CYBER SECURITY

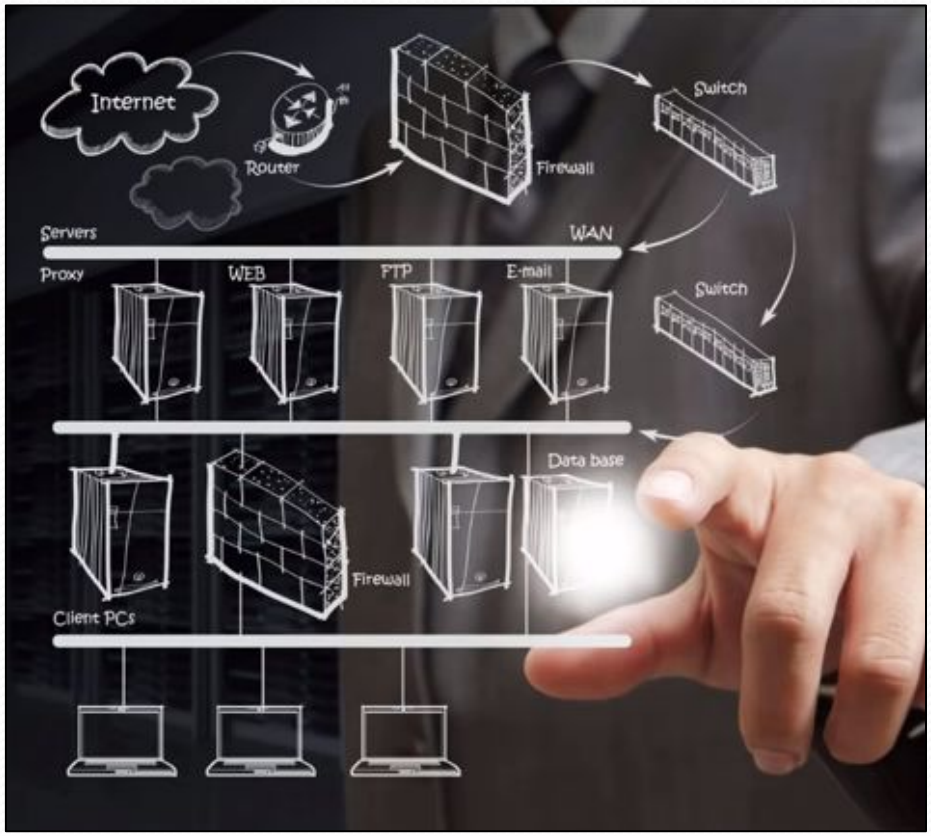
PRESENTED BY: Mazhar K

Agenda:

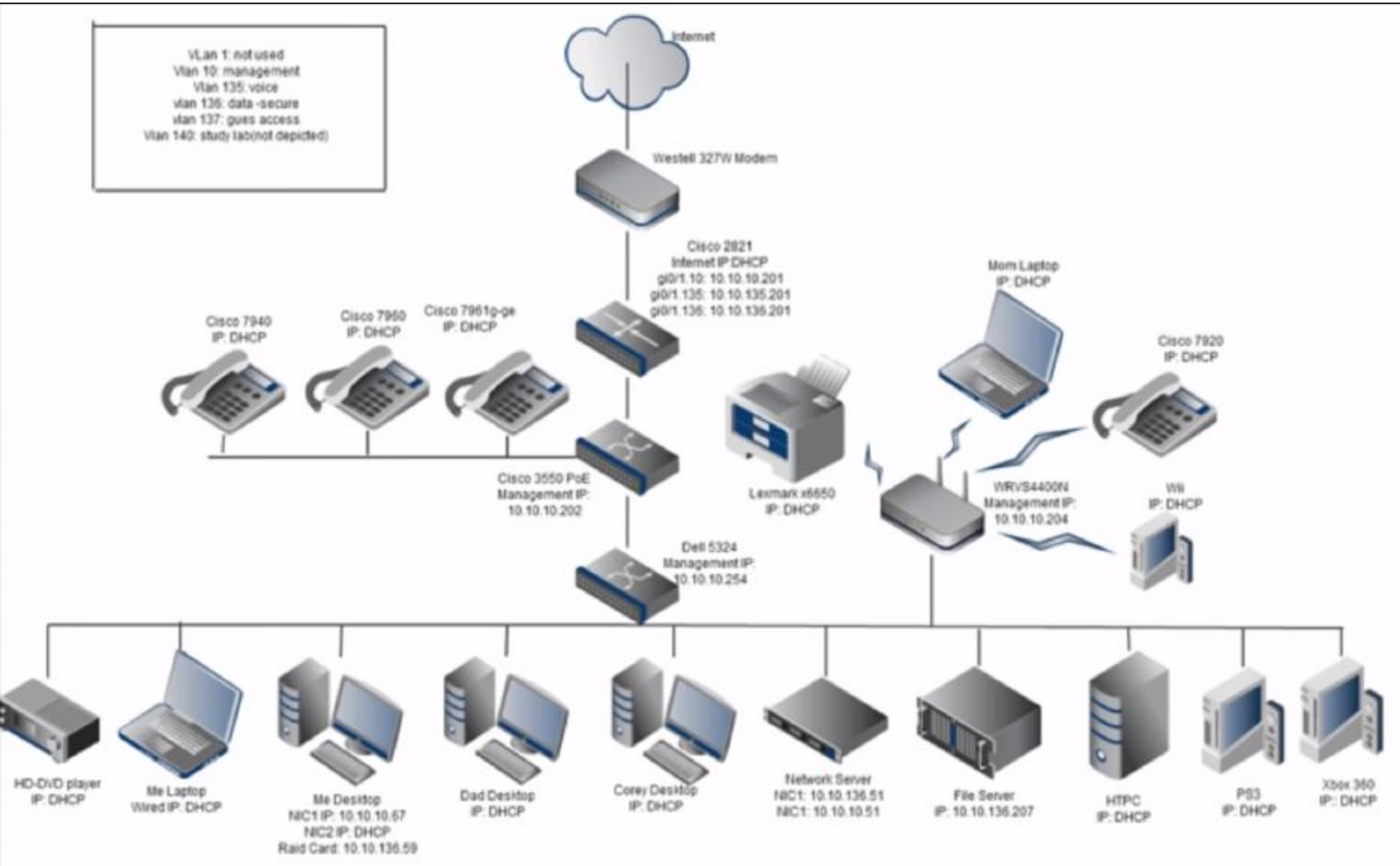
- Introduction to IT Infrastructure
- Origin of “Cyber Security”
- Purpose of Cyber Security
- What is Cyber Security?
- Adversary Types
- Vulnerability Types (Pen Testing)
- Threat Types
- Information Security (Regulatories)
- Tools
- Certifications

IT Infrastructure

- Basic elements of IT Infra
  - Data Centers
  - Servers and Clients
  - Network Devices
- Communication Media
- Types of Data Networks

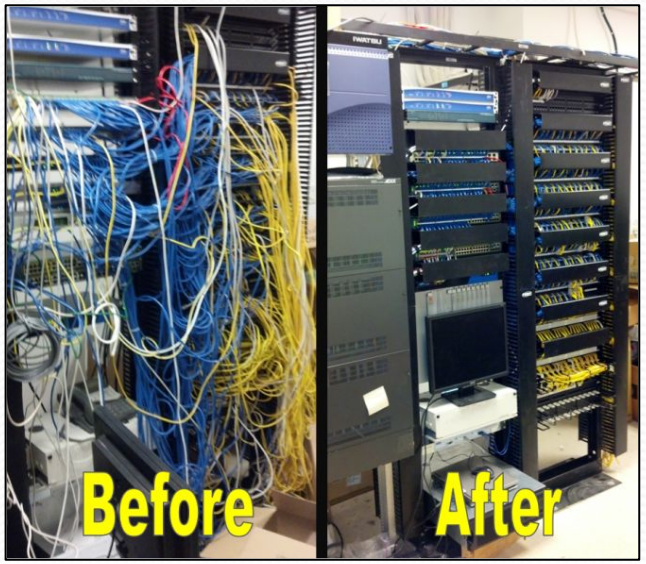


Basic Infrastructure Diagram

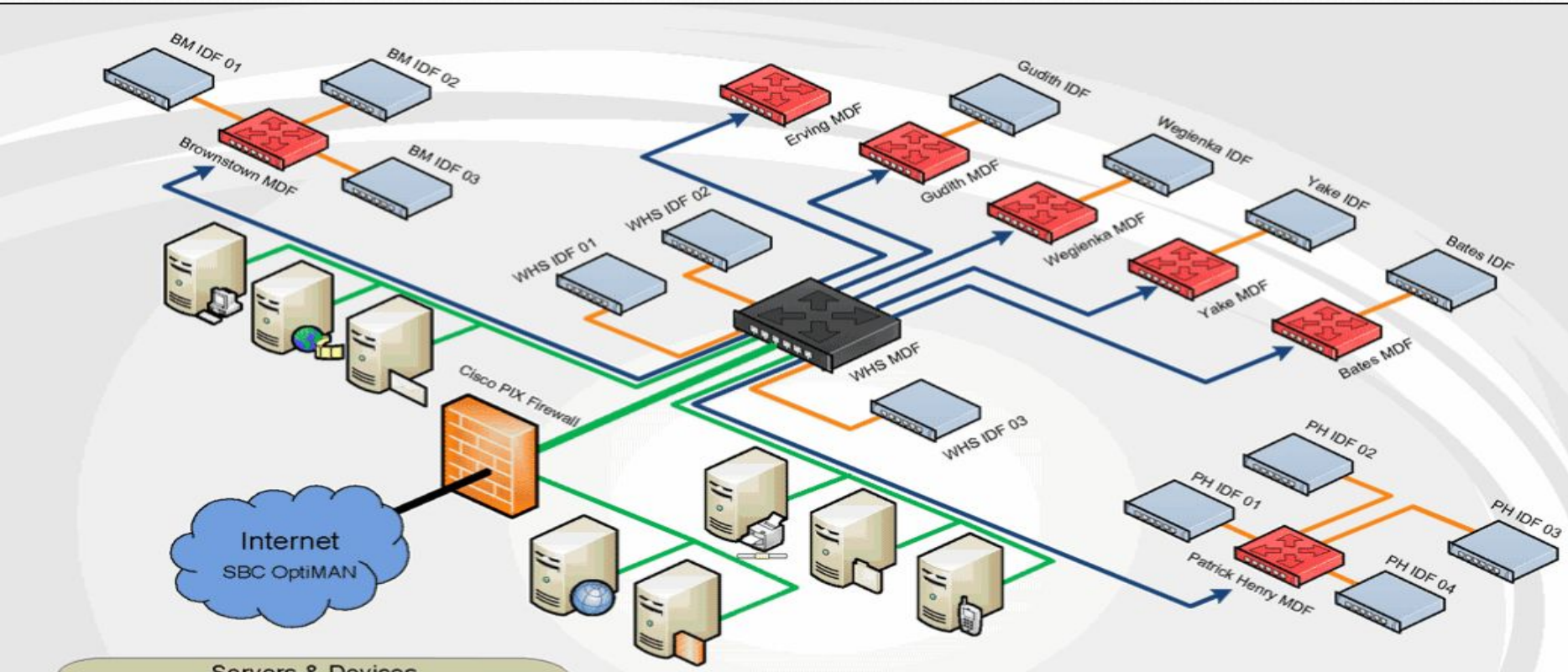


Data Centers

- Physical space - servers and network devices.
- Requires access control, cooling, redundant power supplies, etc.
- Usually organized in “racks”.
- Vary significantly in sizes.



Sample Network Diagram

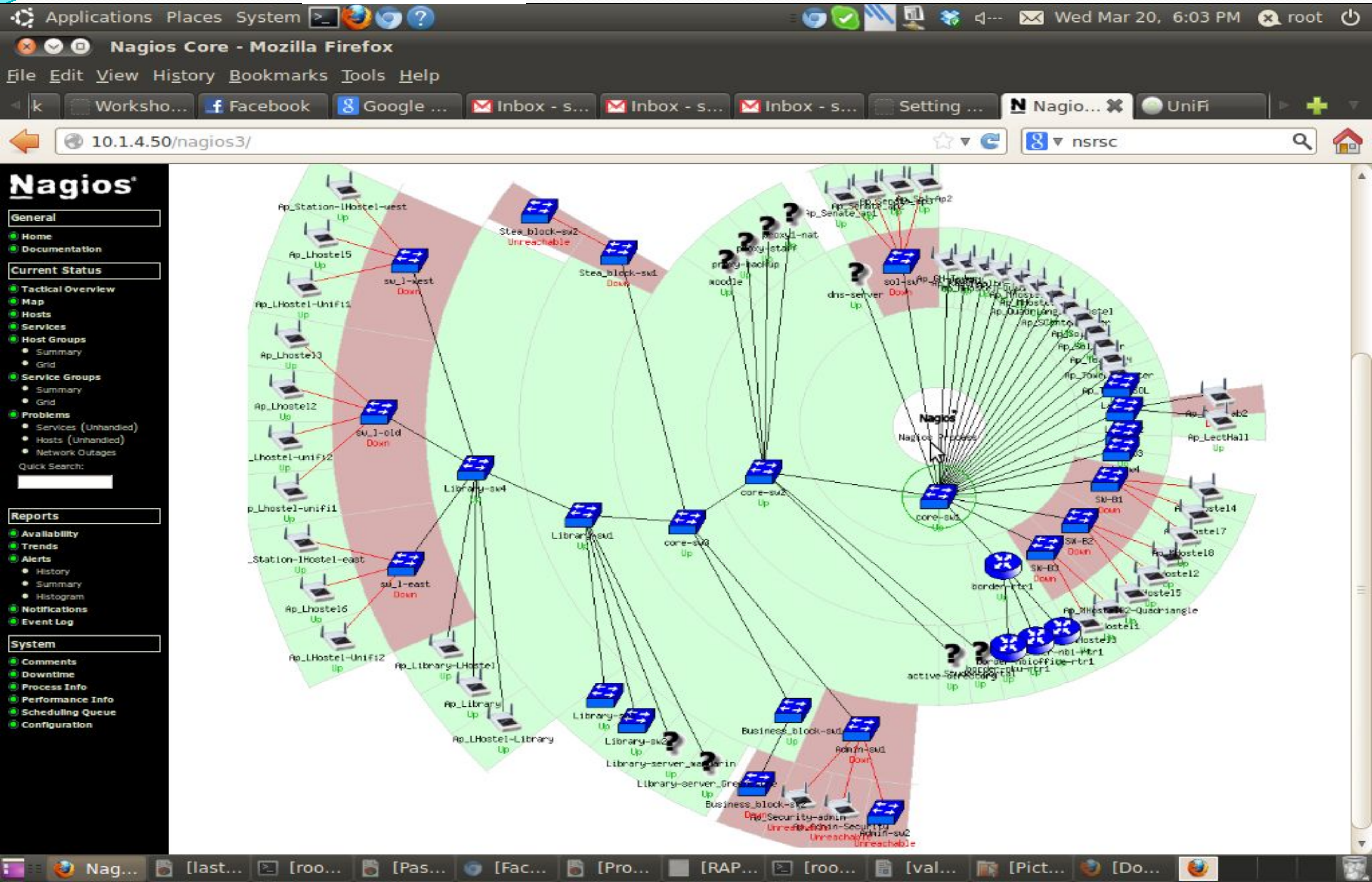


Servers & Devices

Symbol	Cont	Description
	1	GroupWise Email Server
	1	MediaCast Streaming Server
	2	Novell eDirectory / File Servers
	1	Cisco PIX Firewall
	1	Print & Backup Server
	1	Barracuda Spam Appliance
	1	BlackBerry Enterprise Server
	1	8e6 Content Filtering Appliance
	1	Neaxmail / Aimworks Servers

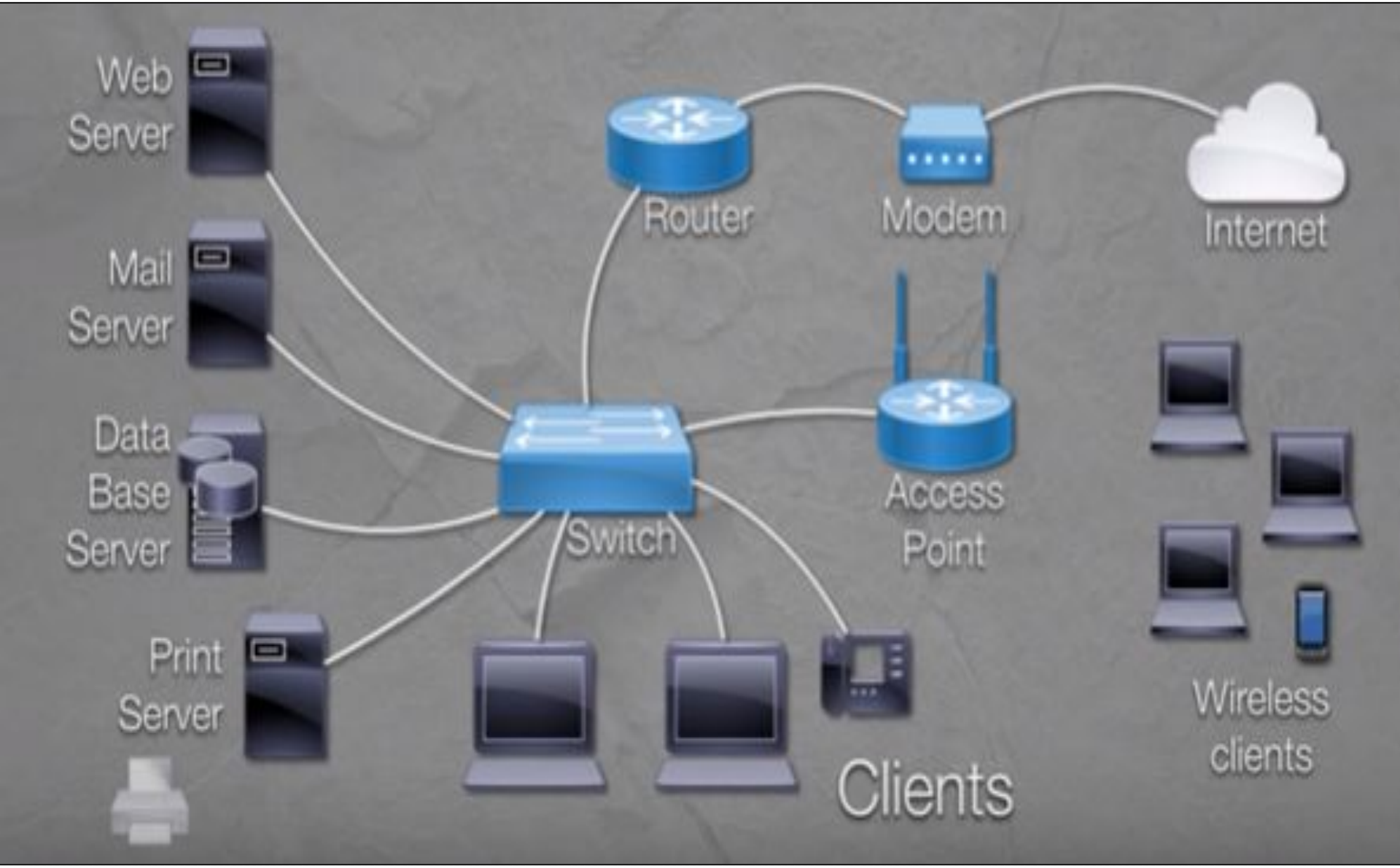
SM Fiber
MM Fiber
100/1000 Eth
DMZ

Nagios®



Applications Places System
Wed Mar 20, 6:03 PM
root
Nagios Core - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Worksho...
Facebook
Google ...
Inbox - s...
Inbox - s...
Inbox - s...
Setting ...
Nagio...
UniFi
10.1.4.50/nagios3/
nsrsc
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Nag...

Elements in a LAN:



Servers

Name based on their function:

- File Server
  - FTP, Samba
- Print Server
- Web Server
  - Apache, Nginx, Microsoft IIS (Internet Info Services)
- Applications Server
  - SAP, any software developed locally
- Mail Server
  - MS Exchange, Zimbra
- Database Server
  - MS SQL, Oracle, MySql, MariaDB
- Media Server
- Collaboration Server
  - MS Sharepoint, IBM Lotus

Servers ...contd

Name based on their platform:

- Generally refers to their hardware and O/S
- Hardware
  - Make and Model
- Operating System
  - MS Windows Server
  - Redhat Linux, UNIX
- For example:
  - IBM P-Series with Linux
  - Dell PowerEdge with Windows
  - “Linux Server”
  - “A Linux”

Types of Servers:

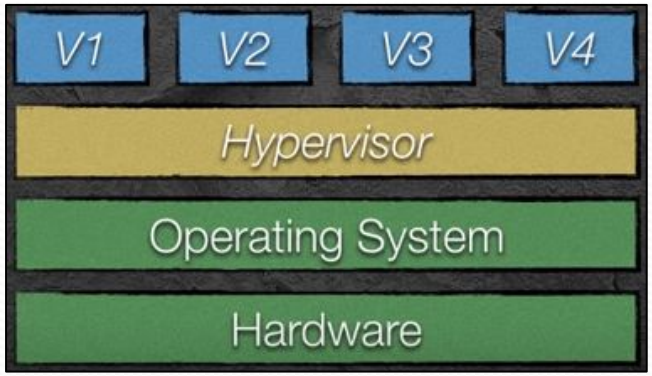
- Mainframe
  - Large multi-functional environment
  - Huge no. of transactions and users
  - $$$$$ Mils
  - Ex: IBM zSeries, System z9 and System z10 servers

- High Availability
  - Powerful PCs with high availability
    - Multiple hard disks (RAID)
    - Redundant power supply
    - Redundant network interfaces (cards)
  - $$$$ Thousands
  - Ex: RAID 0, RAID 1, RAID 5, RAID 6

Types of Servers ...contd

- Cluster
  - Group of servers performing same function
  - Distribute workloads and are highly scalable
  - Organization
    - Primary and slave or secondary
    - Mirror

- Virtual
  - Server within a server
  - Physical server running a *hypervisor* on top of or within which you run multiple servers
    - *Hypervisor* - creates and runs virtual machines
  - Ex: VMware ESXi, Citrix Xen



Clients

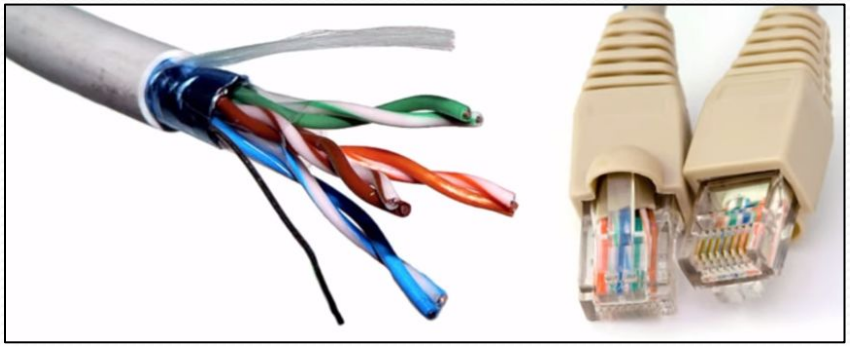
"Devices that access the servers"

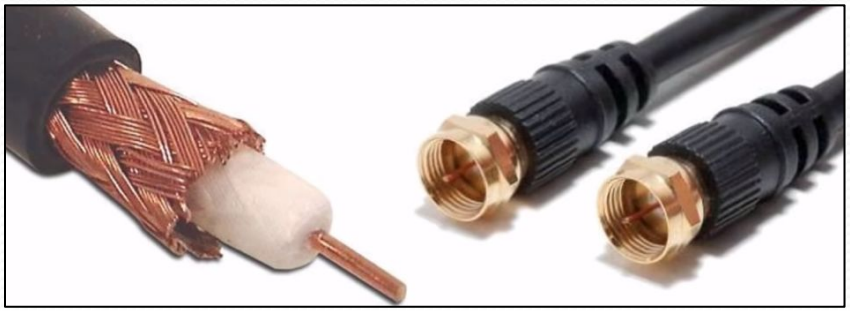
- Hardware used for I/O of information used by final users
- Offer access to servers and other clients
- Examples:
  - PCs and laptops
  - Dumb terminal and network computers
  - Transactional terminals: ATM / POS
  - Mobile: Smartphones, Tablets, Watches

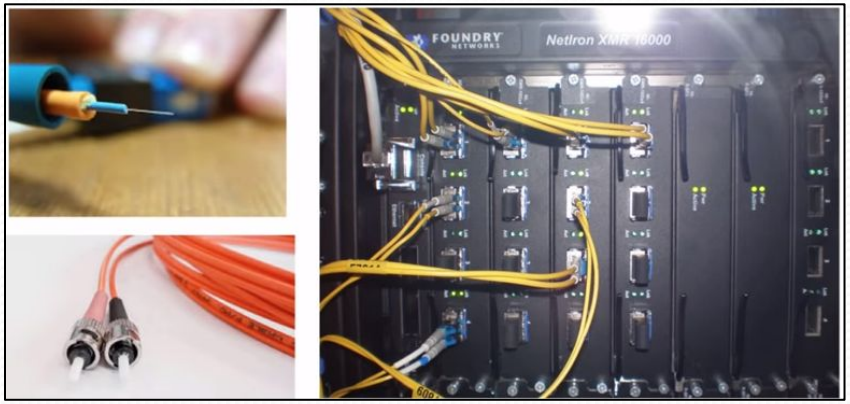
Network Devices

Communication Media

Cable or Wired







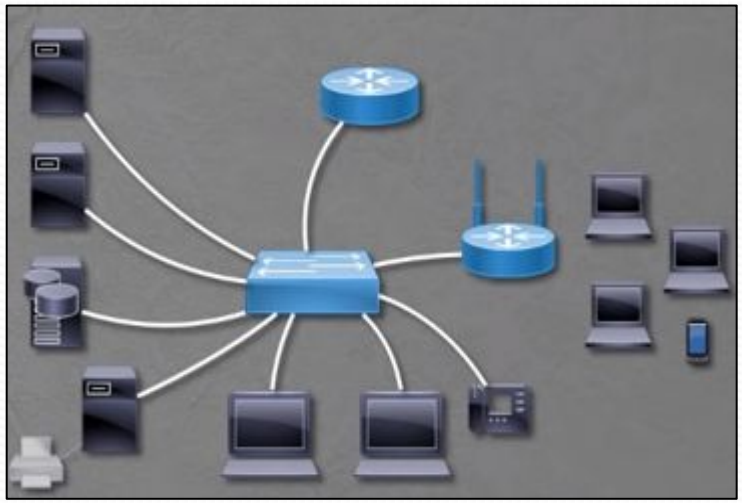
Wireless

Types of Networks

LAN | Backbone | MAN | WAN

LAN

- Local Area Network
- Scale: a room or a building
- Elements: Clients, Servers, Switches, Access points, Printers, Router to exit the LAN
- Typical speeds: 100 Mbps to 1 Gbps

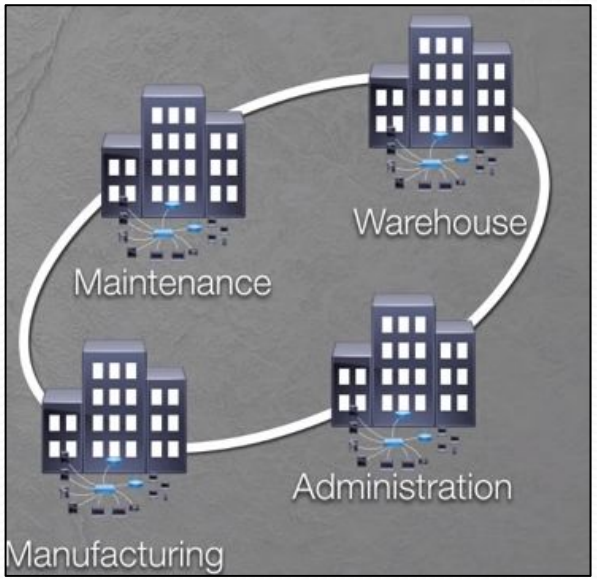


Types of Networks

LAN | Backbone | MAN | WAN

Backbone

- Scale: less than a few kms
- Elements: LANs, high-speed switches or routers, high-speed circuit (fibre optic cables) to interconnect LANs
- Typical speeds: from 1 - 40 Gbps

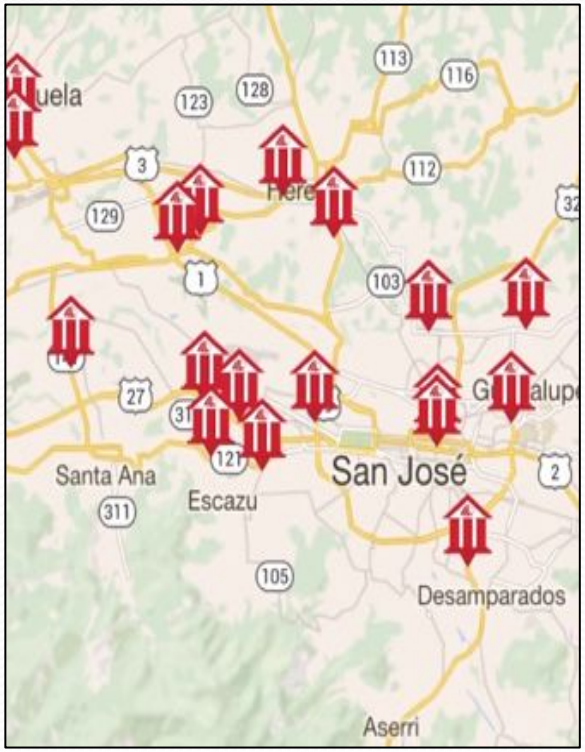


Types of Networks

LAN | Backbone | MAN | WAN

MAN

- Metropolitan Area Network
- Scale: more than a few kms
- Elements: LANs, BNs, circuits leased to public providers (cable co.), microwaves
- $$$$ and internet as an alternative
- Typical speeds: from 64 Kbps - 10 Gbps



Types of Networks

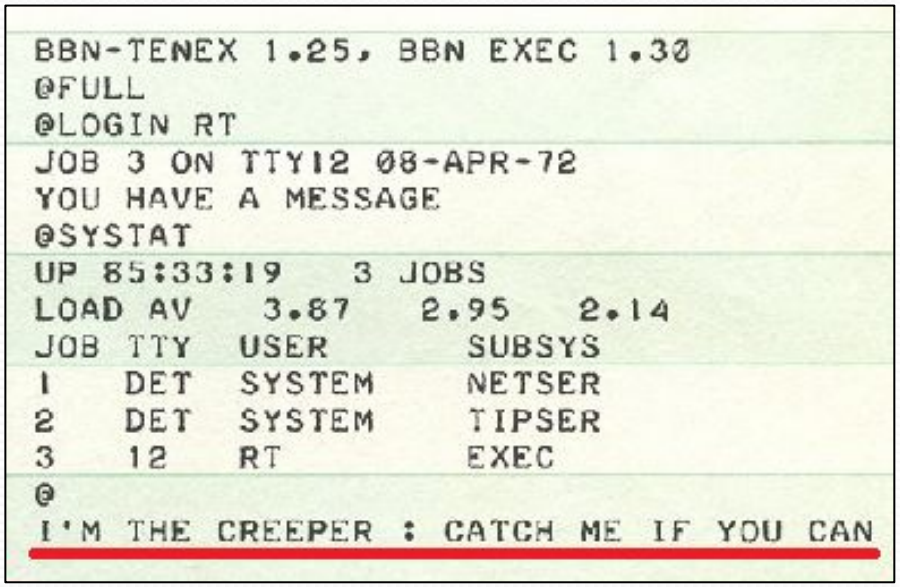
LAN | Backbone | MAN | WAN

WAN

- Wide Area Network
- Scale: more than tens/ thousands of kms
- Elements: same as MAN, but at greater distance
- Typical speeds: from 64 Kbps - 10 Gbps

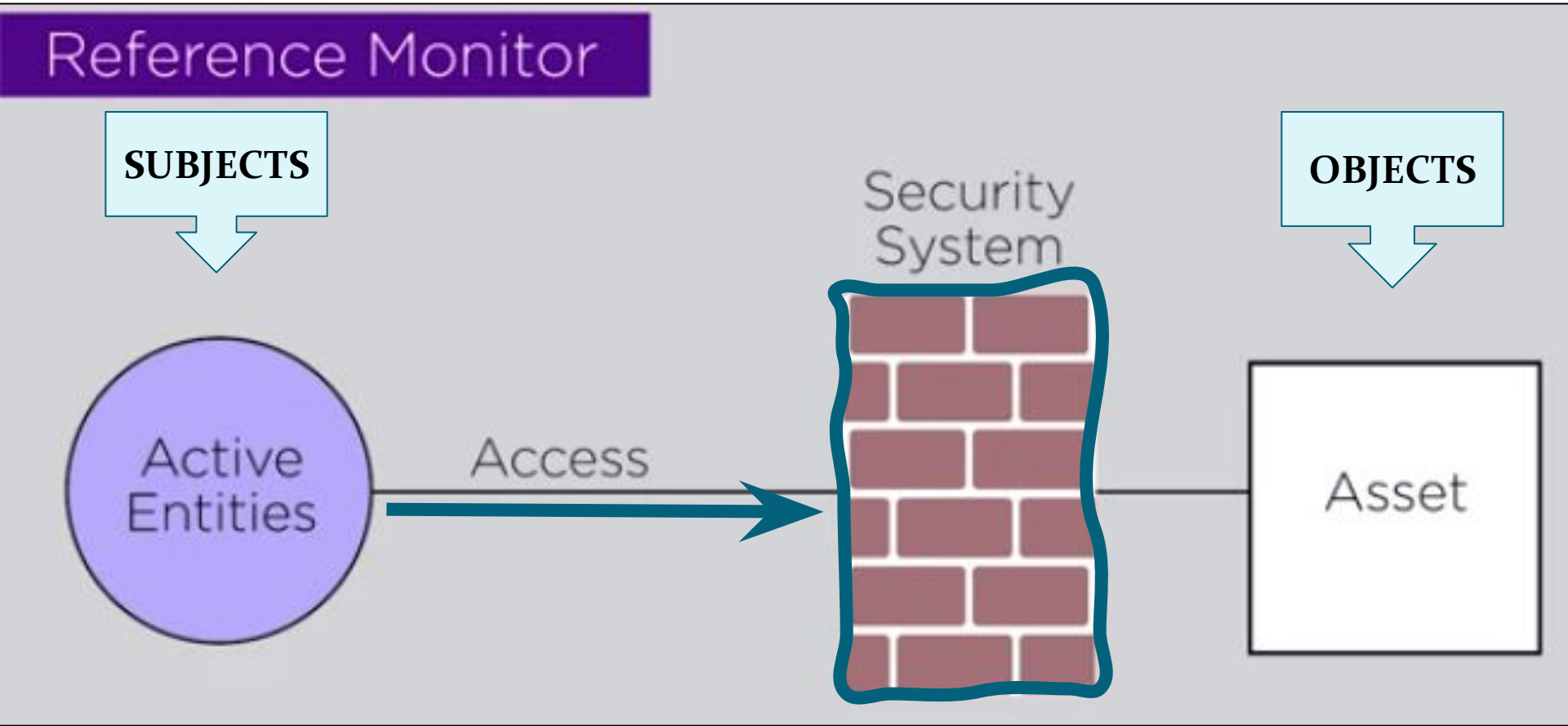
Origin - Cyber Security

- **Bob Thomas** designed a computer program to navigate through Tenex terminals & named it as "*Creeper*"
- "*I'M THE CREEPER: CATCH ME IF YOU CAN*"
- **Ray Tomlinson** (who invented email) saw this program and tinkered the code to fix, hence named it as "*Reaper*"
- First Antivirus Software: which would chase "*Creeper*" and delete it.



Purpose - Cyber Security

- **James Anderson** (late 70's) named it "*Reference Monitor*"
- "*Security as an Enabler*" enables Subjects & Objects to communicate



Cyber Security?

- Practice of protecting systems, networks, and programs from digital or cyber attacks & unauthorized threats.
- Protects the data and integrity of computing assets belonging to or connecting to an organization's network.

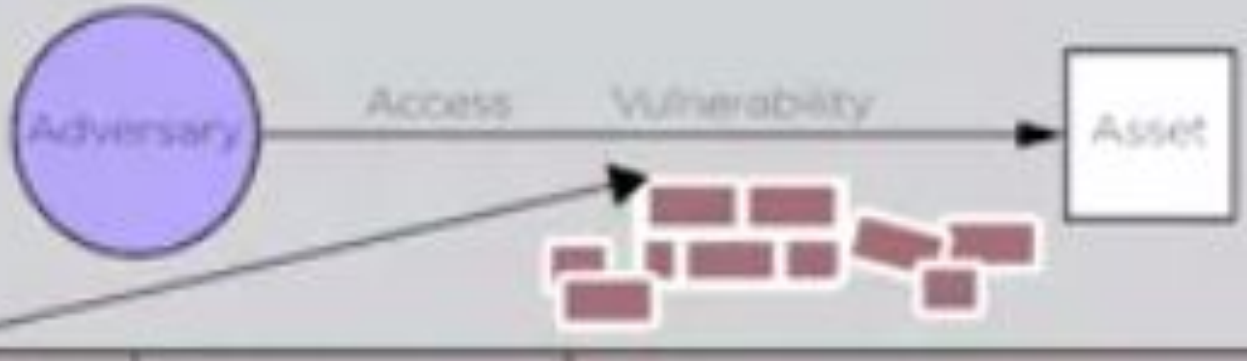
Adversaries

- Hackers
- Criminals
- Hacktivists
- Nation-state Actors

Adversary Type	*Motivation*	*Defining Attributes*
Vandal	Mischief	*Individually capable, predictable*
Hacktivist	Anger	*Group capable, unpredictable*
Criminal	Greed	*Well funded, financial motivation*
Nation-State	Dominance	*World class capability and support*

Vulnerabilities

"A system attribute or feature that can be exploited to cause an adverse effect."



Vulnerability Type	*Root Cause*	*Defining Attributes*
System Flaw	Complexity	*Insufficient design, test, build, operate*
Lack of Security	Budget	*Attention not paid to proper protection*
Human Actions	Ignorance	*Lack of security awareness and training*
Organizational	Irresponsibility	*Inadequate staff, procedures and process*

Cyber Threats

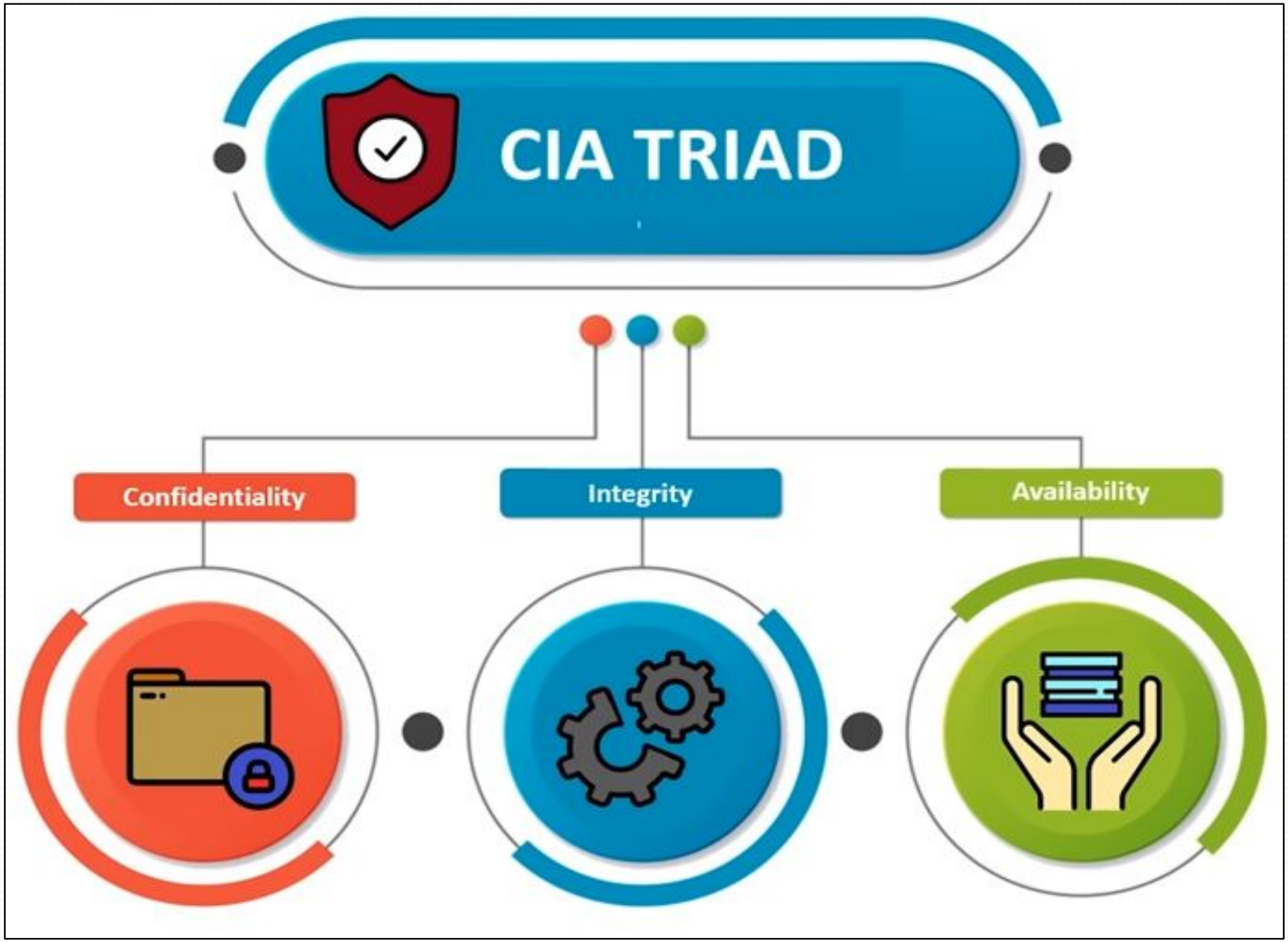
Sample Video

Example for a "Man in the Middle" threat:

https://drive.google.com/open?id=1tWZoFhgtDdMASEkGaqXT-ct-Gy6gr6gH

- Never access your sensitive info while on a public wifi (ex: Malls, Airports, Hotels)
- Install a security solution on your smartphone

Information Security



Information Security ...contd

Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

Integrity

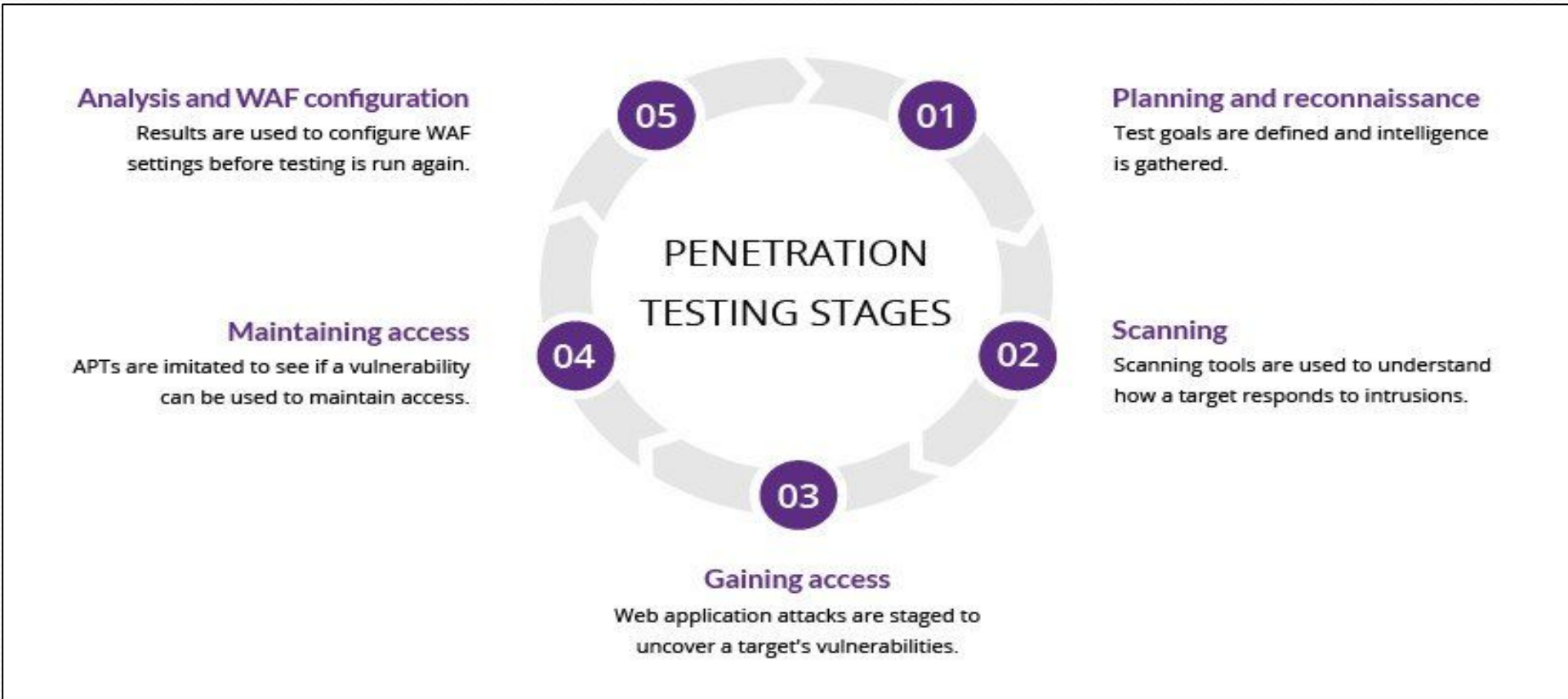
- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

Availability

- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

Penetration Testing

- *Pen Testing or Ethical Hacking, is the practice of testing a computer system, network/ web application to find security vulnerabilities that an attacker could exploit.*
- *Penetration testing can be automated or performed manually.*



Regulatories

- **SOX**: Sarbanes-Oxley, introduced an Act in 2002
- **PCI-DSS**: Payment Card Industry
- **PA-DSS**: Payment Application
- **NIST**: National Institute of Standards and Technology
- **SSAE-16**: Statement on Standards for Attestation Engagements No. 16
- AT-101
- **ISO**: International Organization for Standardization
- Privacy Shield
- HIPAA/HITECH

Tools Involved

- **Metasploit**: Very popular collection of various penetration tools.
- **Nmap**: Also known as Network mapper - a free and open source tool for scanning your systems/ networks for vulnerabilities.
- Wireshark
- Aircrack-ng
- John the Ripper
- Nessus
- Burpsuite

Certifications

- **CISSP:** Certified Information Systems Security Professional
- **CISA:** Certified Information Systems Auditor
- **CISM:** Certified Information Security Manager
- **GSEC:** GIAC Security Essentials Certification
- **CRISC:** Certified in Risk and Information Systems Control
- **CEH:** Certified Ethical Hacker
- **ECSA:** EC-Council Certified Security Analyst
- **GPEN:** GIAC Penetration Tester
- **CompTIA Security+**
- **SSCP:** Systems Security Certified Practitioner