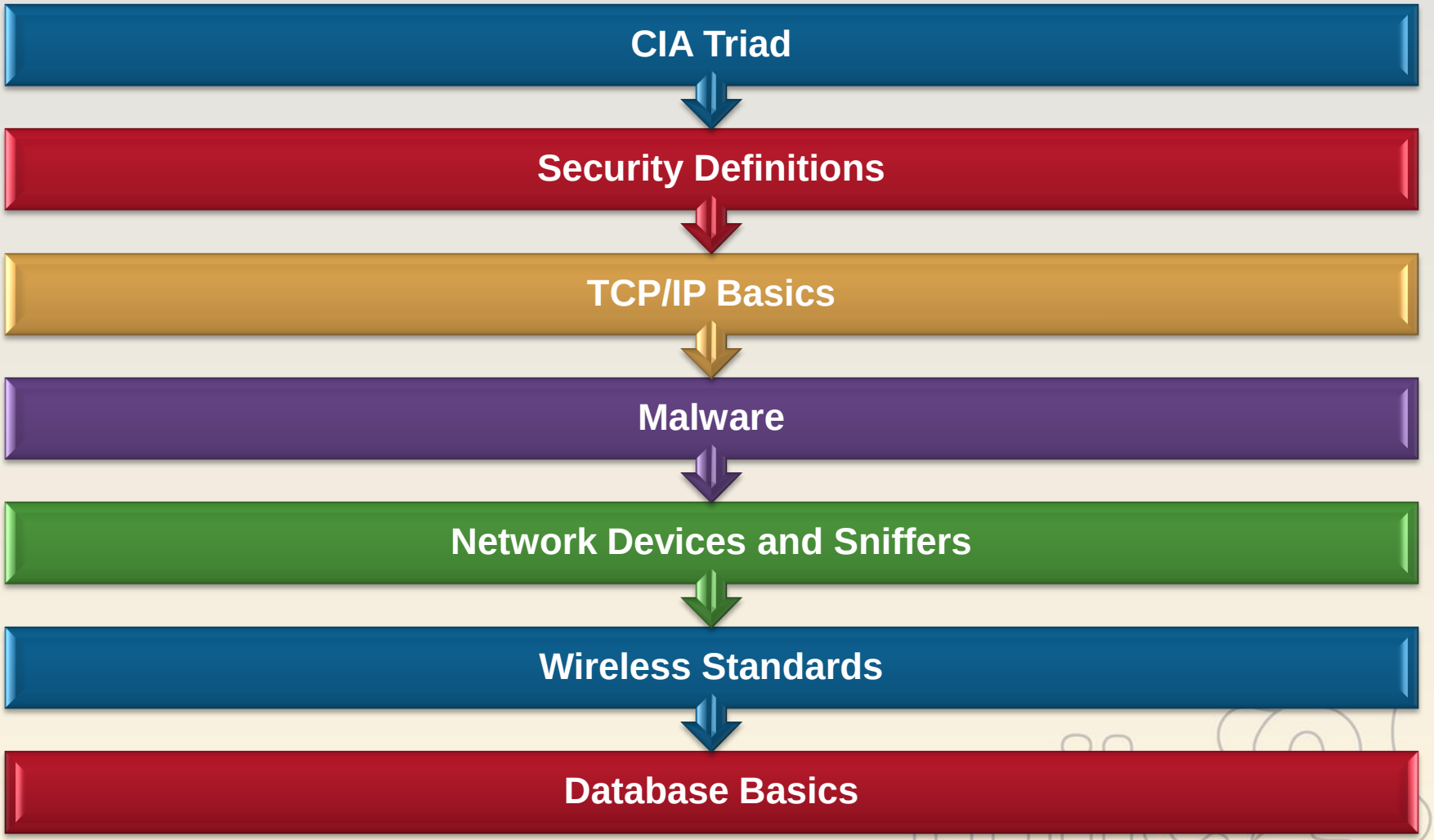
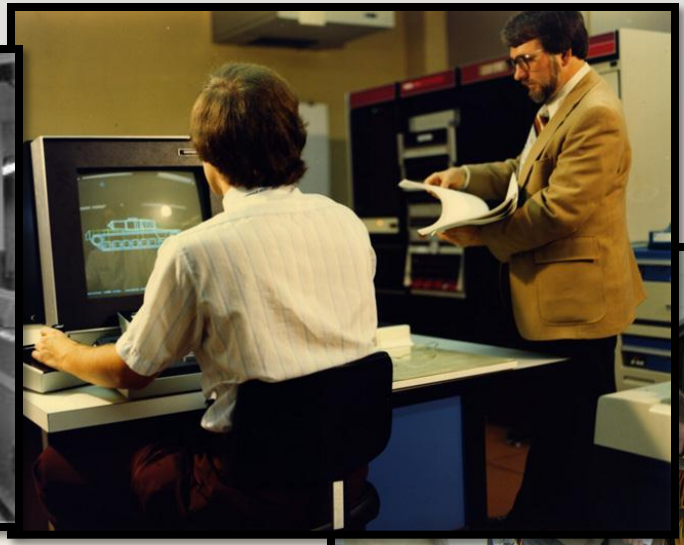
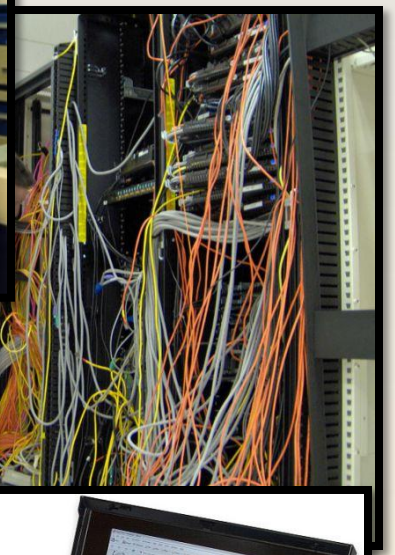
The Basics

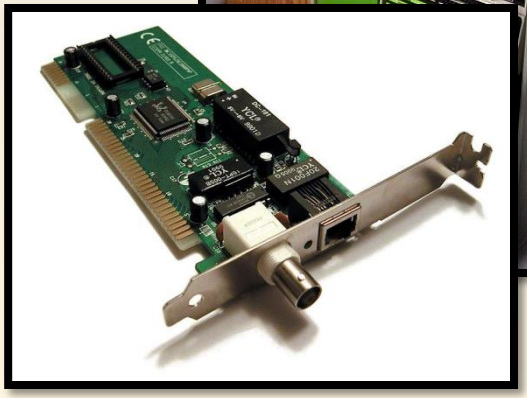
Overview



The Growth of Environments and Security



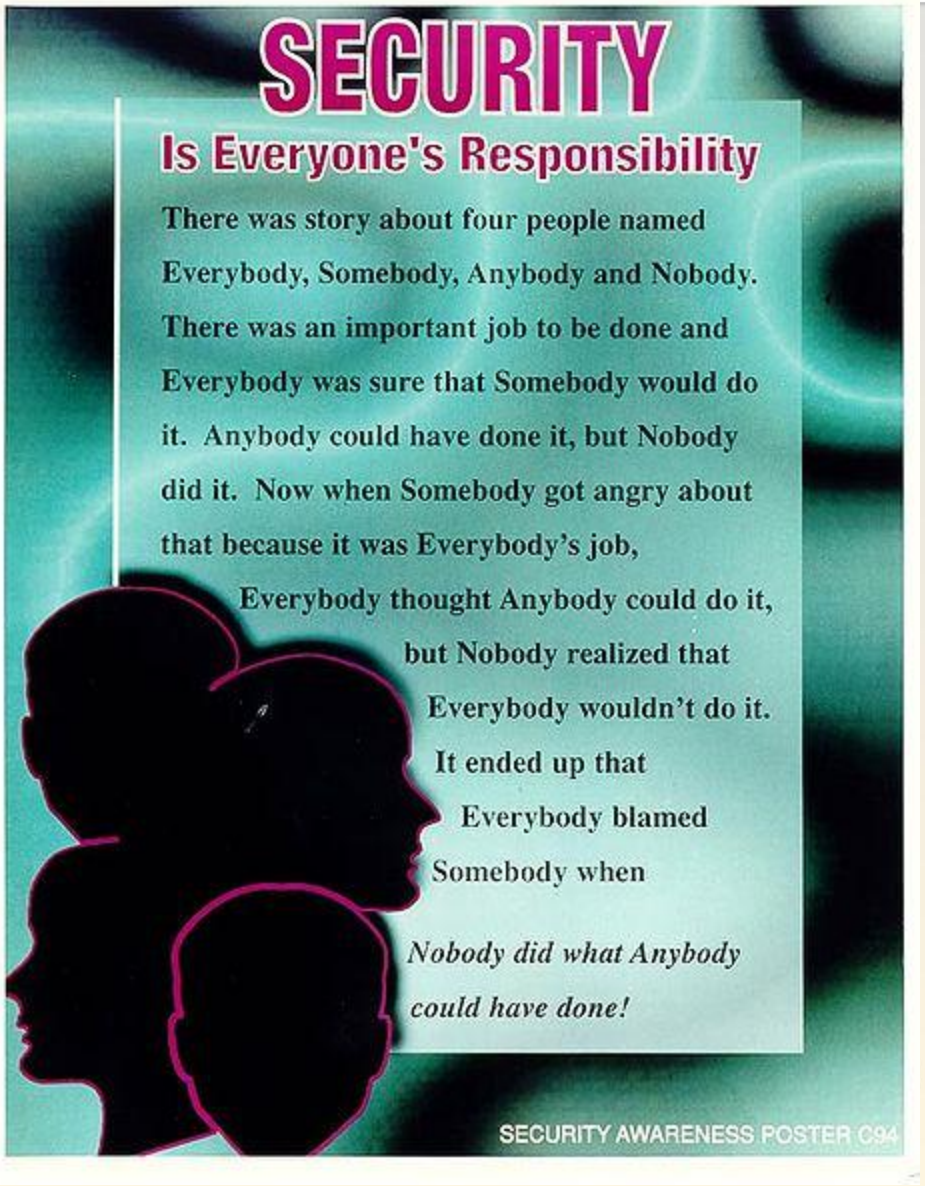




Our motivation…

The exponential rise in cyber crime.

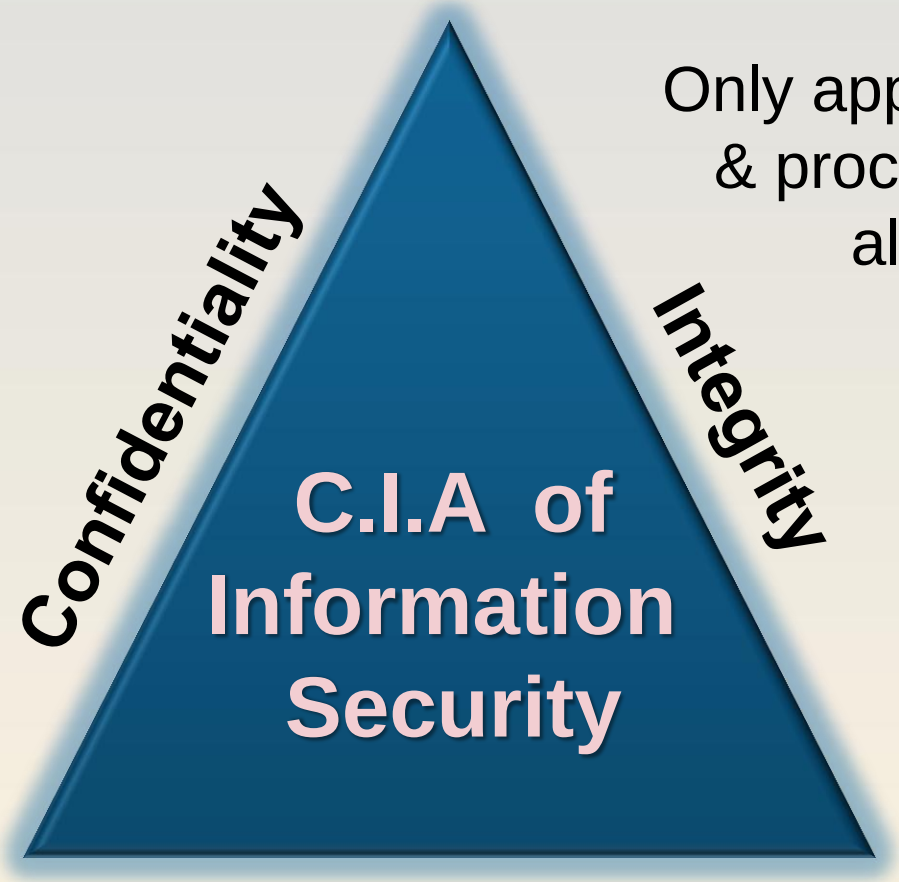
Prevention is far more realistic than prosecution.



The Goal: Protecting Information!

Only approved persons should access data.

Only approved persons & processes should alter data.



Availability

Data must remain available when and where needed.

CIA Triad in Detail

Confidentiality

- Secrecy, sensitivity, privacy
- Prevents unauthorized disclosure of data
- Protects sensitive data and processes from things like:
  - Shoulder surfing
  - Social engineering

Integrity

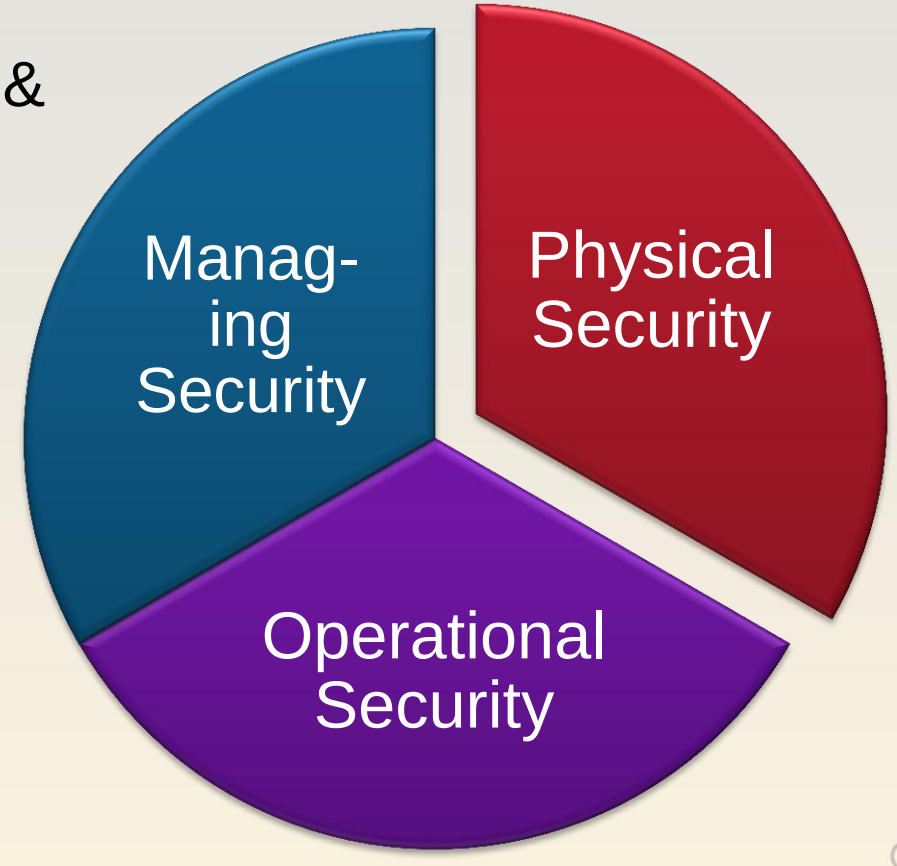
- Accuracy, completeness
- Prevents unauthorized modification
- Protects data and production environment from things like:
  - Modifying data or configurations
  - Changing security log information

Availability

- Usability, timeliness
- Prevents disruption of services
- Protects production and productivity from things like:
  - Man-made, technical, or natural disaster
  - Failure of components or a device
  - Denial-of-service attacks

Approach Security *Holistically*

Enforcing & guiding a culture of security.



Securing the facilities.

Behaving & “being” secure.

Security Definitions

Vulnerability

- Weakness in a mechanism that can threaten the confidentiality, integrity, or availability of an asset
- Lack of a countermeasure

Threat

- Someone uncovering a vulnerability and exploiting it

Risk

- Probability of a threat becoming real, and the corresponding potential damages

Exposure

- When a threat agent exploits a vulnerability

Countermeasure

- A control put into place to mitigate potential losses

Definitions Relationships

TCP/IP Basics

Method: Ping

Basic network connectivity can be tested using the ping command. To determine the range of IP addresses mapped to a live host.

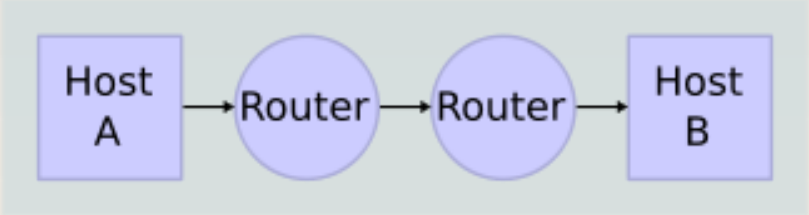
Ping sends out ICMP Echo Request packets and if the address is live, an ICMP Echo Reply message will be received from an active machine.

Alternatively, TCP or UDP packets can be sent if ICMP messages are blocked.

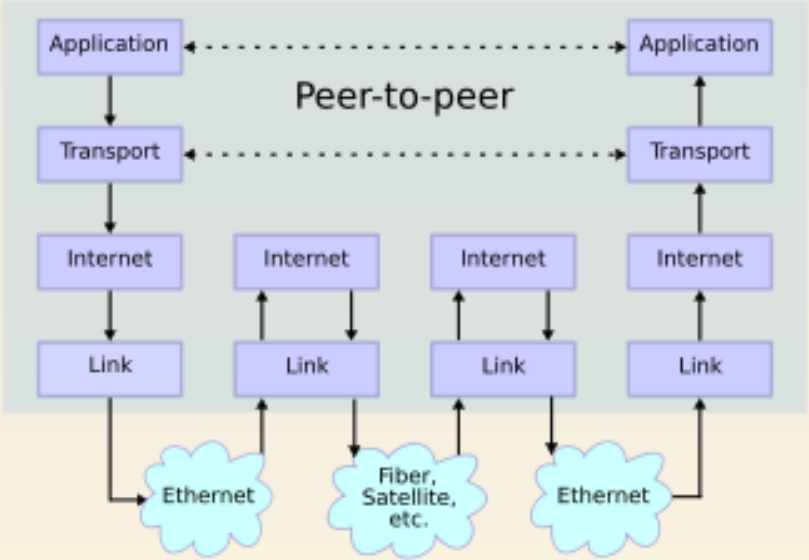
Num	Source Address	Dest Address	Summary
1	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
2	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
3	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
4	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
5	209.59.165.80	194.111.81.189	ICMP: Echo (ping) reply
6	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request
7	194.111.81.189	209.59.165.80	ICMP: Echo (ping) request

The TCP/IP stack

Network Connections



Stack Connections

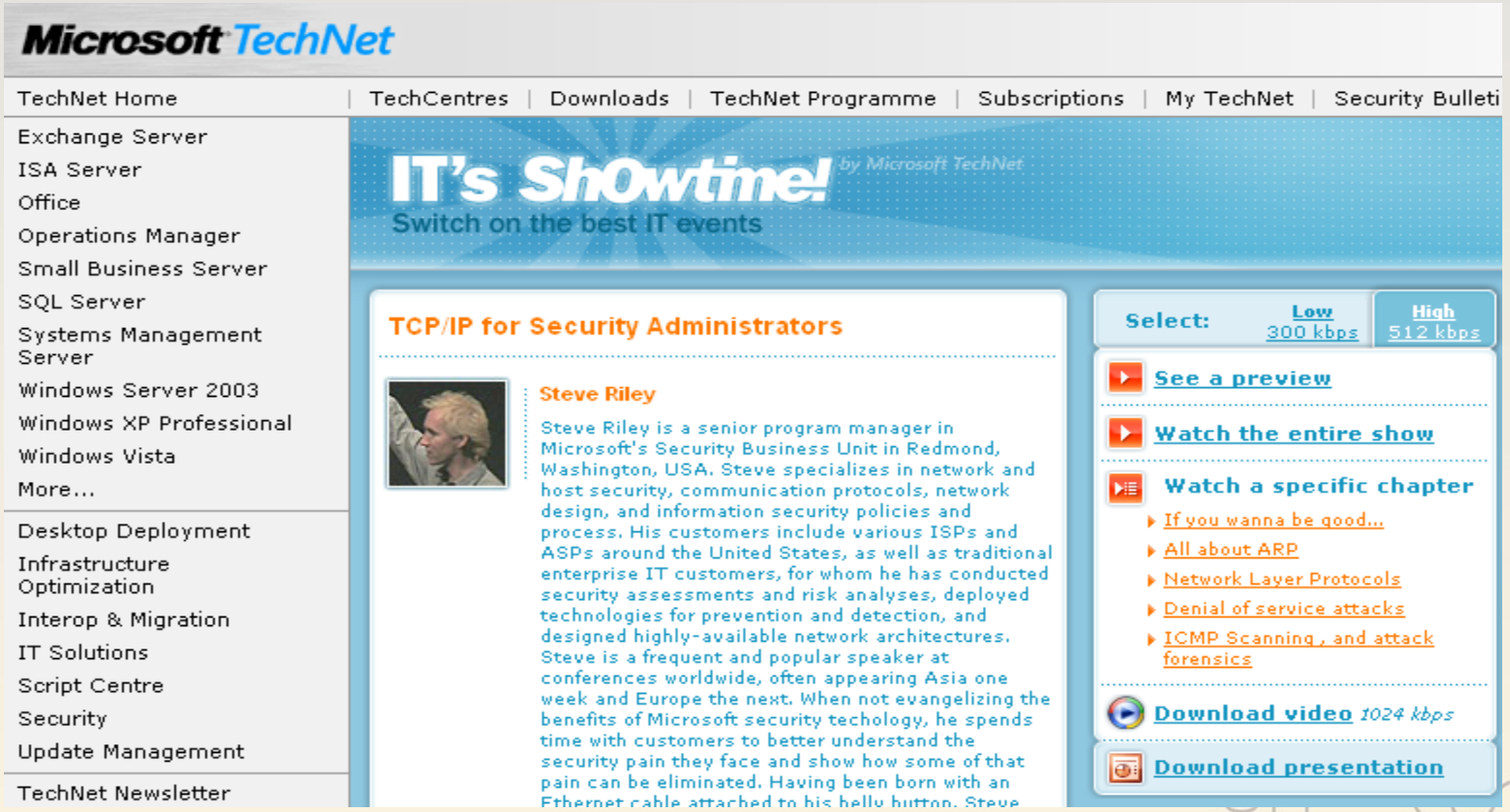


OSI Model	*DoD Model*	*TCP/IP Suite of Protocols*						
Application	Application (Port)	HTTP 80	SNMP 161 162	FTP 20 21	TFTP 69	SMTP 25	Telnet 23	NNTP 119
Presentation								
Session								
Transport	Host to Host	TCP			UDP			
Network	Internet	ICMP	IP					
			ARP					
Data Link	Network Access	Network Devices						
Physical								

http://en.wikipedia.org/wiki/TCP/IP_model

Recommended Video: It's Showtime

TCP/IP for security Administrators



http://www.microsoft.com/emea/spotlight/sessionh.aspx?videoid=9

Which services use which ports?

These Internet sites list port numbers and associated applications:

http://www.iana.org/assignments/port-numbers

- This lists well known and registered port numbers. This is the main reference for port numbers.

http://glocksoft.com/trojan_port.htm

- This is a list of which Trojans run on which ports

http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html

- This site lists a combination of the two: both well known/registered and Trojan port numbers.

TCP 3-Way Handshake

you

server

SYN, client sequence #X

SYN, server sequence #Y, Ack

Ack

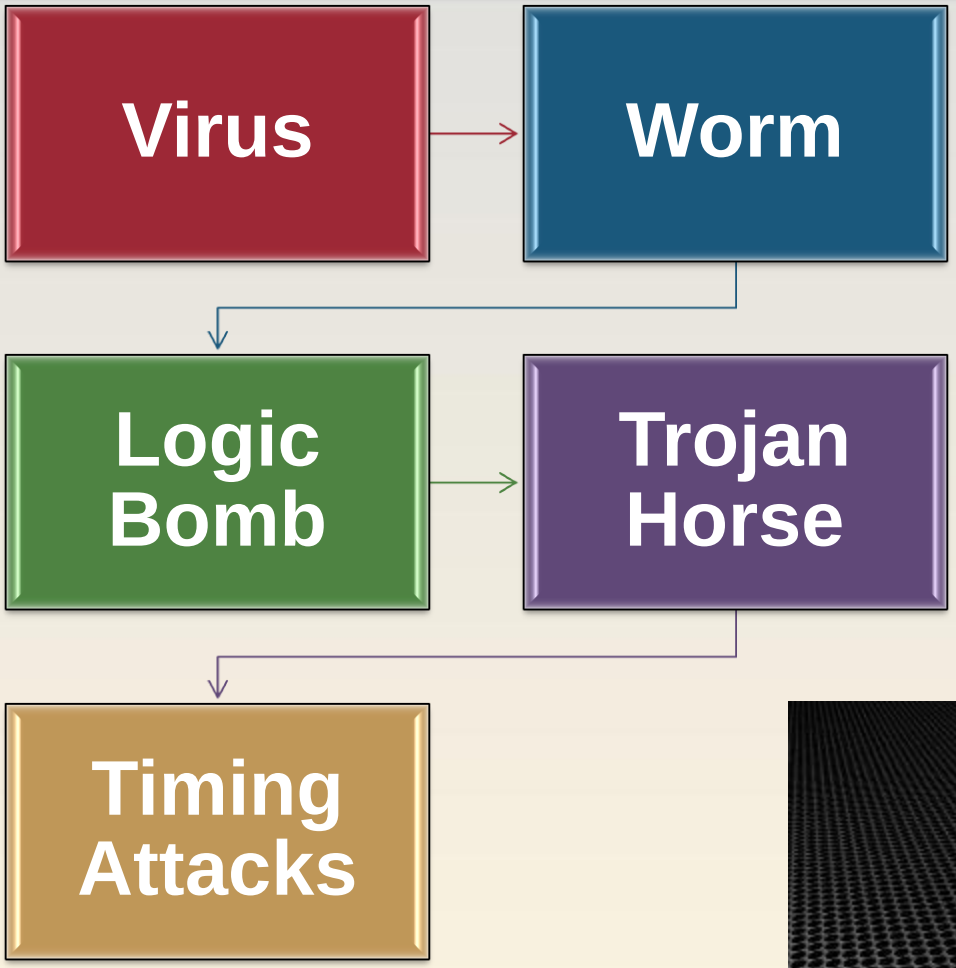
TCP connections begin with your system sending a SYN packet to the server. The server responds with a SYN/ACK. Then your system responds with an ACK, and the connection is established.

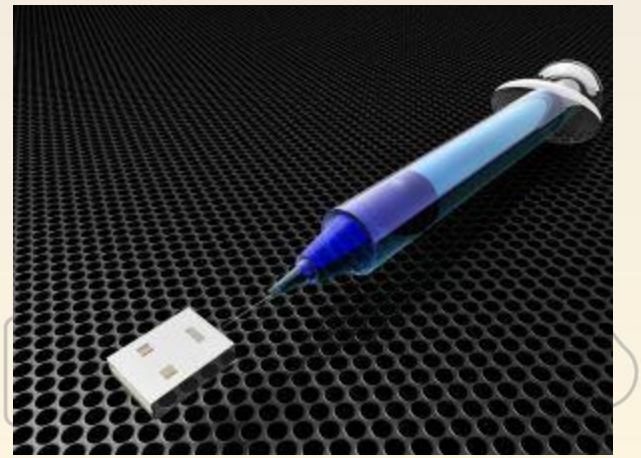
TCP Flags

SYN	synchronize sequence number
ACK	acknowledgement of sequence number
FIN	final data bit is used during the 4 step teardown sequence
RST	reset bit is used to close the connection without going through the 4-step teardown sequence
PSH	Push data bit is used to signify that the data in this packet should be put at the beginning of the queue of data to be processed
URG	Urgent data bit is used to signify that there is urgent control characters in this packet that need to be processed immediately

Malware

Malware





Types of Malware

Worms

- Can reproduce on their own – different to virus
- Self-contained programs

Logic Bomb

- An event triggers the execution of specific code

Trojan Horse

- Program disguised as another program
- Useful program that contains hidden code exploiting the authorization process, enabling it to violate security

Types of Malware Cont...

Virus

- A ***virus*** is a small application, or string of code, that infects applications.
- Fred Cohen wrote the first virus in 1983 to demonstrate the concept because so many people did not believe it was possible
- It is estimated that there are about 60,000 different viruses today.

Types of Viruses

Macro virus is easy to create because of the simplicity of the macro language

Boot sector virus is malicious code inserted into the disk boot sector

Compression virus initializes when it is decompressed

Stealth virus hides its footprints and the changes it has made

Polymorphic virus makes copies and then changes those copies in some way – uses a mutation engine

Multipartite virus = infects both boot sector and file system

Self-garbling virus modifies own code to elude detection

More Malware: Spyware

Spyware is software or hardware installed on a computer which gathers information about that user for later retrieval by whoever controls the spyware. This software is installed without the user's knowledge.

Spyware can be broken down into two different categories, surveillance spyware and advertising spyware. Surveillance software includes key loggers, screen capture devices and Trojans.

Large companies often use surveillance software to monitor employee computer usage.

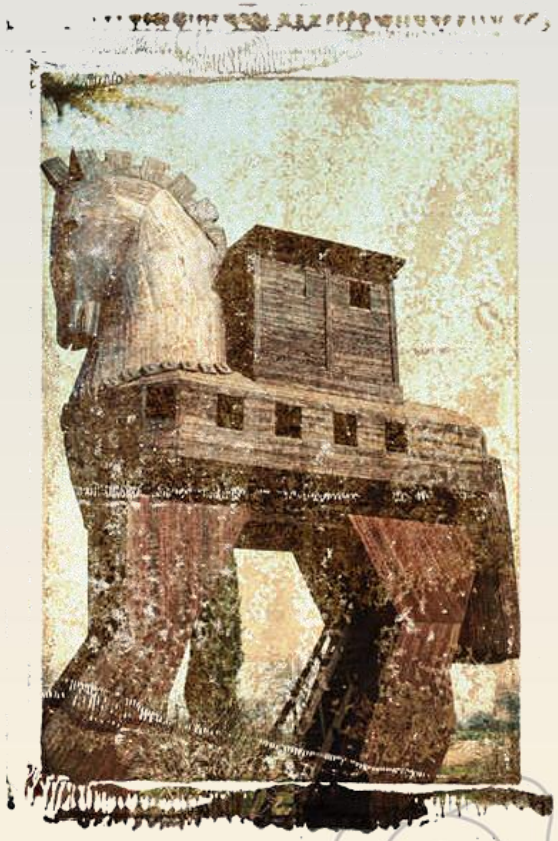
Trojan Horses

A Trojan Horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from the a Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering.

But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.



Back Doors

Back Doors

- Accessing a system by bypassing the access controls
- Allows attacker to enter the computer at any time
- Can be inserted by a Trojan horse
- Maintenance hook
  - Instructions in software that allow for easy access and maintenance
  - Allows entry to code at specific points without security checks
  - Usually accessed through a certain key sequence
  - Should be removed before deployment of software

DoS

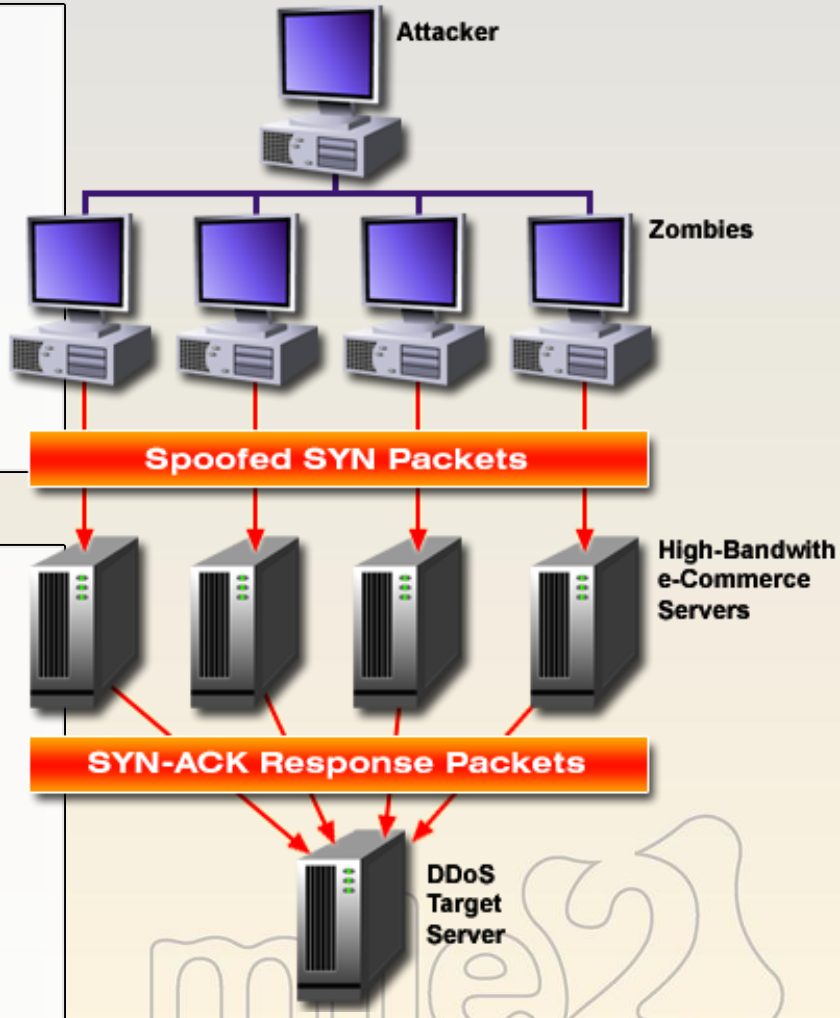
DDoS Issues

Denial-of-Service

- Tying up resources on a computer so it cannot respond to valid requests
- Can be distributed and amplified by using other systems to commit the attack – distributed denial-of-service (DDoS)

Distributed Denial-of-Service

- Masters and zombies
- Ingress filtering
  - Does not allow packets in with internal source addresses
- Egress filtering
  - Does not allow packets to leave with external source addresses



Stachledraht DDoS Attack

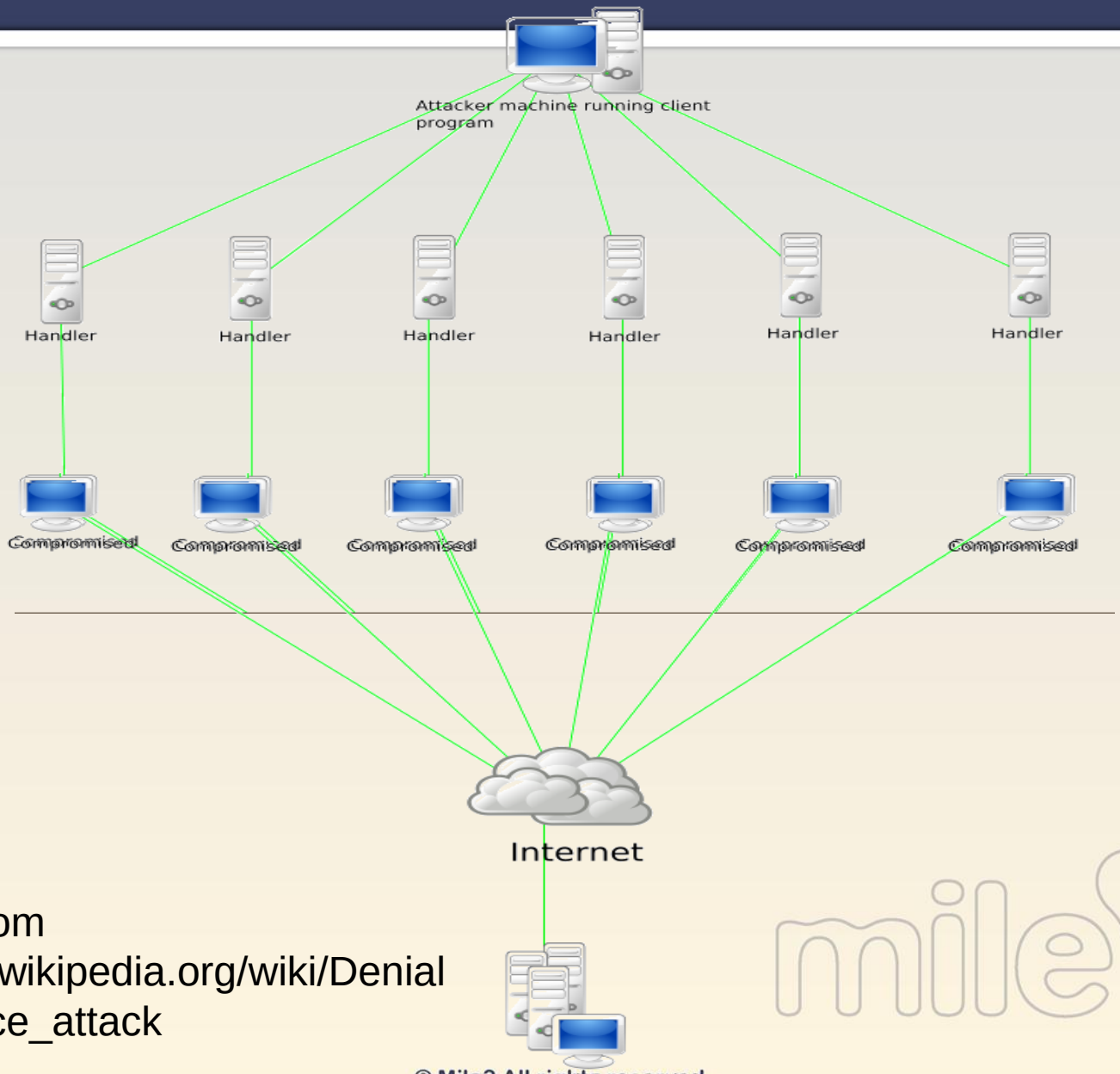


Image from http://en.wikipedia.org/wiki/Denial-of-service_attack

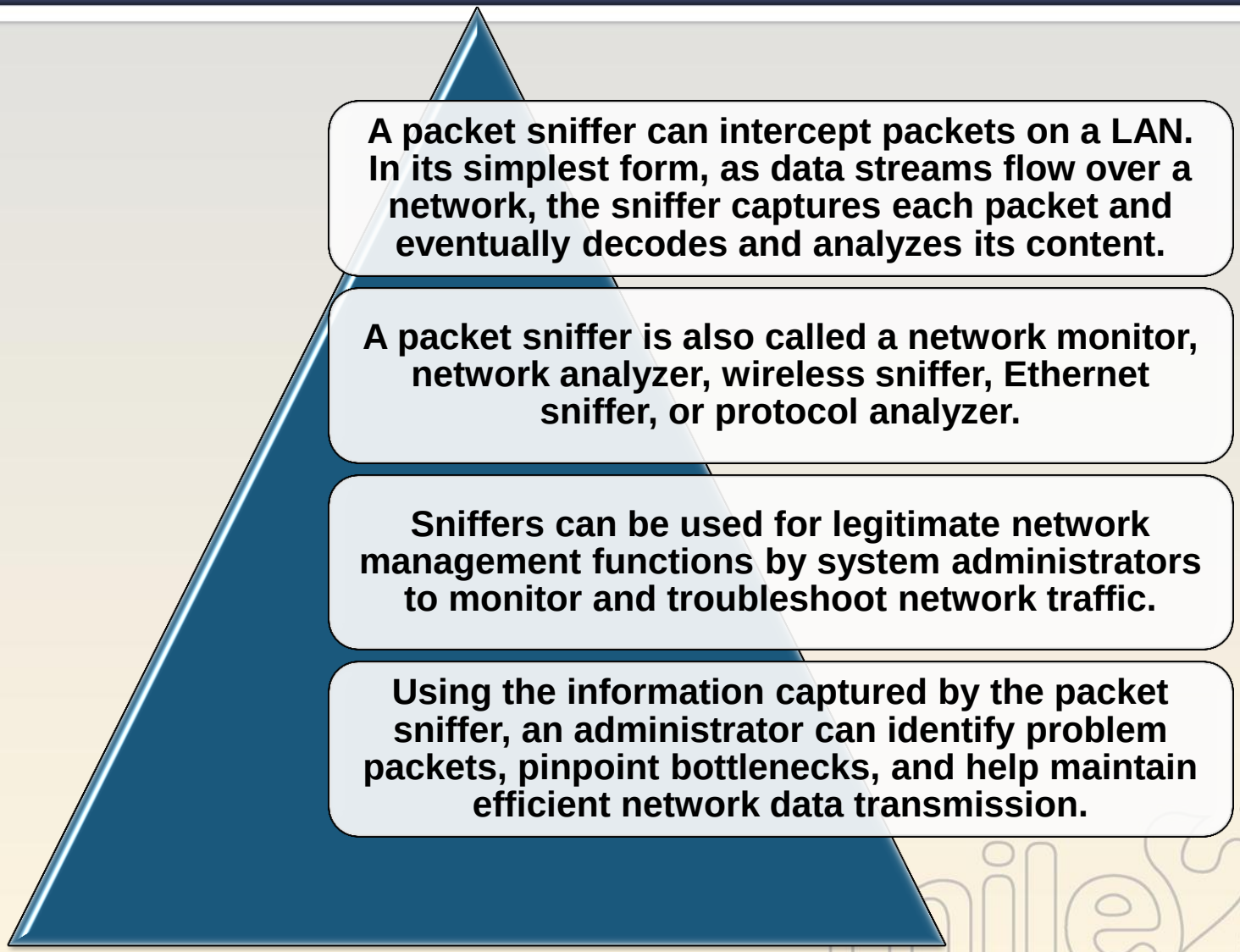
DDoS

DDoS Issues

- First automated tool releases in 1999 with the University of Minnesota as the victim
- Many high-profile attacks in 2000
- In 1999, a fake Internet Explorer update was posted, which contained a Trojan horse that attacked the Bulgarian Telecommunications Company
- Computers using DSL and cable modems are typically used because they are always connected to the Internet and have a static IP address
- Not always malicious
  - After the TV special *Who Wants to Marry a Multimillionaire* in 2000, the network's website was brought down by people seeking the results of the competition

Network Devices and Sniffers

Packet Sniffers



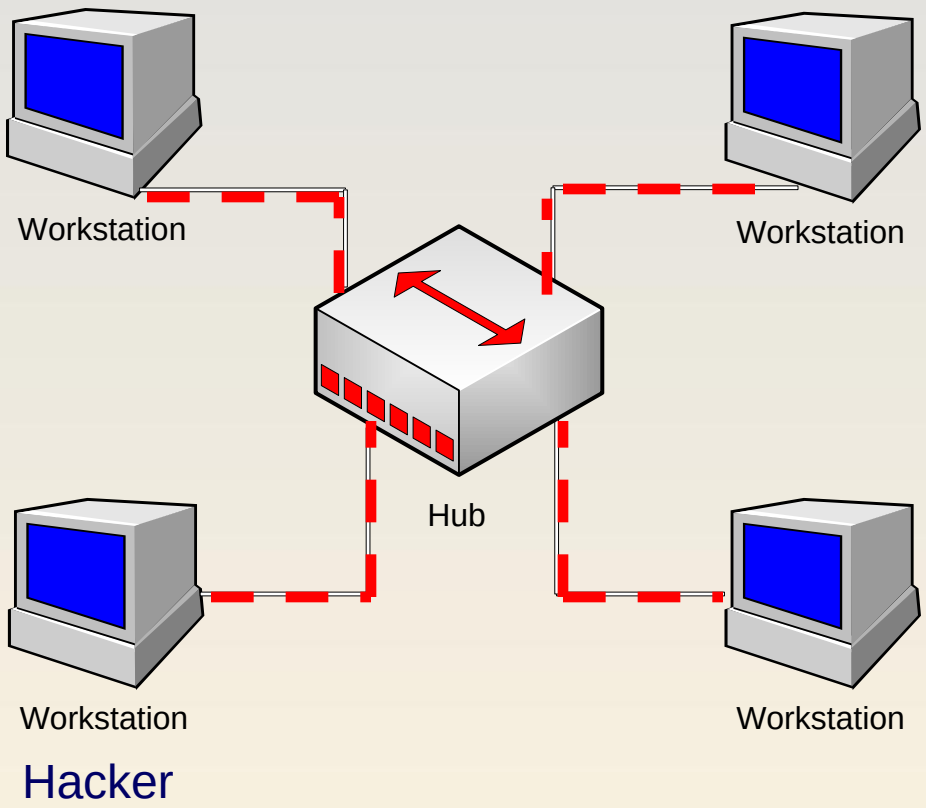
A packet sniffer can intercept packets on a LAN. In its simplest form, as data streams flow over a network, the sniffer captures each packet and eventually decodes and analyzes its content.

A packet sniffer is also called a network monitor, network analyzer, wireless sniffer, Ethernet sniffer, or protocol analyzer.

Sniffers can be used for legitimate network management functions by system administrators to monitor and troubleshoot network traffic.

Using the information captured by the packet sniffer, an administrator can identify problem packets, pinpoint bottlenecks, and help maintain efficient network data transmission.

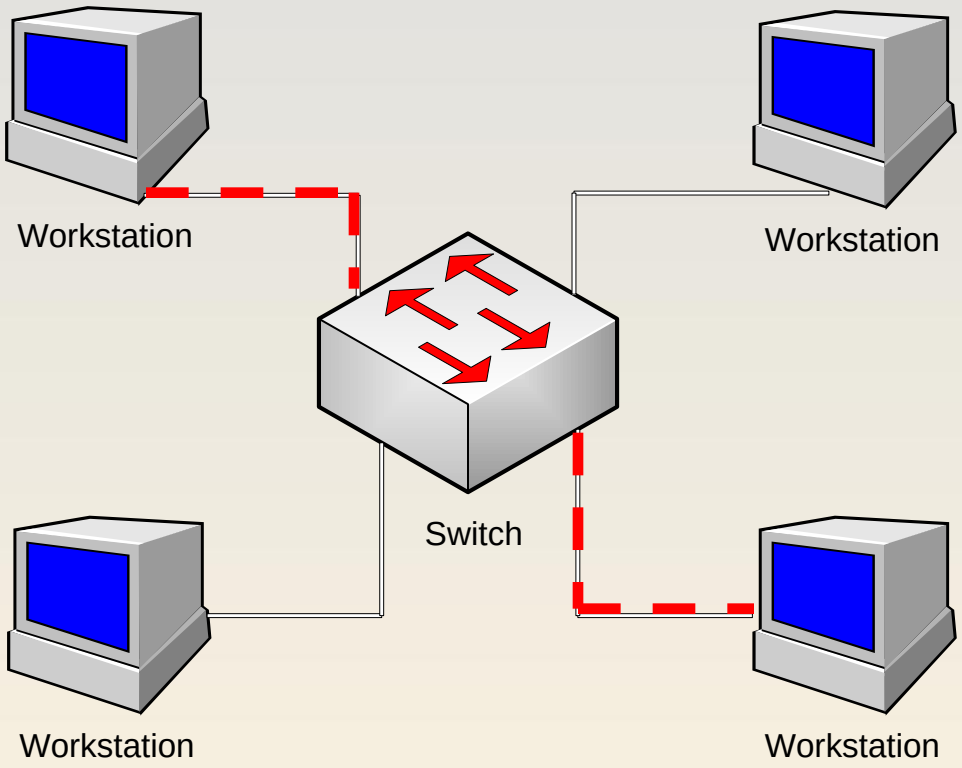
Passive Sniffing



Passive sniffing is sniffing traffic through a hub without having to inject packets.

Passive sniffing is basically hooking up to a hub and starting your sniffer.

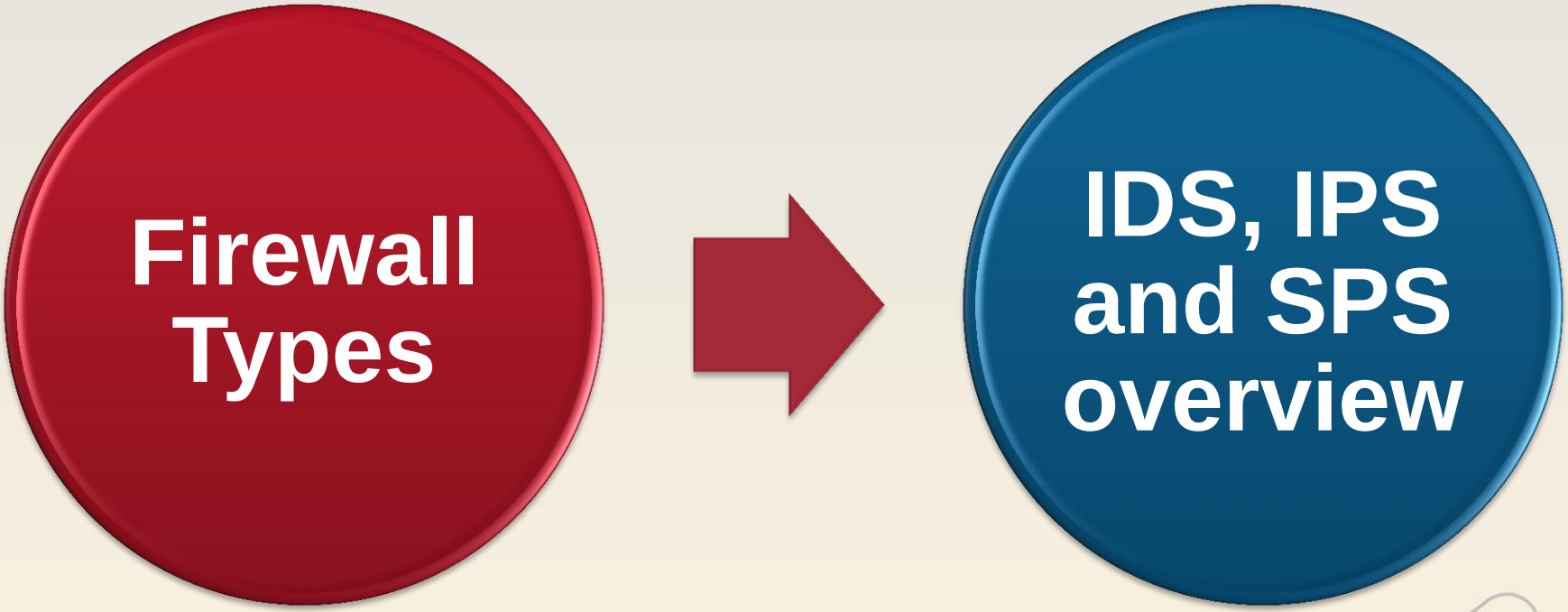
Active Sniffing



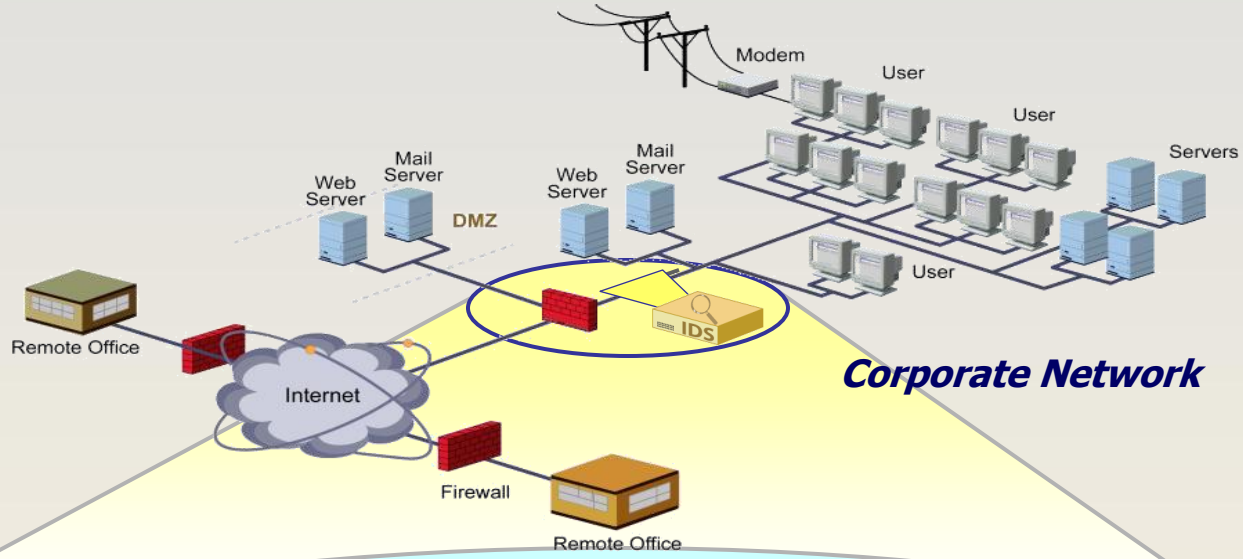
Active sniffing is sniffing traffic on the local LAN, but in order to do that, packets must be injected that cause data to be rerouted to the sniffing machine.

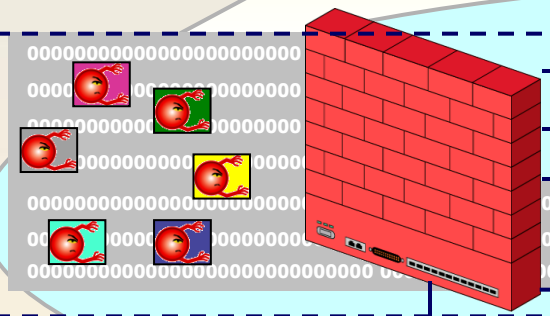
Active sniffing occurs on LANs that have switches connecting the computers.

Firewalls, IDS and IPS



Firewall – First line of defense





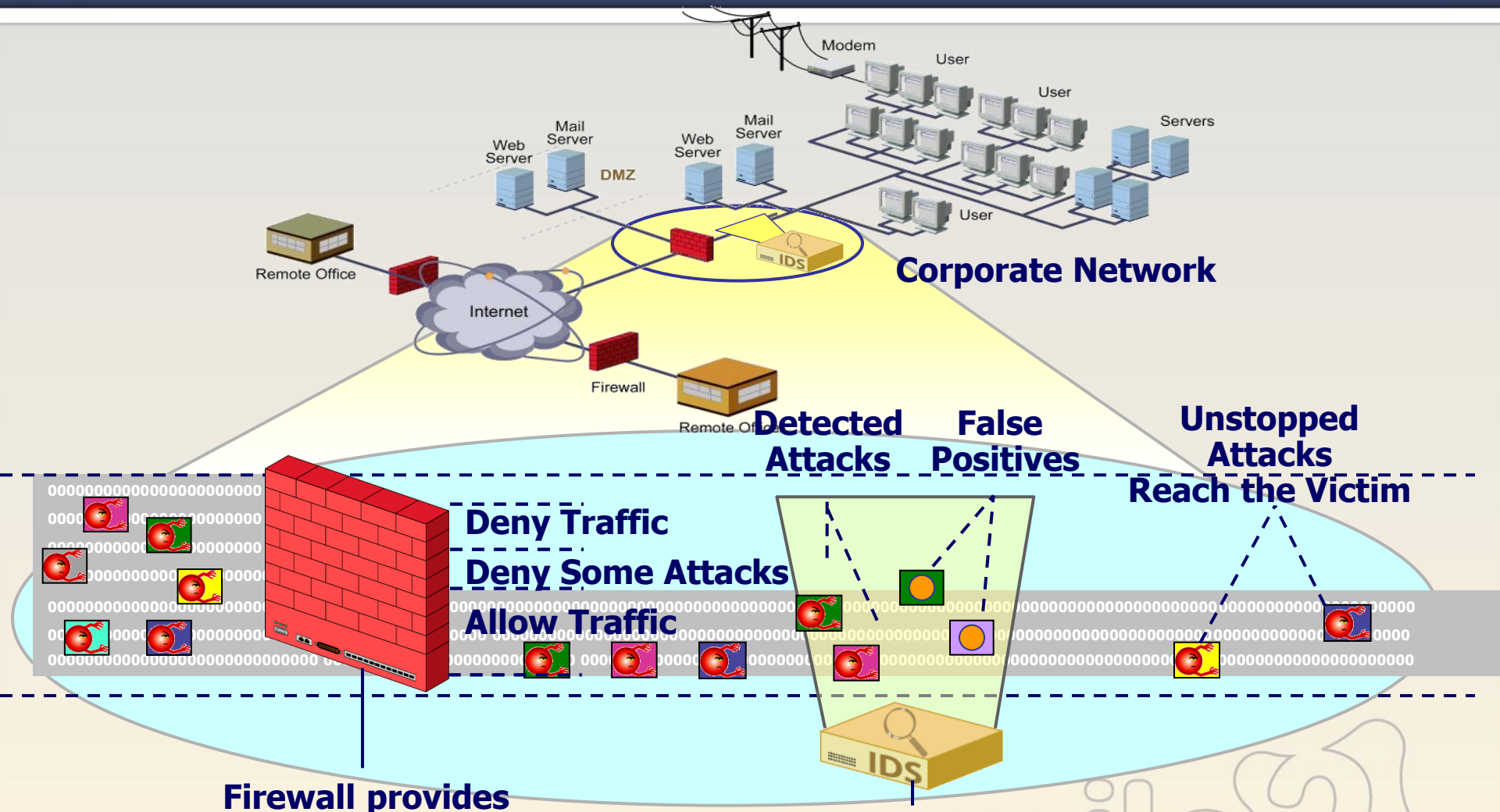
Deny Traffic

Deny Some Attacks

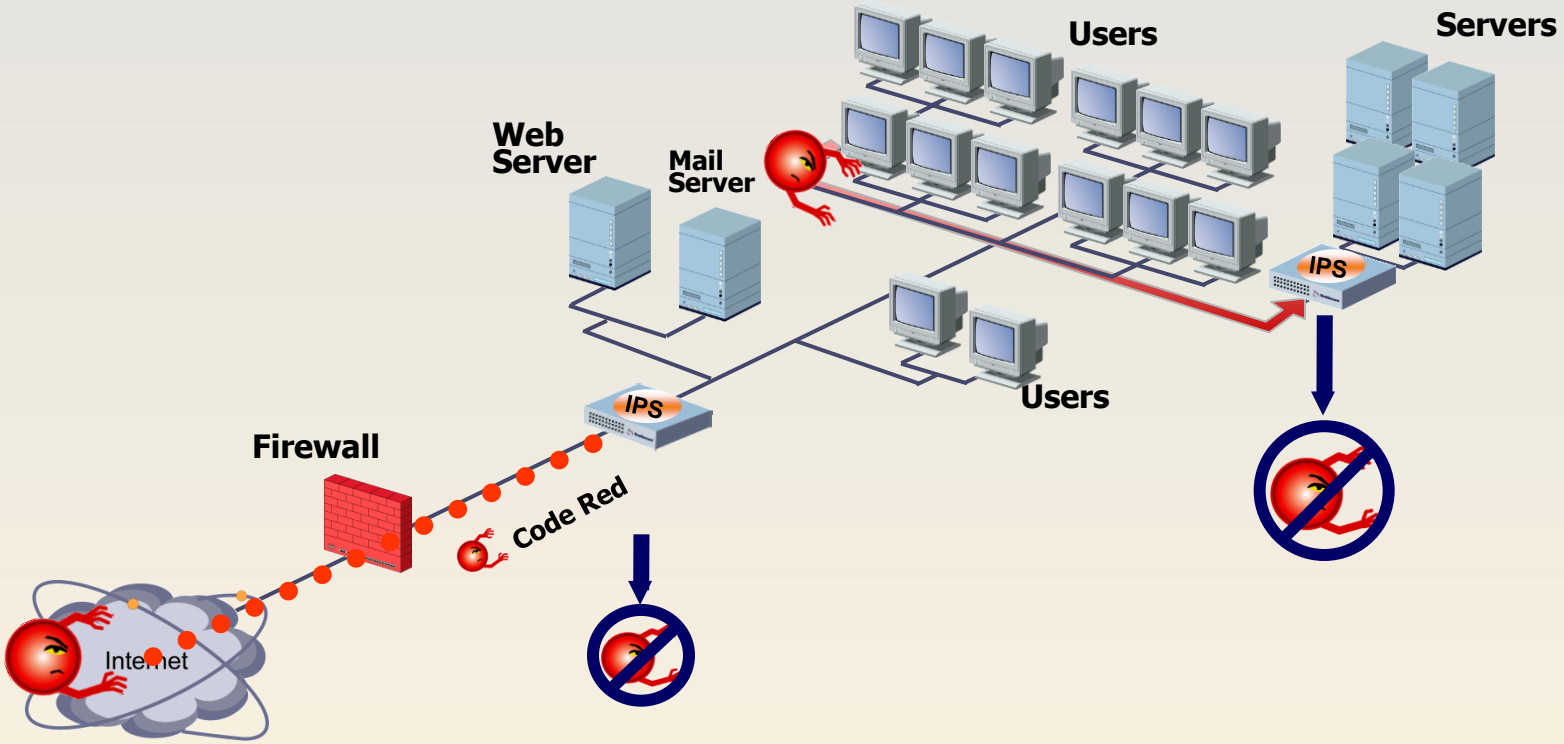
Allow Traffic

Firewall provides access control

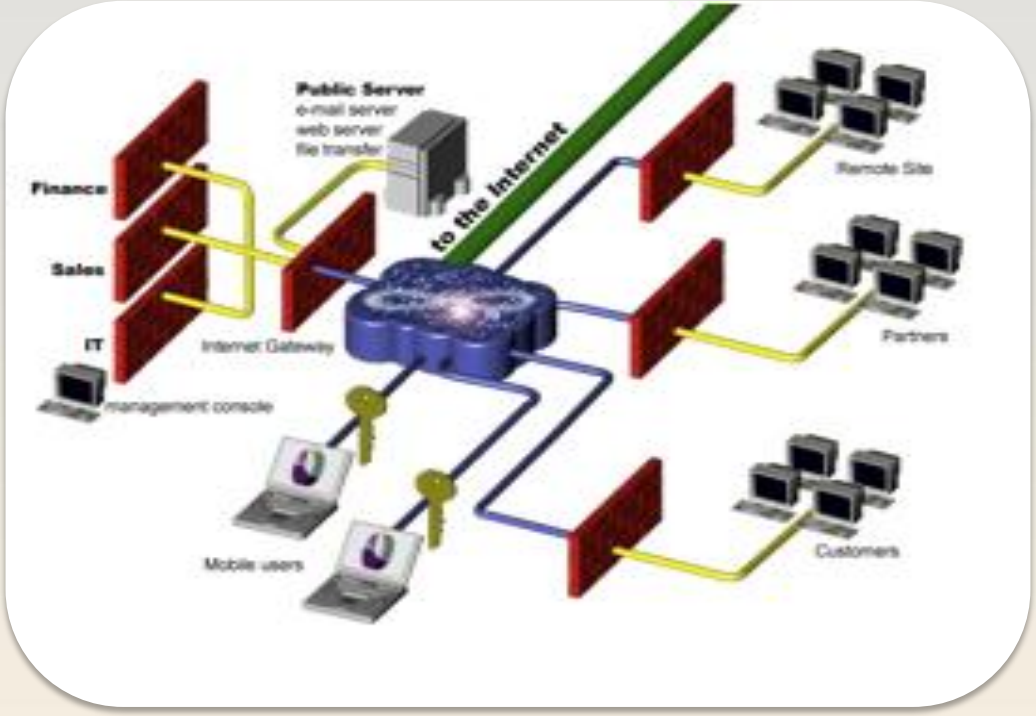
IDS – Second line of defense



IPS – Last line of defense?



Firewalls



Firewall Characteristics

- Many types on the market today
  - Different functionalities and protection levels
- Provides transparent protection to internal users

Firewall Types

- Generation 1 = Packet filtering
- Generation 2 = Proxy
- Generation 3 = Stateful
- Generation 4 = Dynamic packet filtering
- Generation 5 = Kernel proxies

Firewall Types: (1) Packet Filtering

Packet Filtering Characteristics

- Simplest and least expensive type of firewall
- Screening routers with a set of ACLs
- Access decisions are based on network and transport layer header information
- Referred to as a Layer 3 device
- Cannot keep state information on connections
- Best in low-risk environments
  - Or should be used in combination with other types of firewalls
- First-generation firewall

Firewall Types: (2) Proxy Firewalls

Proxy Firewall Characteristics

Breaks connections between trusted and untrusted entities

Only the proxy firewall's IP address is exposed to the outside of the network

Acts as a middle man

No direct communication taking place

Firewall converts public address to internal addresses

Firewall Types – Circuit-Level Proxy Firewall

Circuit-Level Proxy Characteristics

- Makes access decisions based on network and transport layer header information
  - Similar to a packet filter
  - But it is a proxy, so it breaks the connection
- Is not application- or protocol-dependent
- Provides more protection than a packet filter, but less than other types of firewalls
- SOCKS is the most often used circuit-level proxy today
- Second-generation firewall

Type of Circuit-Level Proxy – SOCKS

SOCKS Characteristics

All clients must have the necessary software

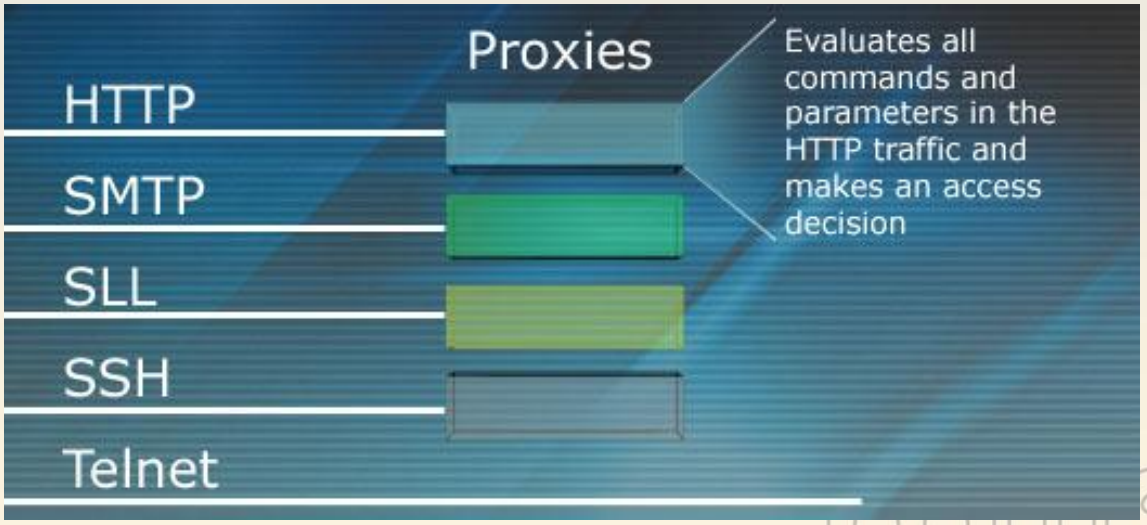
- SOCKS-ified

Mainly used for outbound Internet access

Firewall Types – Application-Layer Proxy

Application-Layer Proxy Characteristics

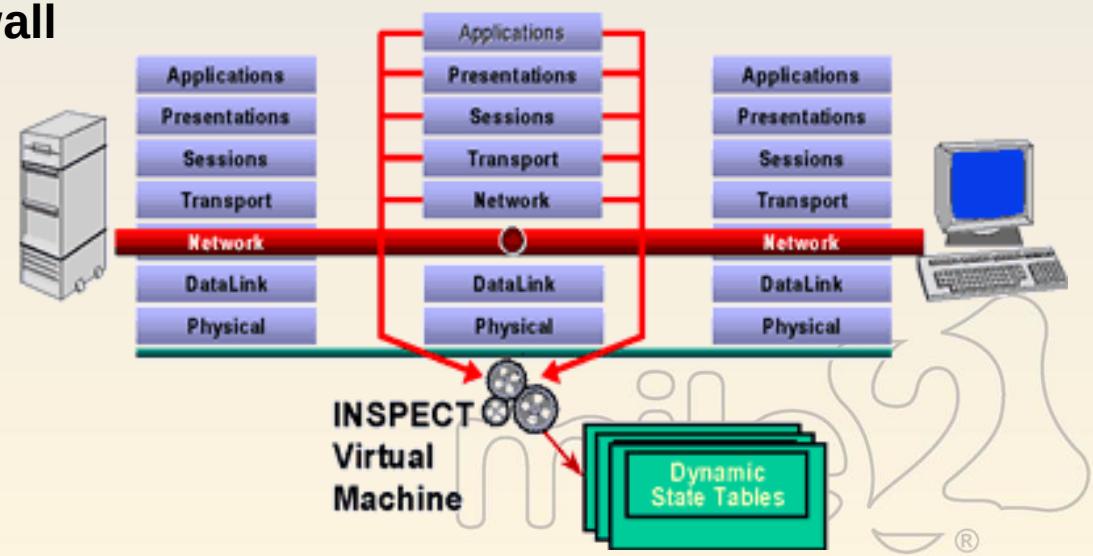
- Access decision is based on data payload information
  - Protocol commands
- Must understand the command structure of protocols
  - One proxy per protocol is required
- Provides a high level of protection
  - Requires a lot of resources
  - Performance issues



Firewall Types: (3) Stateful

Stateful Firewall Characteristics

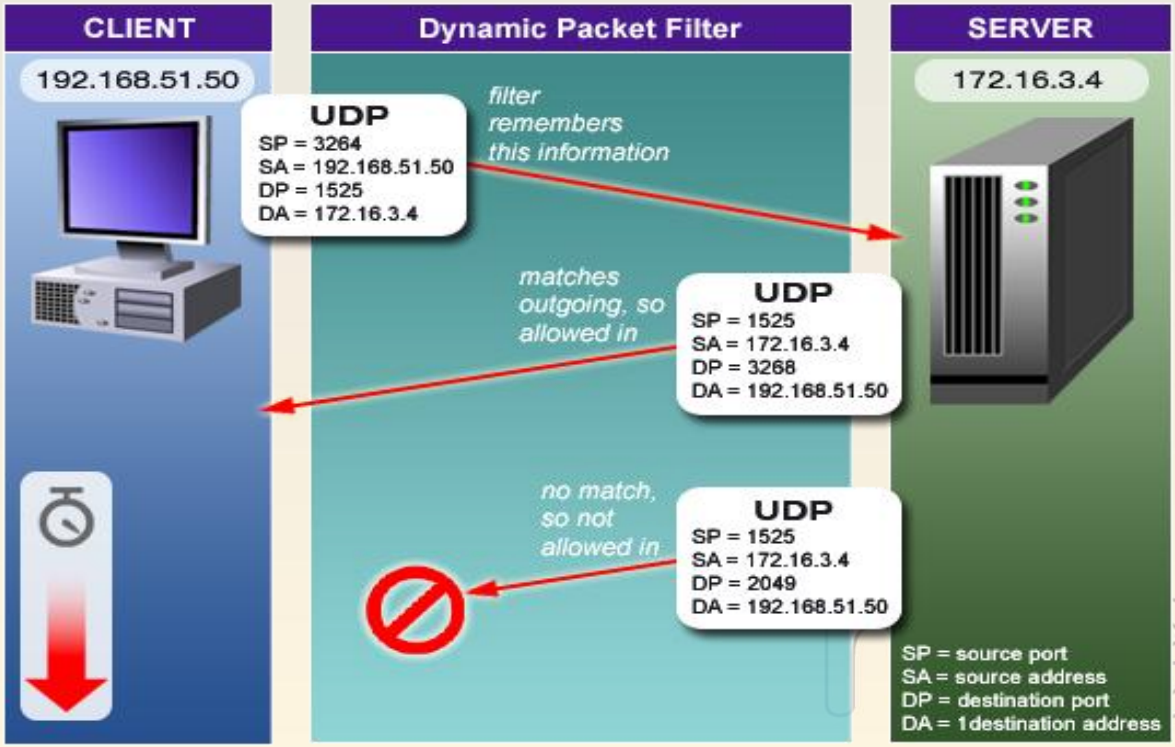
- Makes access decisions based on the following information:
  - IP addresses
  - Protocol commands
  - Historical comparisons with previously sent packets
  - The condition and content of packets
- Uses a state engine and creates and maintains a state table
- Can monitor connection-oriented and connectionless protocols
- Third-generation firewall



Firewall Types: (4) Dynamic Packet-Filtering

Dynamic Packet-Filtering Characteristics

- Combination of application proxies and stateful inspection firewalls
- Dynamically changes filtering rules based on several different factors
  - Reactive to predesigned changes and situations
- Fourth-generation firewall



Firewall Types: (5) Kernel Proxies

Kernel Proxy Characteristics

- Firewall software runs in the kernel (protected ring) of a system
- Direct integration with operating system
- Faster than application-level proxy since processing is taking place at the core of the operating system
- Fifth-generation firewall

Firewall Placement

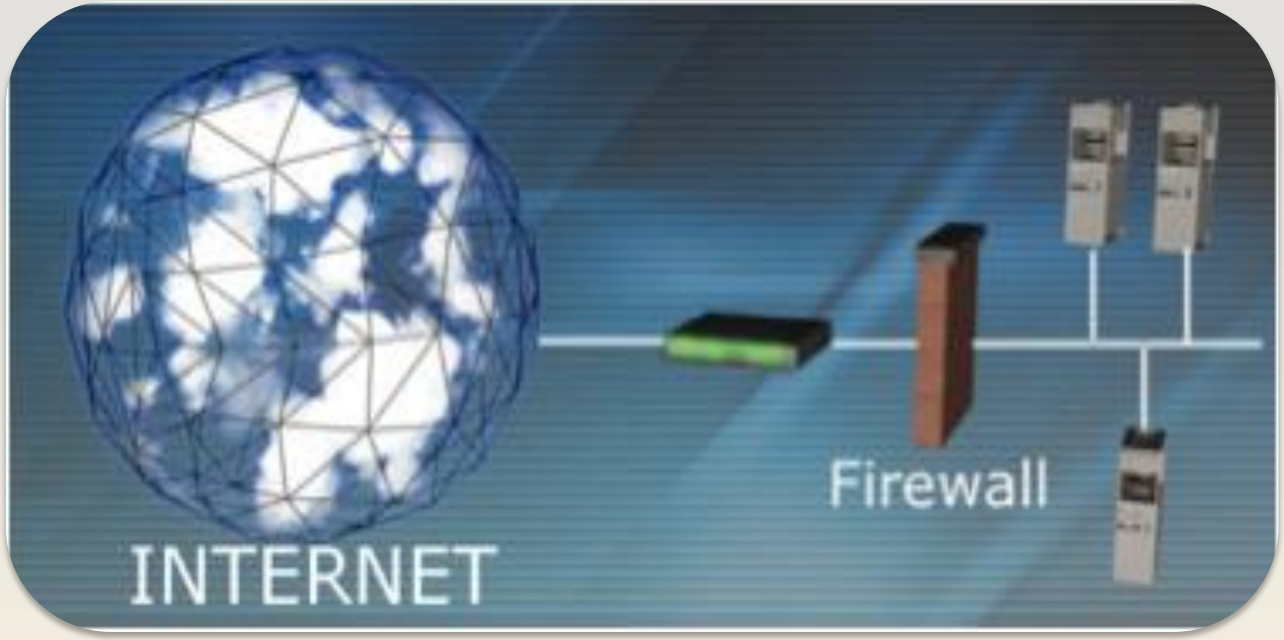
Considerations

- Segments internal network subnets and sections to enforce the security policy
- Acts as a choke point between trusted and untrusted entities
- Creates a DMZ where specific systems need to reside

Types of Architectures

- Screened host
- Multi- or dual-homed firewall
- Screened subnet

Firewall Architecture Types – Screened Host



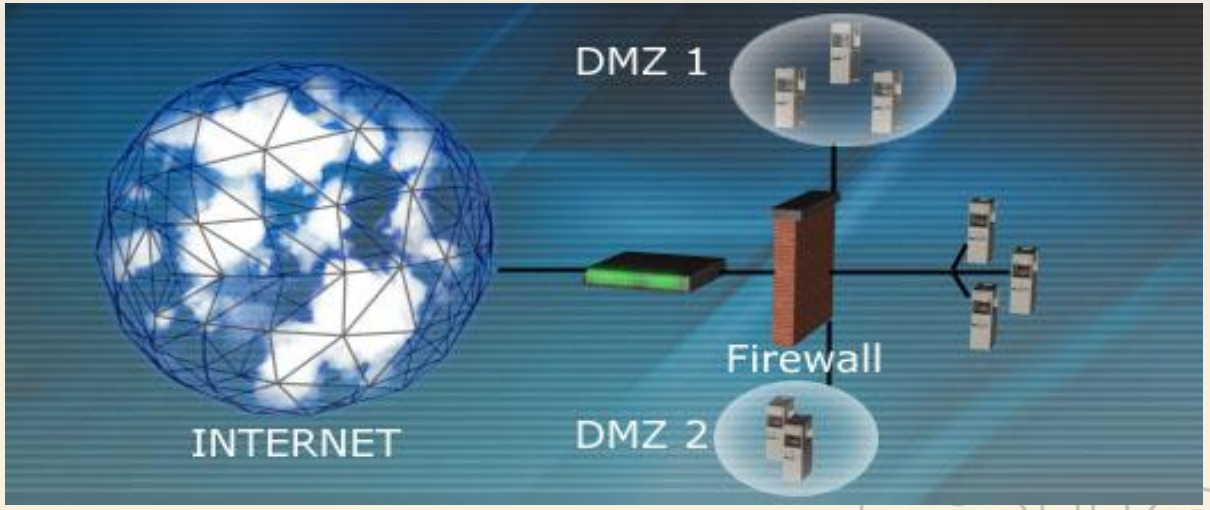
Screened Host Characteristics

- The usual configuration is a router filtering for a firewall
  - Reduces the amount of traffic the firewall (screened host) has to work with
- Screening device = filtering router
- Screened host = firewall

Multi- or Dual-Homed

Characteristics

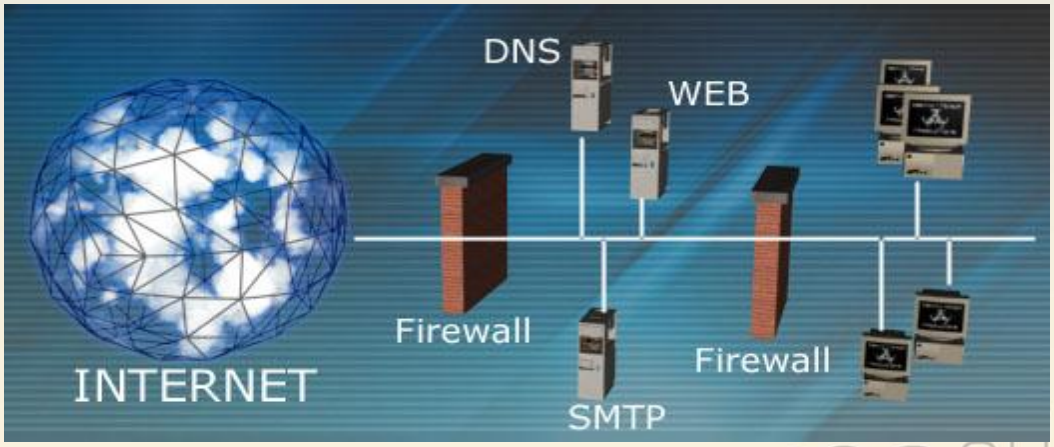
- Two or more interfaces, one for each network
- Allows for one firewall to create more than one DMZ
- Forwarding and routing need to be turned off
  - Otherwise, packets would not be inspected by firewall software



Screened Subnet

Characteristics

- A buffer zone is created by implementing two routers or two firewalls
  - Creation of a single DMZ
- Provides the most protection out of the three architectures
  - Three devices must be compromised before attacker can get into the internal network



Wireless Standards

Wi-Fi Network Types

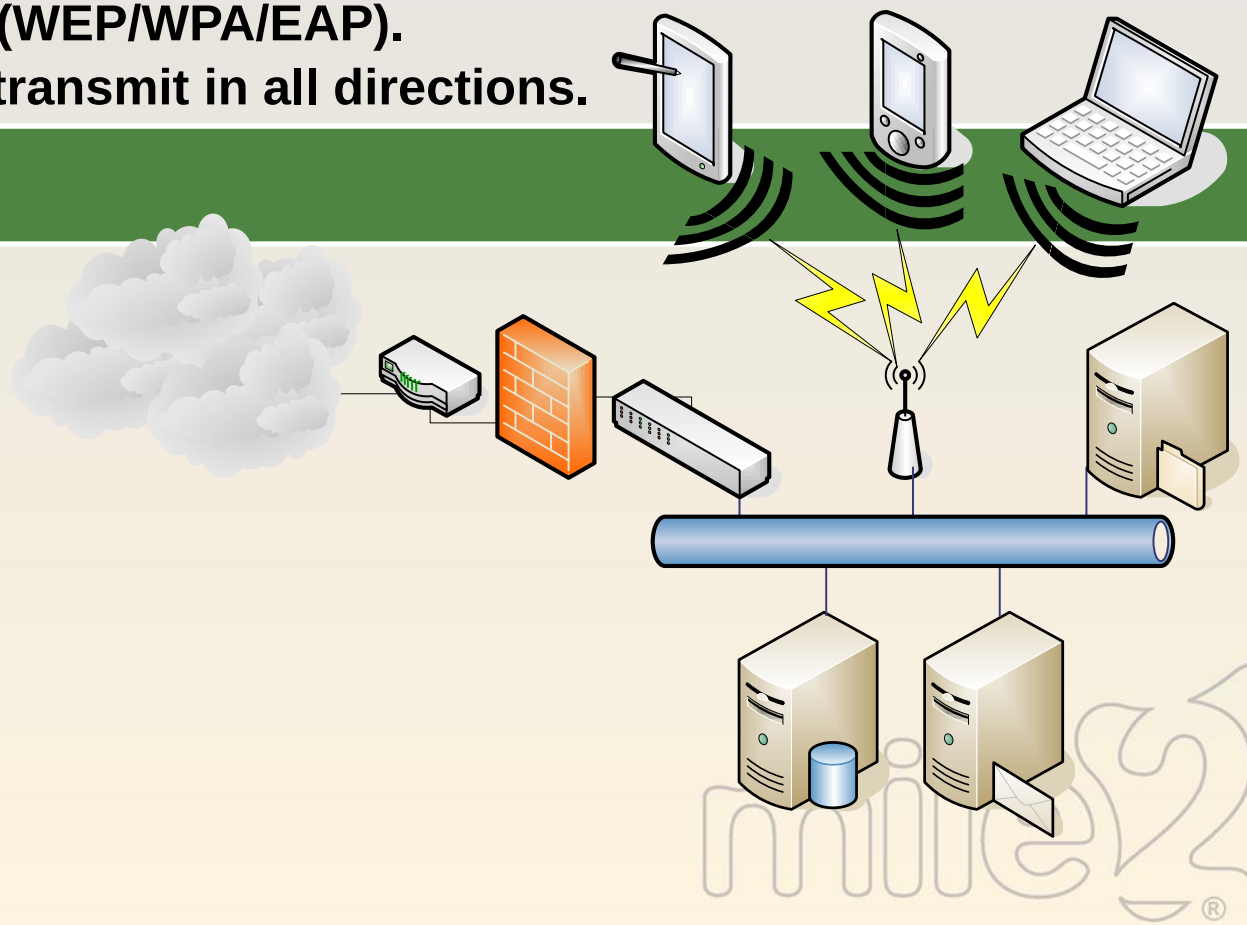
Peer-to-Peer/Ad-Hoc network.

- No central point of communications.
- No central management interface.
- All devices transmit to all devices.
- Easy to setup.

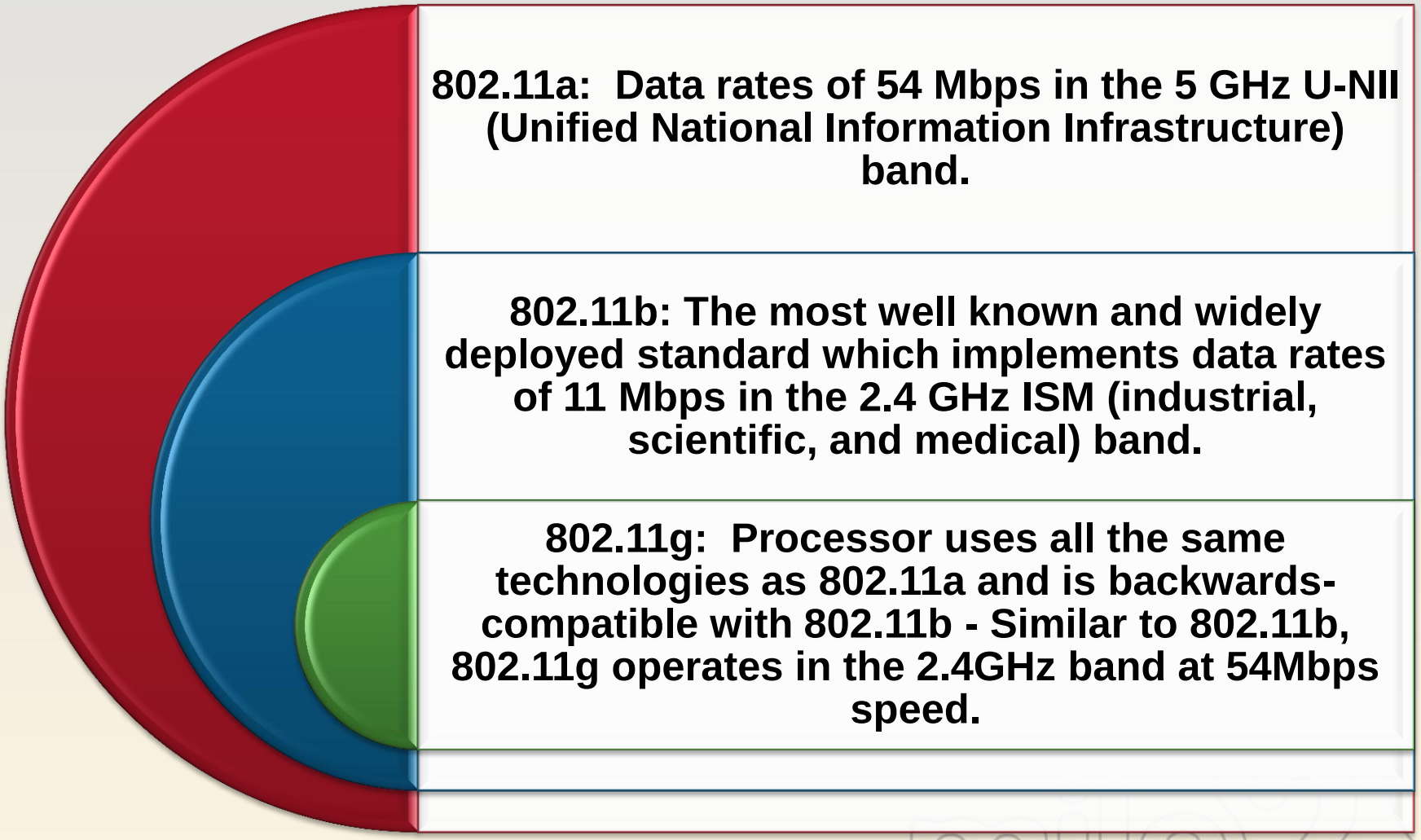
Wi-Fi Network Types

Infrastructure Mode.

- Central point of configuration/management.
- More secure (WEP/WPA/EAP).
- Devices still transmit in all directions.



Widely Deployed Standards



802.11a: Data rates of 54 Mbps in the 5 GHz U-NII (Unified National Information Infrastructure) band.

802.11b: The most well known and widely deployed standard which implements data rates of 11 Mbps in the 2.4 GHz ISM (industrial, scientific, and medical) band.

802.11g: Processor uses all the same technologies as 802.11a and is backwards-compatible with 802.11b - Similar to 802.11b, 802.11g operates in the 2.4GHz band at 54Mbps speed.

Standards Comparison

820.11 Protocol	Release	Freq. (GHz)	Thru. (Mbit/s)	Data (Mbit/s)	Mod.	Radius In – (m)	Radius Out – (m)
-	1997	2.4	0.9	2		~20	~100
a	1999	5	23	54	OFDM	~35	~120
b	1999	2.4	4.3	11	DSSS	~38	~140
g	2003	2.4	19	54	OFDM	~38	~140
n	2009	2.4, 5	74	248	OFDM	~70	~250
y	2008	3.7	23	54		~50	~5000

802.11n - MIMO

MIMO **stands for multiple-input | multiple-output; the use of multiple antennas to increase throughput and/or reduce bit error rates.**

MIMO can be split into 3 categories:

- **Pre-coding – Used to increase the signal gain.**
  Spatial Multiplexing – This technique is used for increasing channel capacity at higher Signal to Noise Ratio (SNR).
  Diversity Coding – Used to enhance signal diversity.

Advantages of 802.11n:

- **More Coverage Area**
- **Higher throughput speeds**
- **With MIMO, even your existing 802.11b and 802.11g clients will get a boost in range of up to 20% if you are using compatibility mode.**

Database Basics

Overview of Database Server

Database

- A collection of information or data that is stored in a computer system usually organized by files, records, and fields.

DBMS(Database Management System)

- A database management system (DBMS) is a collection of programs designed to let you enter, organize and select data in the database.
- There are different types of databases: relational, network, flat, and hierarchal all refer to the way a DBMS organizes information internally.

Types of databases

- Introduced by the team lead by Dr. Edmund F. Codd
- Based on the principles of relational algebra
- Used by a majority of the Fortune 500 companies
- Oracle, SQL Server, Sybase, Informix, Ingress, Gupta SQL, DB2, Microsoft Access
- The most likely database you will encounter

Relational DBMS or RDBMS

Overview of Database Server

Tables

- A collection of data or data structures linked through relations, tables are constructed of columns and rows.

Record set

- A record set is the requested data, a subset of the entire row.

Attributes

- The data type a field can contain. Currency, Date, Characters etc.

Domain

- A set of allowable values that an attribute can take, i.e. currency field can allow $, ¥, £ etc.

These are important concepts to understand as they play a large part in testing database systems.

Overview of Database Server

Data Normalization

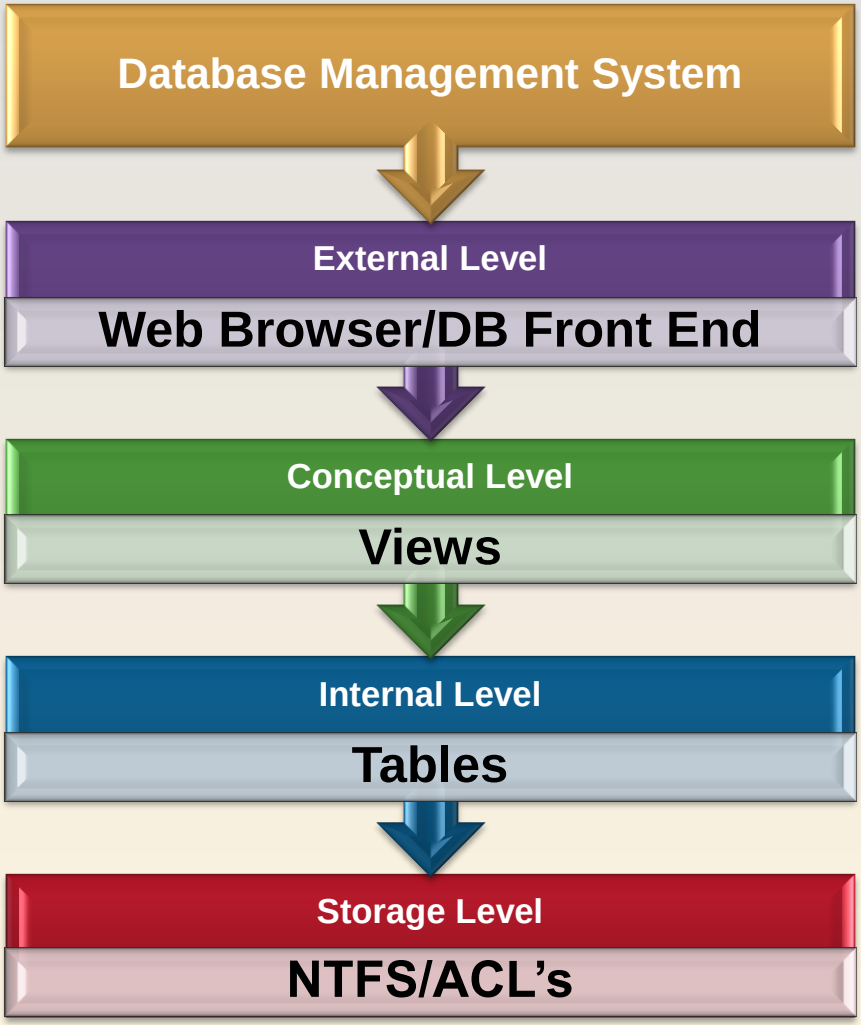
- A process that database designers go through to eliminate redundant data, repeating groups and attributes.
- This makes the database more efficient.

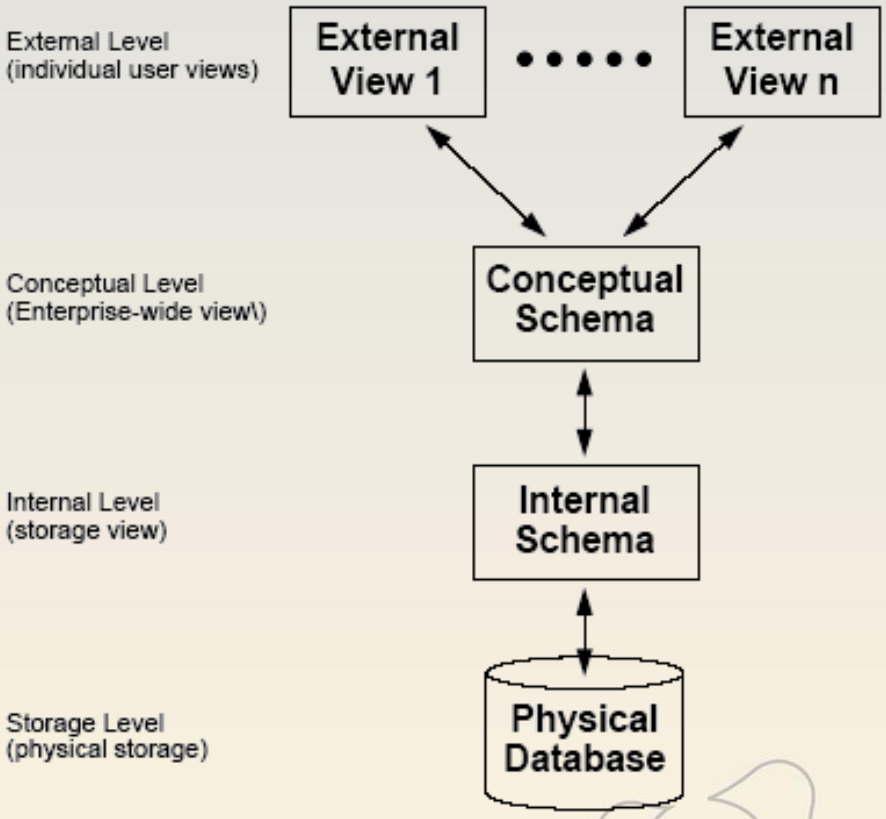
SQL (Structured Query Language)

- Data manipulation and relational database definition language.
- All SQL database systems use a core structure of SQL, vendors then have a subset proprietary to their own server, i.e. MS-SQL server uses Transact-SQL, Oracle uses PL-SQL
- Common commands are SELECT, UPDATE, DELETE, INSERT, Grant, Revoke, OR, HAVING etc.

It is critical to the successful penetration of a database system for the tester to have a good knowledge of the core structure of SQL.

Overview of Database Server





Review