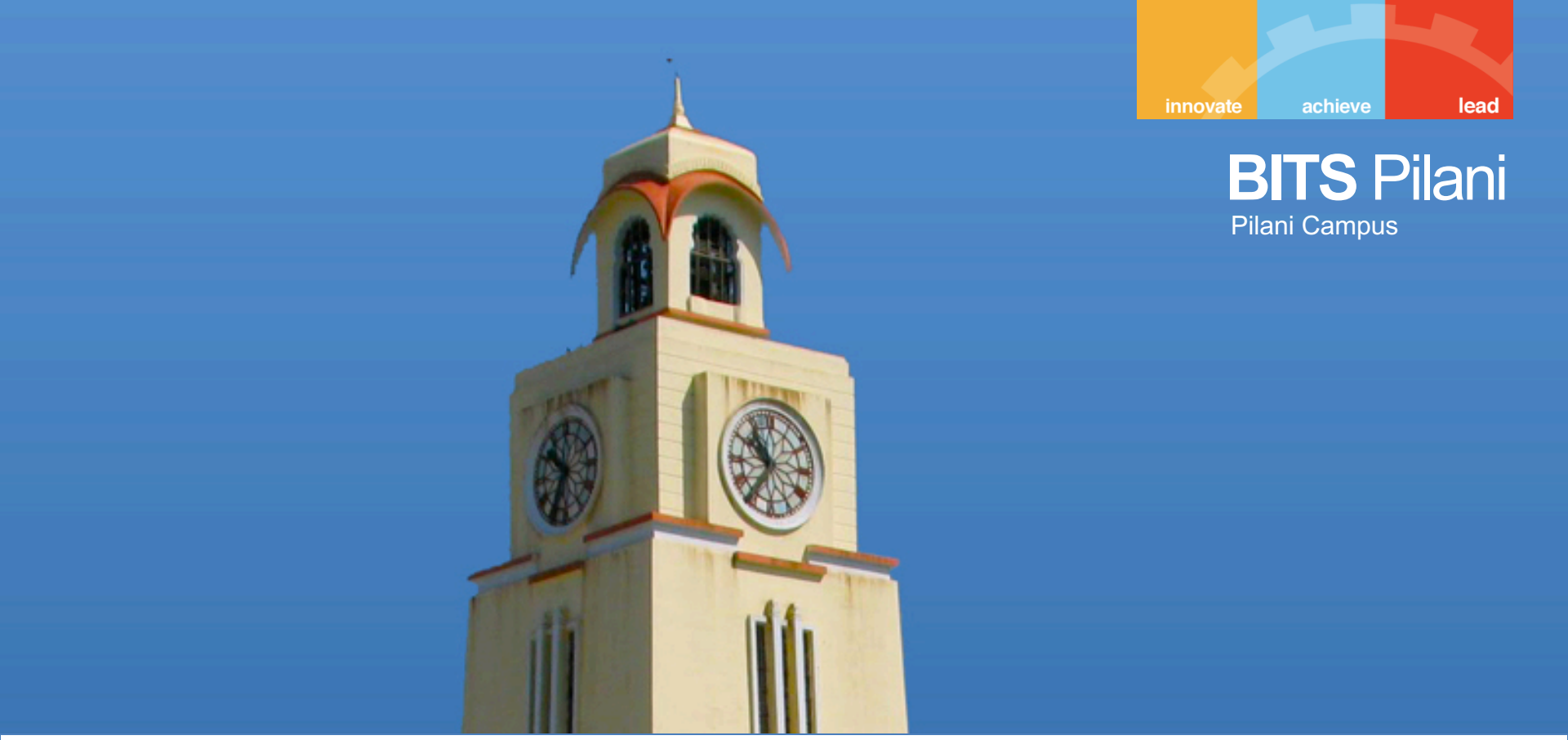
# BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



innovate achieve lead

BITS Pilani
Pilani Campus

# SSZG681: Cyber Security
# Lecture No: 04

## Attacks in Network

# Agenda

innovate achieve lead

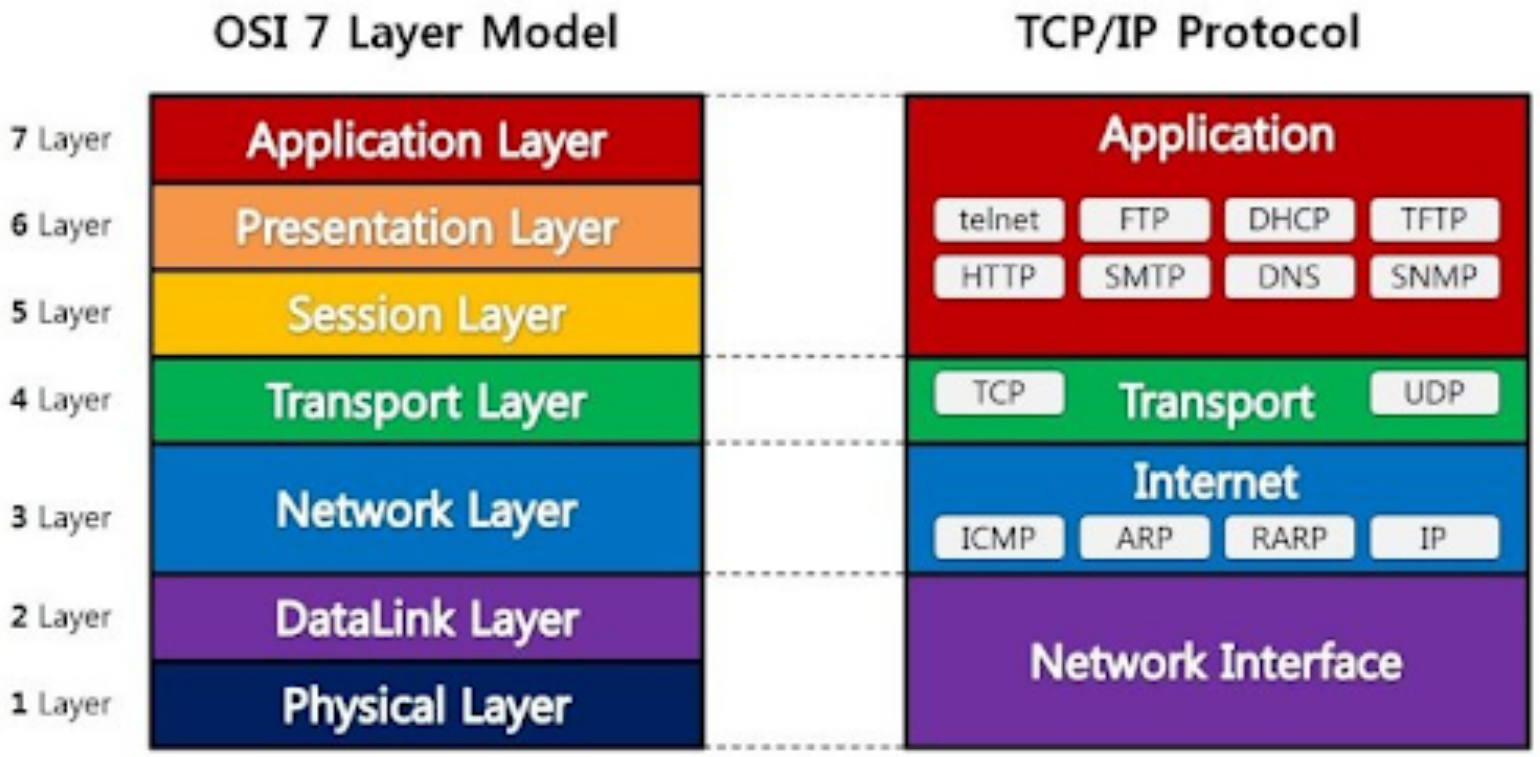
- Network Transmission Overview
- Network Flooding
  - Malicious Code
  - Resource Exhaustion
- Distributed Denial-of-Service
  - Scripted Denial-of-Service Attacks
  - Bots
  - Botnets
- Autonomous Mobile Agents

# Network Transmission Media

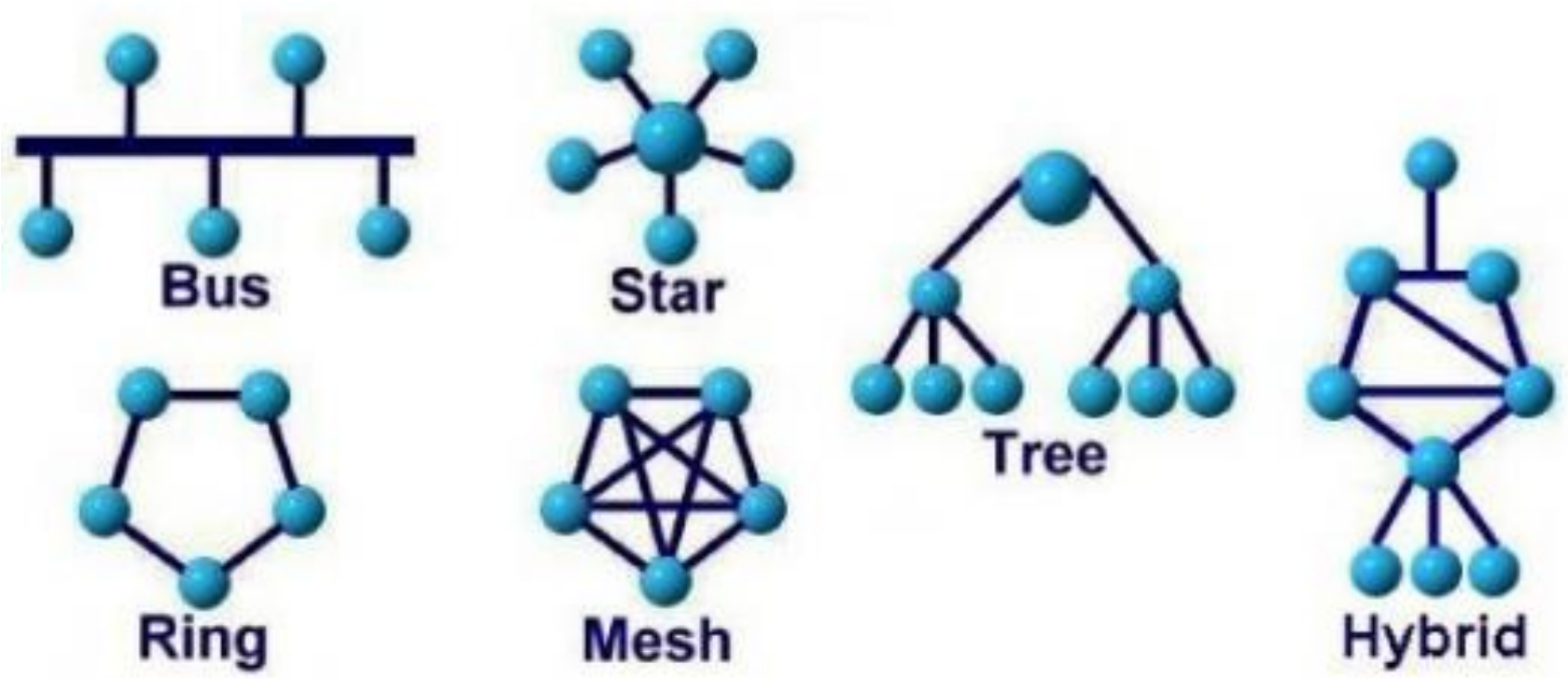


| Medium | Strength | Weakness |
|---|---|---|
| Wire/Cable | • Widely used<br>• Inexpensive | • Susceptible to wiretapping<br>• Susceptible to radiation |
| Optical Fiber | • Immune to radiation<br>• Difficult to wiretap | • Potential exposure of radiation at join points |
| Microwave | • Strong signal<br>• Not impacted by weather | • Can be intercepted along path of transmission<br>• Requires line of site for transmission<br>• Signal must be repeated approx every 50Km |
| Wireless (Radio, WiFi) | • Widely available<br>• Built as part of computers | • Suitable for short range<br>• Can be intercepted around transmitter |
| Satellite | • Strong signal<br>• Faster signal speed | • Signal travel larger distance<br>• Signal exposed in WAN |

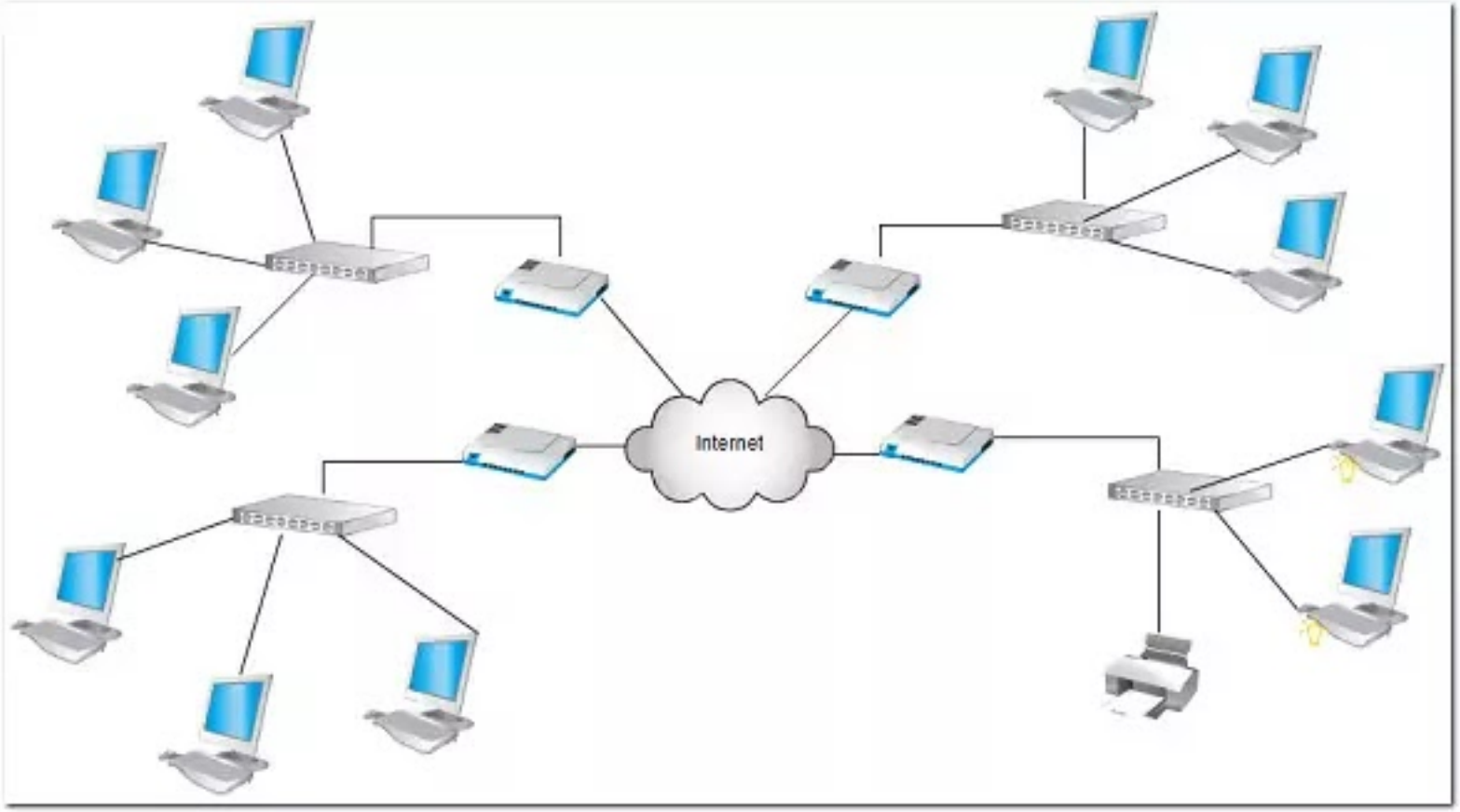
# OSI & TCP/IP Models of Networking



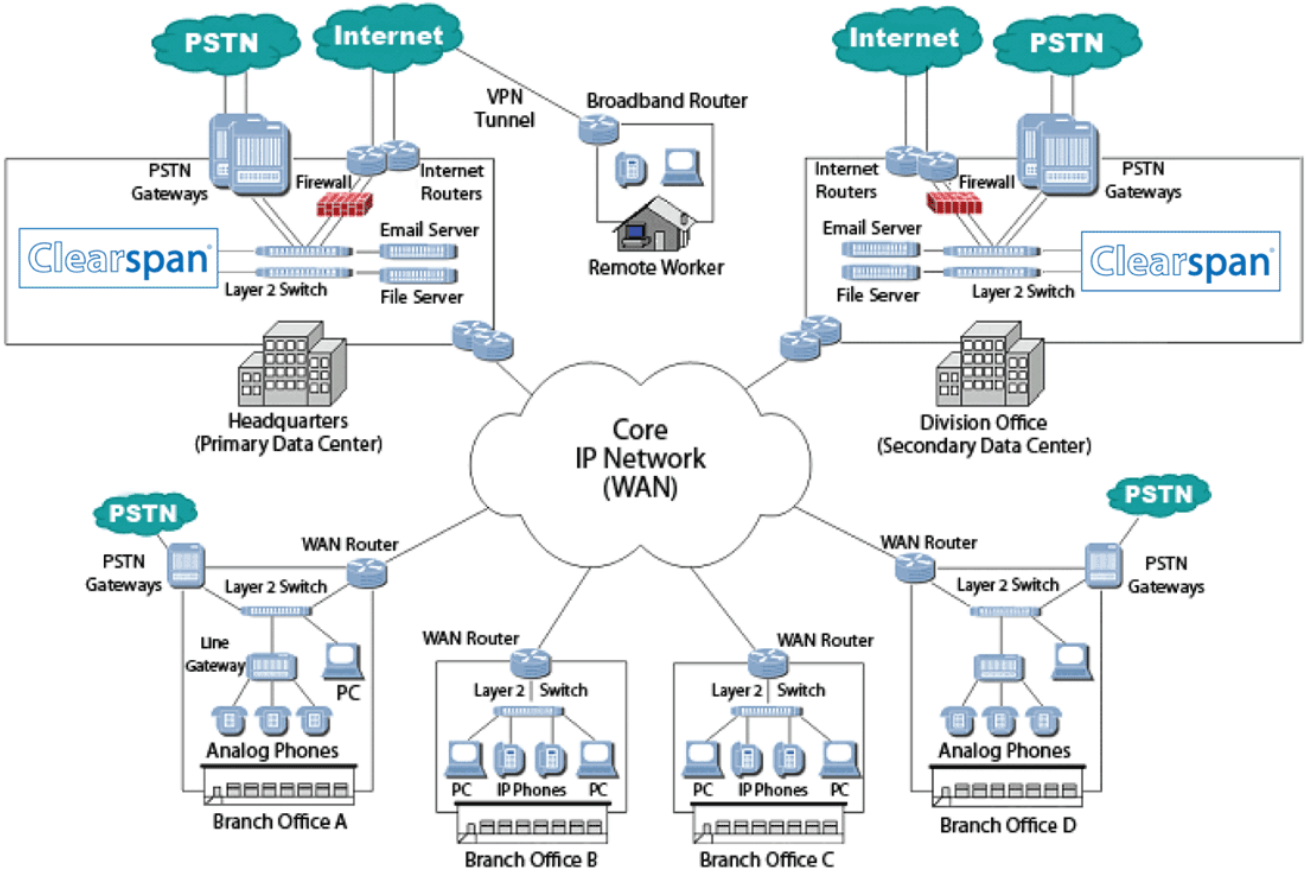
# Network Topology Types



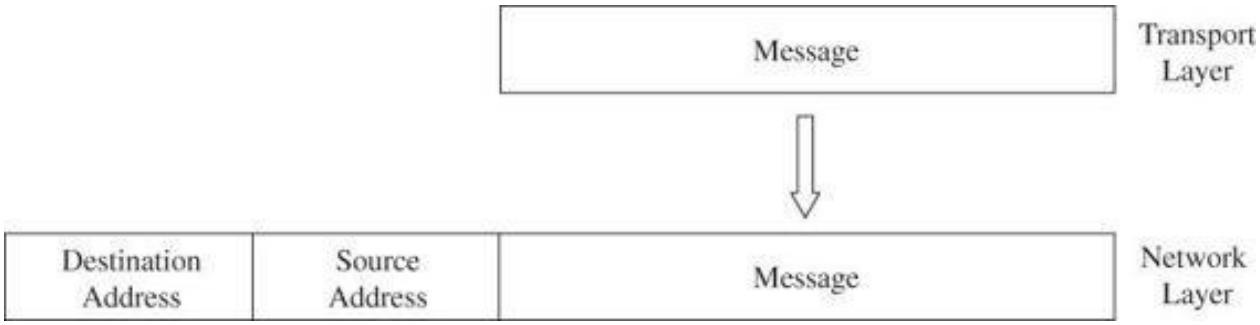
# Network Transmission: Example 1



# Network Transmission: Example 2

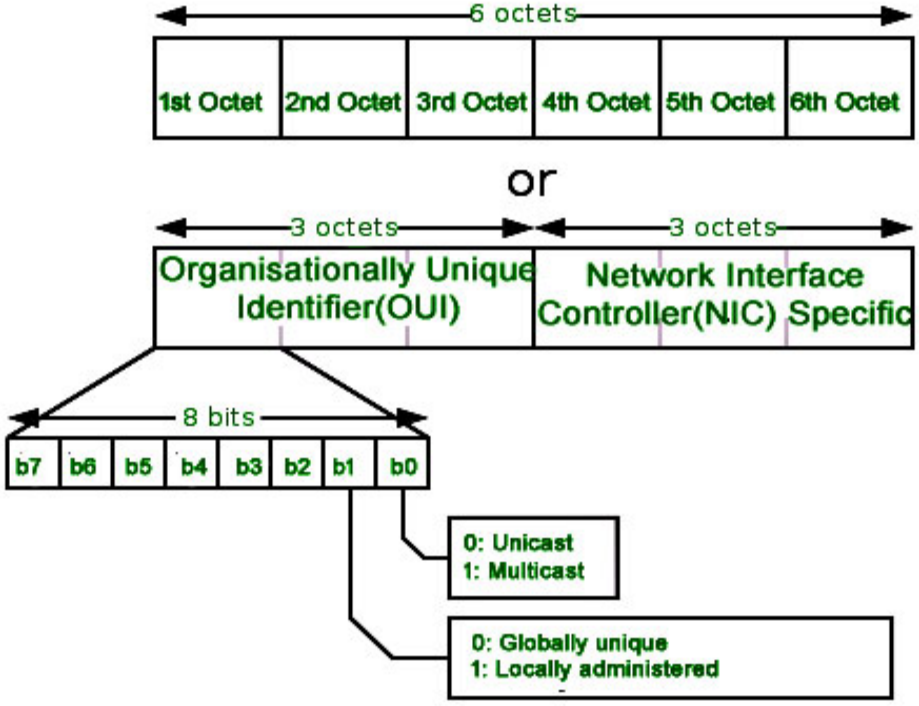


# Addressing and Routing




- **MAC (Media Access Control):** Unique of a Network Interface Card (NIC) that connects a computer and a network
- Routers direct traffic on a path that leads to destination
- **Port:** Number associated with an application program that serves or monitors for a network service

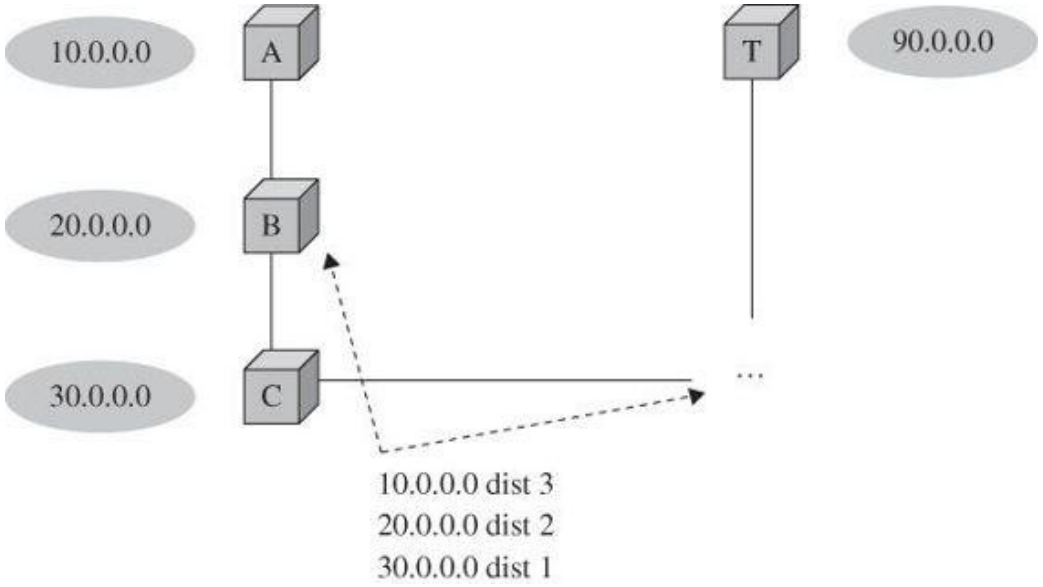
# MAC Address Format




- 12-digit hexadecimal number (6-Byte binary number), represented by Colon-Hexadecimal notation.
- First 6-digits (ex 00:40:96) of MAC Address identify the manufacturer, called as OUI (**Organizational Unique Identifier**).
- IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

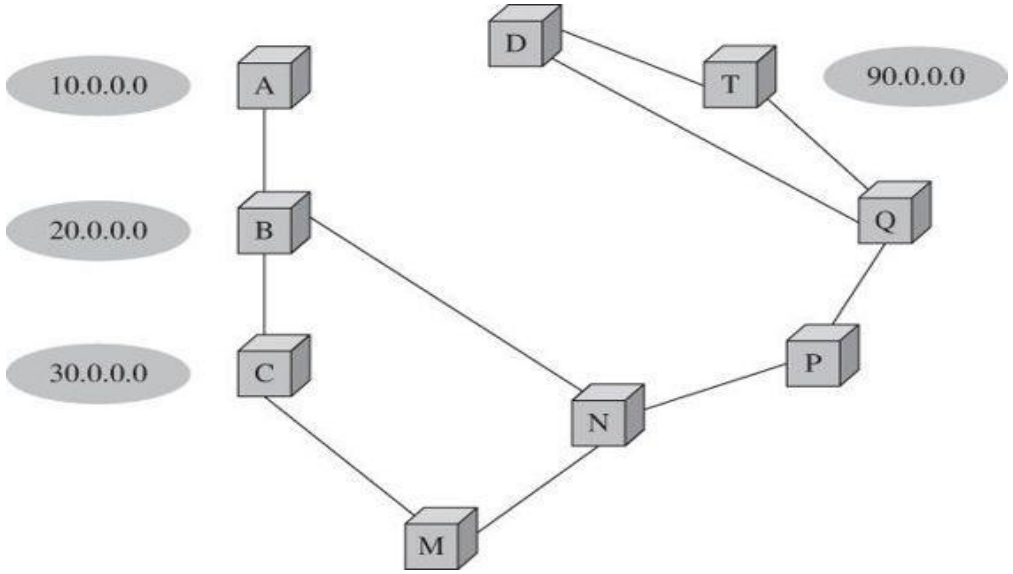
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

# Message Routers




- Network routers are loose confederation of mutually trusting components
- Each router sends message to other routers listing addresses to which it has path
- This way routers build a web of network and use an optimum path for sending messages from one user to another

# Example: Message Routers




- A is not directly connected with T. Shortest path is ABNPQT. Can also communicate thru ABCMNPQT
- Any corruption in routers tables can lead to traffic mis-alignment i.e. if T broadcasts that it's 1 distance away from 10.0.0.0 subnet all request will come to it instead A
- Routers implicitly trust each other

# Source Routing



- Internet traffic travels by best available route (next hop) – routers determine the path
- **Strict source routing:** Sender can specify the exact route for the message to receiver
- **Loose source routing:** Sender can specify certain required intermediate points of the route
- Source routing is usually used for testing and troubleshooting the identified path
- Source routing can be mis-used to flood a particular route on the network

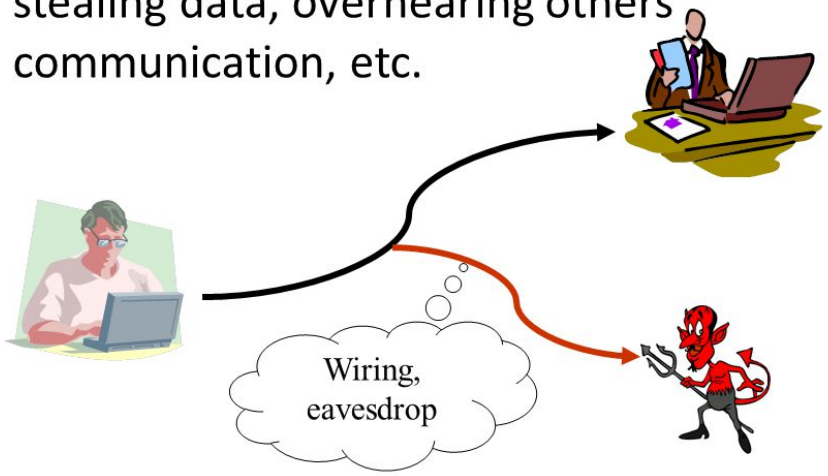
# Threats to Network Communication

- **Interception:** Unauthorized viewing
- **Modification:** Unauthorized change
- **Fabrication:** Unauthorized creation
- **Interruption:** Preventing authorized access

# Interception

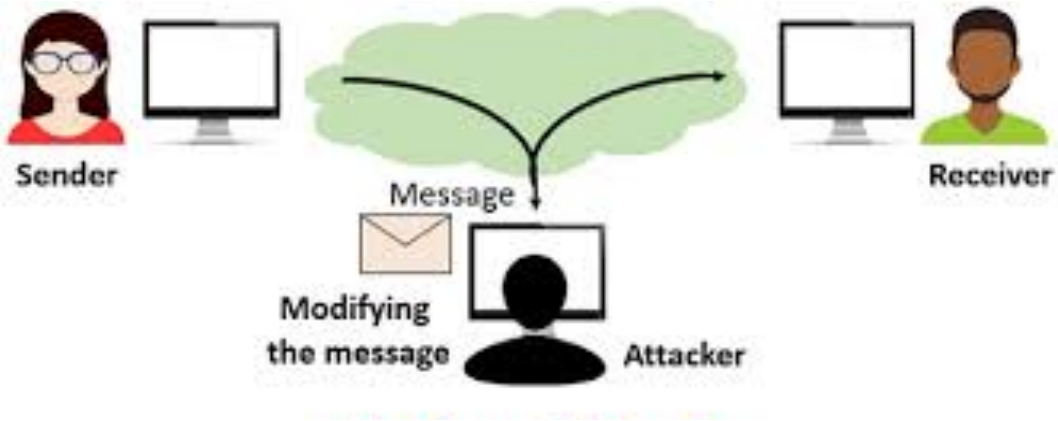
- Wiretapping
- Causes for interception
  - Anonymity
  - Many points of attack
  - Sharing
  - System complexity
  - Unknown perimeter
  - Unknown path

***Interception:*** an unauthorized subject has gained access to an object, such as stealing data, overhearing others communication, etc.



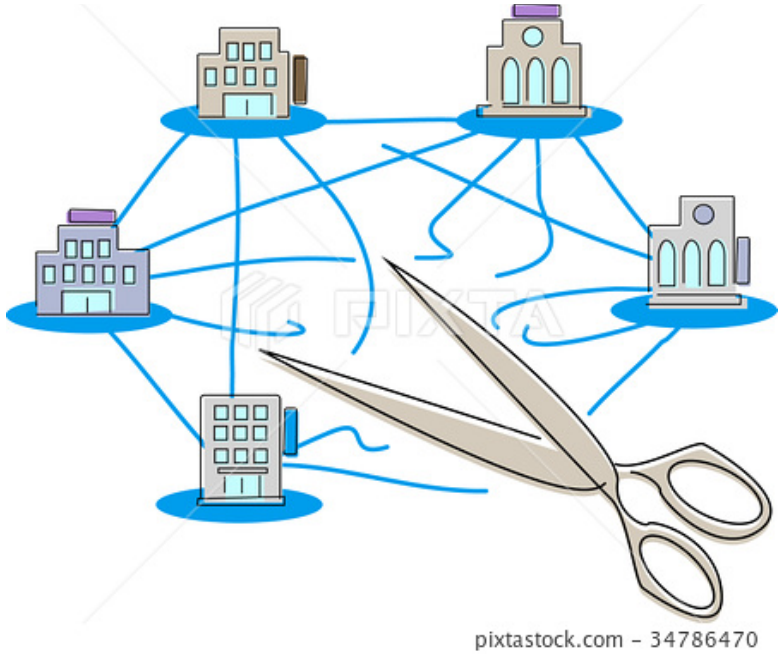
# Modification and Fabrication

- Causes data corruption
  - Can occurs naturally because of minor failures of transmission media
  - Can also be induced for malicious purposes.
- Causes for modification/ fabrication
  - Sequencing
  - Substitution
  - Insertion
  - Replay
  - Physical replay



# Interruption

- Loss of service
- Causes for interruption
  - Routing
  - Excessive demand
  - Component failure
- Network design incorporates redundancy to counter hardware failure



# Port Scanning



- A port scan maps the topology and hardware and software components of a network segment
- Port scanning tools: Nmap, Netcat, Unicornscan, Zenmap
- Port scanning data
  - how many hosts are there and what their IP addresses are
  - what their physical (MAC) addresses are
  - what brand each is and what operating system each runs, and what version
  - what ports respond to service requests
  - what service applications respond, and what program and version they are running
  - how long responses took
- Network and vulnerability scanners can be used positively for management and administration and negatively for attack planning

# Port Scanning: Nmap Examples



- **nmap -v scanme.nmap.org**

  Scans all reserved TCP ports on the machine scanme.nmap.org in verbose mode
- **nmap -sS -O scanme.nmap.org/24**

  Launches a stealth SYN scan against each machine that is up out of the 256 IPs on the class C sized network where Scanme resides. It also tries to determine what operating system is running on each host that is up and running.
- **nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127**

  Launches host enumeration and a TCP scan at the first half of each of the 255 possible eight-bit subnets in the 198.116 class B address space. This tests whether the systems run SSH, DNS, POP3, or IMAP on their standard ports, or anything on port 4564.
- **nmap -v -iR 100000 -Pn -p 80**

  Asks Nmap to choose 100,000 hosts at random and scan them for web servers (port 80).
- **nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20**

  This scans 4096 IPs for any web servers (without pinging them) and saves the output in grepable and XML formats.

# Port Scanning: Nmap Examples



```
root@wks01:/home/vivek# nmap --top-ports 10 192.168.1.1

Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IST
Interesting ports on 192.168.1.1:
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

# Network Flooding

innovate achieve lead

- Flooding is caused by excessive demand which is far more than available capacity
- Can be caused by malicious or natural events
- It is a routing technique in computer networks where a source or node sends packets through every outgoing link
- A packet tries to access all available network routes and ultimately reaches its destination, but there is always the potential for packet duplication
- Hop count and some selective flooding techniques are used to avoid communication delay and duplication
- Flooding is also used as a denial of service attack by flooding network traffic to bring down a network service
- The service is flooded with many incomplete server connection requests
- Due to the number of flooded requests, the server or host is not able to process genuine requests at the same time

# Network Flooding…

- Volume based attacks generating much higher demand than available system capacity
  - Attacker can present commands more quickly than the system can handle
  - Commands queue up and ultimately chock the system by overloading or flooding
- Application based attack to overwhelm network capacity
- Targets for flooding: database, network, operating system, print servers, routers etc
- Block Access
  - interfere with network routing and prevent access requests to the system
  - Change/delete access control records or disable access fully
- Access failure
  - Software failure due to malfunction
  - Hardware failure due faulty device or component
  - Disable communication link between two points

# Example: Estonian Web Failure



- In 2007 Estonia decides to move a statue ‘Bronze Soldier’ which commemorated Russian involvement in WW2
- Russia doesn’t like it – large scale public protests in Moscow around Estonian embassy and in Estonia by Russian ethnic people
- Estonia is one of highest computerized countries in world
- Immediately after protests, Estonian govt & public organization websites are flooded with traffic of 100-200 mbps – a very high traffic volume in 2007
- Attacks started on Apr 27 and continued for several days
- Attacks surged again during May 8-9 period when Russia celebrates victory over Germany and surged again around middle May
- Security experts found that attacks largely came from outside Estonia
- Pinpointing the source of attack was not possible due to complex re-routing of traffic but suspicion is on Russia

# Few More Examples



- In Jan 2013, New York Times, Washington Post and Wall Street Journal sites were sent massive traffic resulting in collapse of these sites
- Allegedly these were attacked by hackers with allegiance to China
- In August 2013, Syrian Electronic Army shut access to New York Times website for 20 hours
- In June 2014, Syrian Electronic Army redirected Reuters readers to a message that the site has been hacked

# How does Flooding Work?



Flooding exploits weakness in network protocols and utilities:

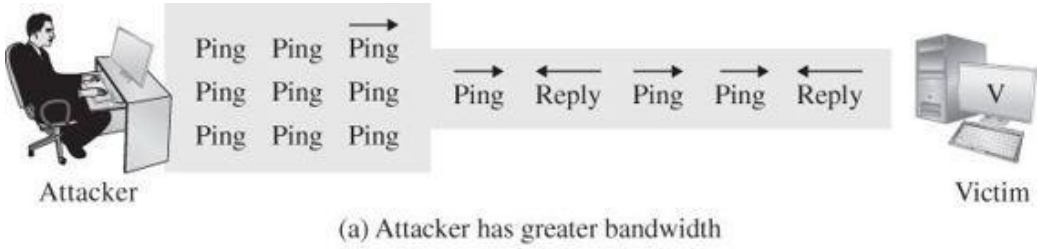
- Insufficient resources
- Insufficient capacity
- Incoming bandwidth is insufficient, or resources like devices, computing power, software or table capacity are inadequate

# Malicious Flooding

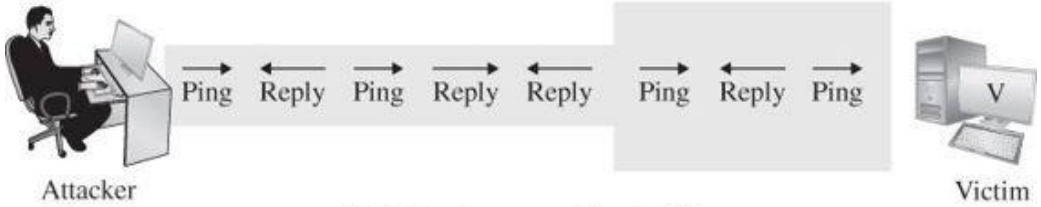


- Basic denial of service tactics are aimed to degrade or stop performance by flooding the network
- Packets don't reach or if reach then performance is severely degraded
- Misusage the robustness of TCP internet protocol
- ICMP protocol commands/utilities
  - Ping, Echo, Destination unreachable, Source quench
  - Can be mis-used for network flooding

# Ex1: Ping Flood




(a) Attacker has greater bandwidth



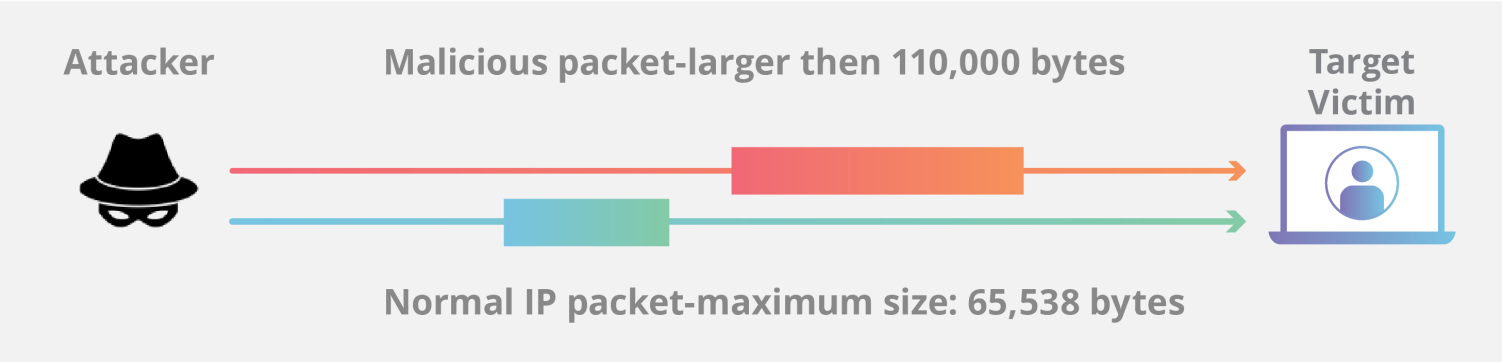

(b) Victim has greater bandwidth

- A ping is a network utility used to test a network connection, a "pulse" is sent out and the "echo" from that pulse tells the operator information about the environment.
- If the connection is working, the source machine receives a reply from the targeted machine.

There are variations of ping that can be used to execute an attack, some are:

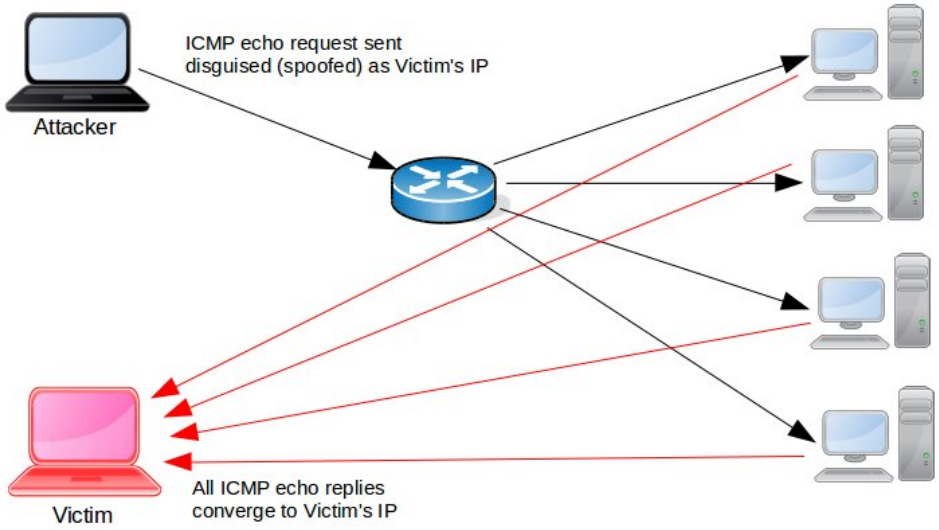
- ping –n : specify the number of times a request is sent
- ping –l : specify the amount of data sent with each packet
- ping –t : continue pinging until the host times out

# Ex2: Ping of Death



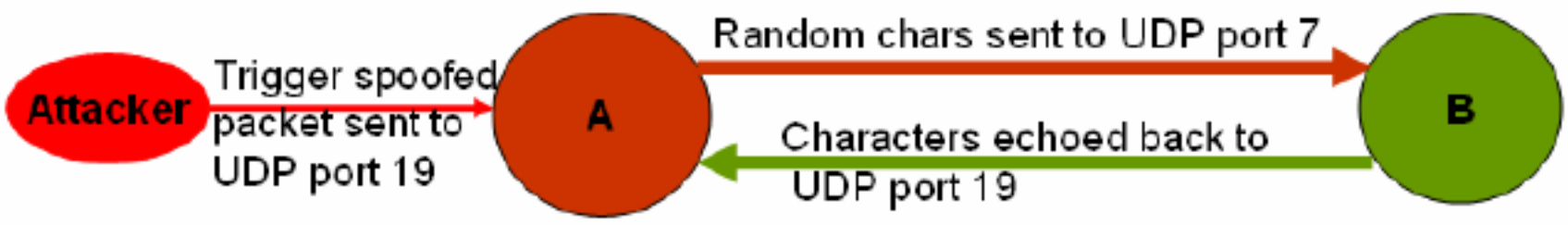

- A Ping of Death is an attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.
- While ping packets are normally very small, IP4 ping packets can be as larger than the maximum allowable packet size of 65,535 bytes. Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.
- When a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit. When the target machine attempts to put the pieces back together, the total size exceeds the limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot.

# Ex3: Smurf




- Smurf malware builds a spoofed packet that has its source address set to the real IP address of the targeted victim.
- The packet is then sent to an IP broadcast address of a router or firewall, which in turn sends requests to every host device address inside the broadcasting network, increasing the number of requests by the number of networked devices on the network.
- Each device inside the network responds to the spoofed address of the target with an ICMP Echo Reply packet.
- The target victim then receives a deluge of ICMP Echo Reply packets, becoming overwhelmed and resulting in denial-of-service to legitimate traffic.

# Ex4: Echo-Chargen



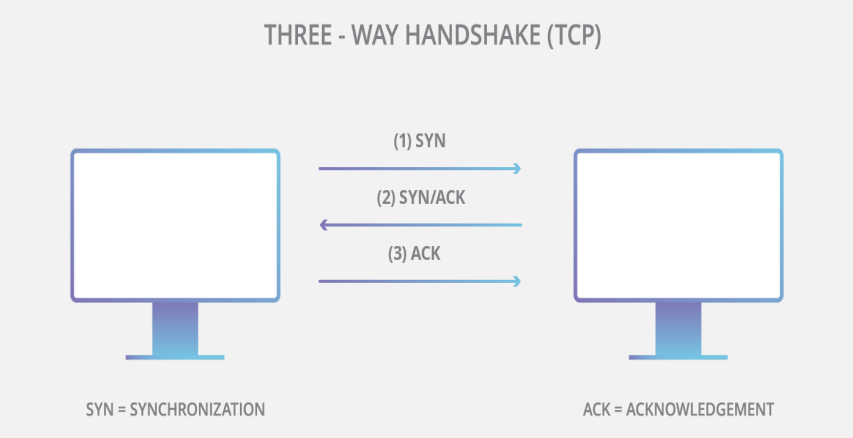

- CHARGEN (character Generation) protocol, is a network service developed to simplify testing, troubleshooting and evaluating networks and applications.
- CHARGEN is a service that can be accessed both by TCP and UDP protocol (via port 19). If the service is accessed, it will use that connection to send a random number of random characters (data).
- CHARGEN attack exploits the CHARGEN protocol points of contact.
- The most common type of these attacks uses CHARGEN as an amplifier for UDP-based attacks using IP spoofing.
- The attack is simple: Attackers have their botnet send tens of thousands of CHARGEN requests to one or more publicly accessible systems offering the CHARGEN service.
- Requests use UDP protocol and the bots use the target's IP address as sender IP so that the CHARGEN service's replies are sent to the target instead of the attacker resulting in tens of thousands of replies getting submitted to the attack target.

# Ex5: SYN Flood



TCP connection exhibits three distinct processes in order to make a connection.

1. First, the client sends a SYN packet to the server in order to initiate the connection.
2. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.
3. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.




An attacker exploits the fact that after an initial SYN packet has been received, the server will respond back with one or more SYN/ACK packets and wait for the final step in the handshake.

1.Attacker sends a high volume of SYN packets to the targeted server, often with spoofed IP addresses.

2.The server then responds to each one of the connection requests and leaves an open port ready to receive the response.

3.While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the server is unable to function normally.

# Ex6: Resource Exhaustion



- Computers do context switching while executing multiple applications
- Context values of switched out applications are stored in registers
- Buffers, log files can be exhausted causing loss of context

# Ex7: Traffic Re-direction



- An attacker can ask a router to declare that it has best path for all IP addresses
- All traffic will be re-directed to this router automatically resulting in flooding

# Ex8: IP Fragmentation: Tear Drop

- Mis-use of a feature actually intended for network performance communication
- Single data unit is fragmented and sent to receiver as per datagram protocol
- Each fragment has a relative position and length in the data unit
- An attacker may send datagrams with overlapping fragments hence receiver will not be able to assemble the assemble the data unit

# How does DNS Work?

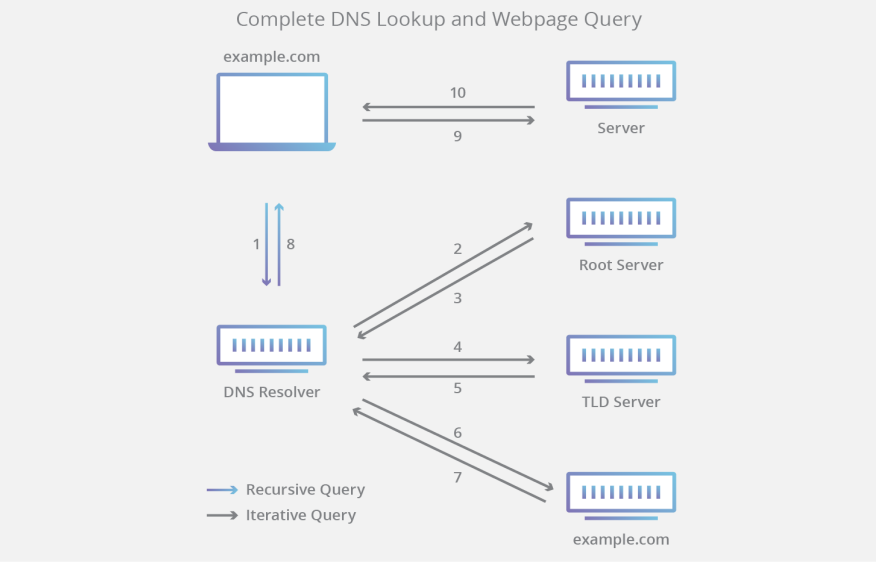


- DNS resolves a hostname into IP address like *www.xyz.com* into 192.152.68.1
- 4 servers involved in this conversion:
  - DNS Recursor: Recursor is like a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor receive queries from client machines through applications such as web browsers. It makes further requests on behalf of client.
  - Root Nameserver: The first step in translating host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
  - TLD Nameserver: Top Level Domain (TLD) server is like a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (in xyz.com, the TLD server is “com”).
  - Authoritative Nameserver: This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor that made the initial request.

# How does DNS Work?



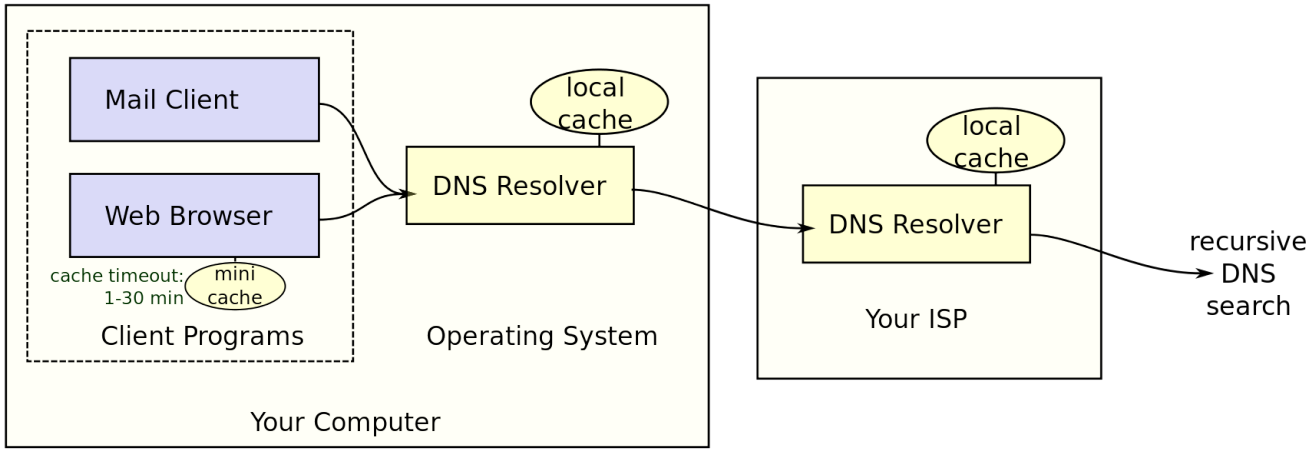
1. A user types ‘xyz.com’ into a web browser. The query is received by DNS recursive resolver.
2. The resolver queries a DNS root nameserver (.).
3. The root server responds to the resolver with the address of a TLD DNS server (such as .com or .net), which stores the information for its domains. The search request for xyz.com is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server responds with the IP address of the domain’s nameserver (xyz.com).
6. The recursive resolver sends a query to the domain’s nameserver.
7. The IP address for xyz.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

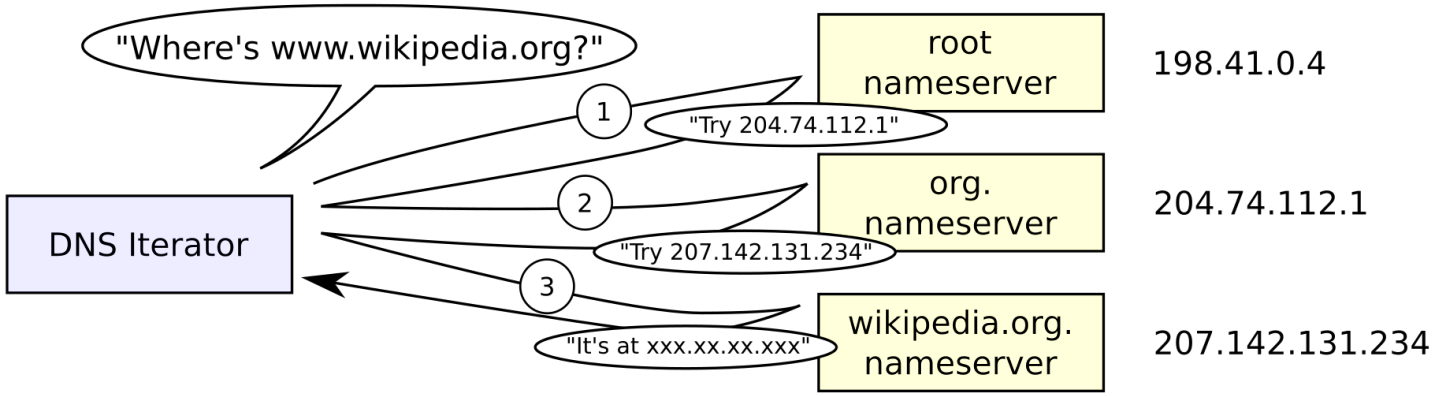



Once the DNS lookup have returned the IP address for xyz.com, the browser is able to make the request for the web page:

9. The browser makes a HTTP request to the IP address.
10. The server at that IP returns the webpage to be rendered in the browser.

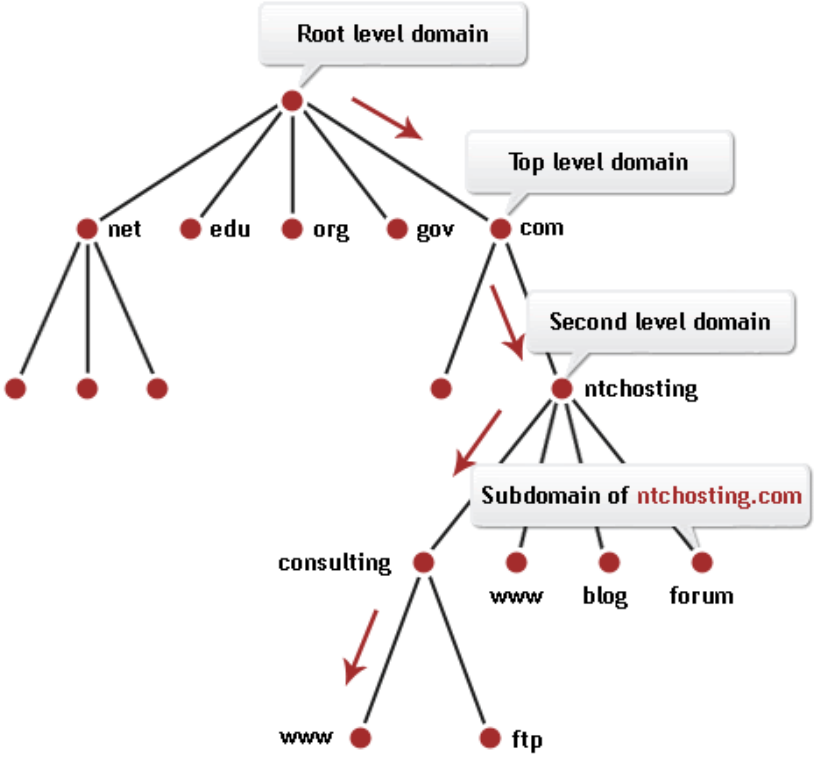
# How does DNS Work?



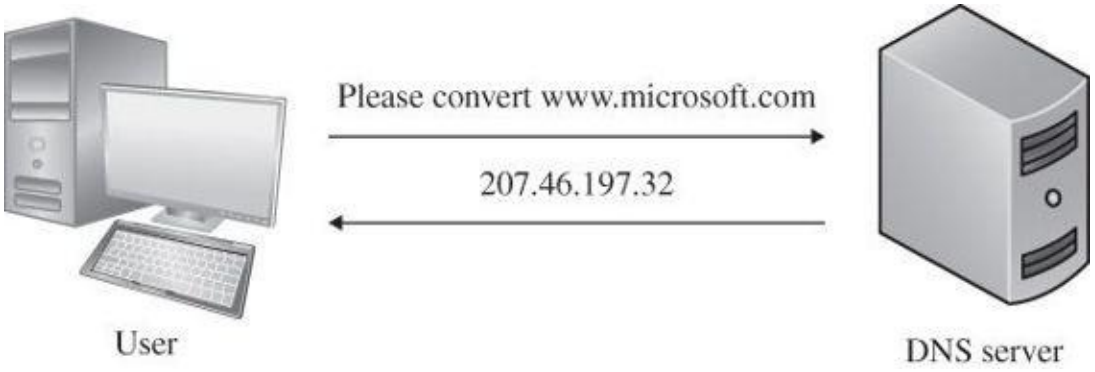



# DNS Attacks

- Most common implementation of name server software is thru BIND (Berkley Internet Name Domain) which has flaws like buffer overflow. An attacker can overtake the server and re-route the traffic
- Top level domain attack
  - 13 top level domain servers spread across world
  - Translate the top level or last part of address like .com, .uk, .in, .org, .edu etc
  - A 2002 attack flooded the top level server causing major internet outages, Possible cause was some mis-configured firewalls
  - 2007 similar attack happened and outages of 6 hours. The attack originated from APAC region.
  - Root name servers use a new design 'anycast' which spreads the lookup to many servers thus nullifying the attack on one single server

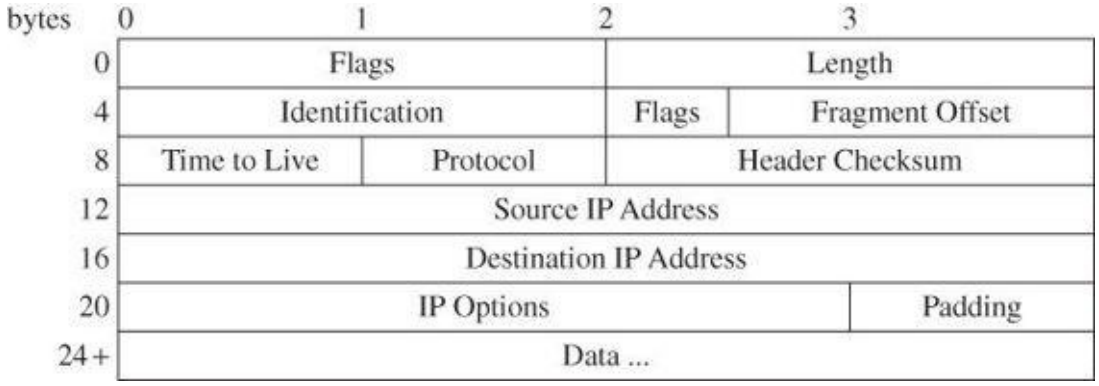


# Ex1: DNS Spoofing




- Mis-routing: change of IP address
- DNS server translates internet names into IP addresses
- A ‘man in the middle’ attack can intercept the communication between user and DNS server and change address resulting in denial of service or be the intermediate person
- Attackers also try to insert inaccurate entries in DNS server cache known as DNS poisoning

# Ex2: Session Hijack




- Attacker allows communication to start between parties and then takes over i.e. take control once authentication is over
- Un-encrypted sites have high exposure to this risk
- It takes advantage of TCP/IP design protocol. Changes source IP in the IP header causing communication redirect

# Ex3: DNS Cache Poisoning



- Send a forged message to DNS regarding change in address of a website
- A DNS server asks it's root server for unresolved queries who passes it to other severs. These queries are assigned a simple sequence number
- A rogue response will result in bad match for an address
- In 2010 internet governing bodies came with a DNSSEC security extension (RFC 4033) which signs the root server DNS records
- This would eliminate fake responses

# Exploiting Known Vulnerabilities

- Hackers often begin with known vulnerabilities for which patches haven't been installed by the user
- **Zero-day-exploit:** exploitation of a vulnerability for which a patch is not yet available
- **R-U-Dead-Yet, EvilGrade, Zeus** are some tools which identify vulnerabilities to help organize an attack

# Denial of Service

# Denial of Services

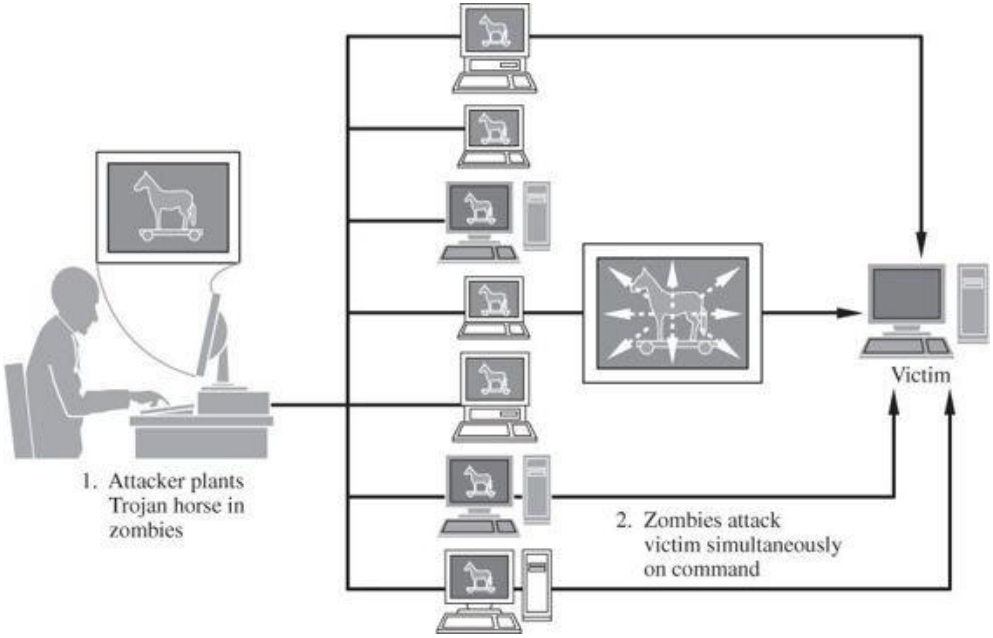


- Attempt to disrupt availability of computer systems
- User is denied access to authorized services or data
- Disruption in the services thru:
  - communication link breakage,
  - sever flooding
- Attack on confidentiality & integrity of service is binary in nature
- Attack on availability is nuanced i.e. it could be of insufficient or unacceptable level

# Distributed Denial of Services (DDOS)

- DDOS attacks change the balance between attacker and victim by marshalling many forces towards attacker
- Stats (Arbor Networks):
  - More than 350,000 DDOS attacks 2009 – one attack every 90 seconds
  - SYN flood accounts for over half of these attacks
  - 20000 attacks exceeded 1 GBPS speed
  - 4000 of the 1+ GBPS attacks lasted for 8 hrs or more
  - 3500 attacks were more than 4 GBPS and 2000 were more than 10 GBPS
  - In 2014 33% attacks were over 20 GBPS
  - Web sites are served 6 – 8 million requests per second which hardly any website is designed to service

# DDOS Approach



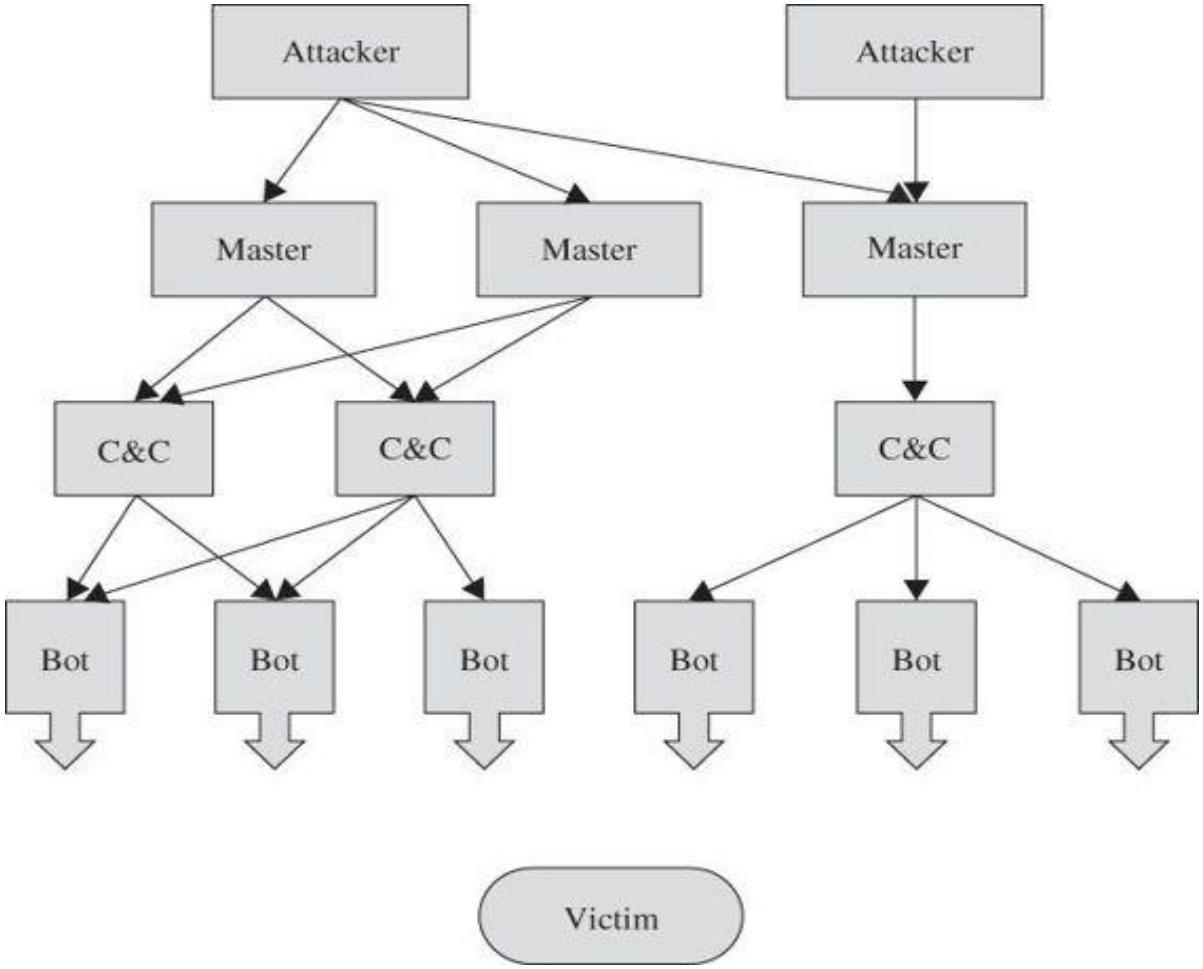

- Attacker conscripts multiple machines thru a Trojan horse
- The Trojan remain silent and is harmless to infected machine
- Each compromised machine is called a Zombie
- Attacker asks Zombies to start attack using varied methods

# DDOS Approach…



- Tool based scripted attacks
- Tool can be used to install and control Zombies
- Zombies/Bots are normally unpatched machines – attackers identifies these by scanning machine for vulnerabilities
- Botnets (network of Bots) is used or massive DDOS attack

# Botnet Command and Control



# Rent-a-Bot



- Bot Master: Person who controls the bots
- Bot master uses bots to:
  - Carry out attacks on victims
  - Rent out bot(s) to others for attacks – revenue generation
  - Create a network of compromised hosts to launch an attacks (for self or rented)
- Opt-in-bot: Like minded bots to add to your lone voice

# Physical Disconnect



- A broken cable, appliance or connector results into denial of service
- Machine along transmission route can fail
- Component failure like circuit board, storage device, monitoring device failure
- Consequences of a hardware failure can be like data corruption, software corruption etc

# Defense against DDOS Attacks



- Develop a DDOS service response plan
- Secure network infrastructure
  - Install patches for vulnerabilities
  - Adjust number of active servers
  - Use load balancers
  - Blacklist rogue IPs
- Practice basic network security – complex password
- Build strong network architecture – build redundancies
- Leverage cloud, Enroll for cloud scrubbers like ‘akamai’
- Understand and listen for warning signs

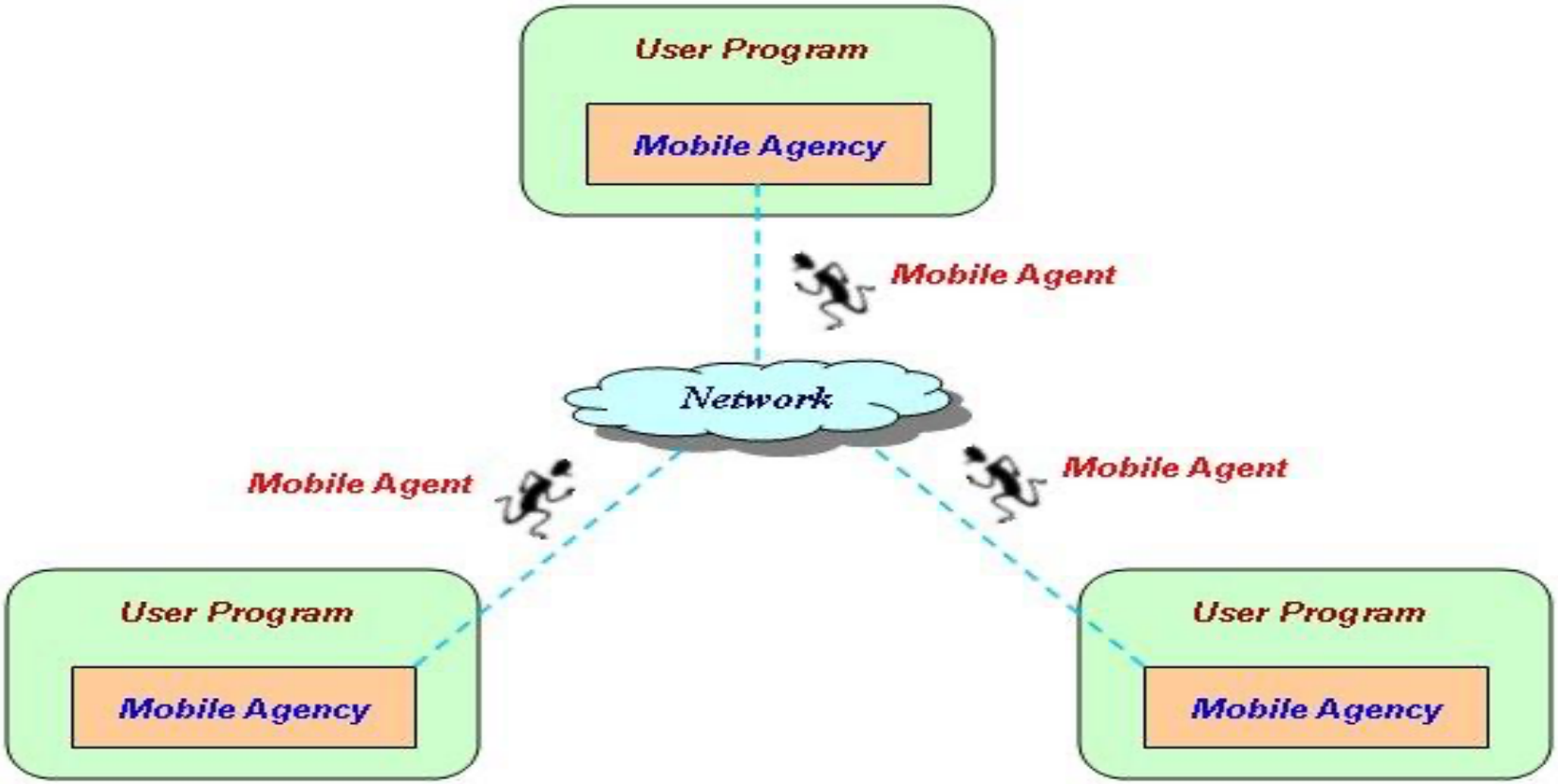
# Mobile Agents

# Mobile Agent



- A mobile agent is a process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment
- Just as a user directs an Internet browser to "visit" a website (the browser merely downloads a copy of the site or one version of it in the case of dynamic web sites), similarly, a mobile agent accomplishes a move through data duplication mobile agent is a specific form of mobile code.
- A mobile agent is a specific form of mobile code and mobile agents are active in that they can choose to migrate between computers at any time during their execution

# Mobile Agent



# Properties of Mobile Agent



- **Adaptive learning:** Mobile agents can learn from experiences and adapt themselves to the environment. They can monitor traffic in large networks and learn about the trouble spots in the network. Based on the experiences of the agent in the network the agent can choose better routes to reach the next host.
- **Autonomy:** Mobile agents can take some decisions on its own. For example, mobile agents are free to choose the next host and when to migrate to the next host. These decisions are transparent to the user and the decisions are taken in the interest of the user.
- **Mobility:** Mobile agents have the ability to move from one host to another in the network.

# Advantages of Mobile Agent



- Reduction in network load
- Overcome network latency
- Protocol encapsulation
- Asynchronous and autonomous execution
- Fault tolerance

# Disadvantages of Mobile Agent



- Security risk in using mobile agents
  - Malicious mobile agent can damage a host
  - A virus can be disguised as a mobile agent and distributed in the network causing damage to the host machines that execute the agent
  - Malicious host can tamper with the functioning of the mobile agent

# Thank You