Internet (ইন্টারনেট)

🔹 ইন্টারনেট আসলে কী?

ইন্টারনেট হলো:

- বিশ্বজুড়ে অসংখ্য ডিভাইসের
- কোটি কোটি রাউটার, সার্ভার, অপটিক ফাইবার লিঙ্কের
- Interconnected network

এই নেটওয়ার্কগুলো **BGP (Border Gateway Protocol)** নামের routing protocol ব্যবহার করে একে অপরের মধ্যে পথ ঠিক করে।

🔹 ইন্টারনেট কিভাবে চলে?

Internet Structure:

1) Tier-1 ISP

- Global-level providers
- Example: Level 3, Tata, AT&T
- এরা world-wide backbone নেটওয়ার্ক পরিচালনা করে

2) Tier-2 ISP

- Large regional ISP
- Example: Banglalink, GP, Airtel
- এরা Tier-1 থেকে bandwidth কিনে

3) Tier-3 ISP

- Local broadband provider
- তোমার বাসায় যেই লাইন আসে

- **Internet Data Flow**

  1. তুমি ব্রাউজারে google.com লিখলে
  2. DNS query যায় DNS সার্ভারে
  3. DNS → Google-এর public IP দেয়
  4. তোমার রাউটার থেকে ISP router
  5. ISP থেকে multiple backbone → Google data center
  6. সার্ভার উত্তর পাঠায়
  7. প্যাকেট ফিরে আসে একই বা ভিন্ন রুটে

Important Components:

- **DNS** → Domain → IP রূপান্তর
- **BGP** → Internet routing control করে
- **CDN (Cloudflare, Akamai)** → Content world-wide দ্রুত পৌঁছায়
- **Optical Fiber Backbone** → Undersea cables
- **IXP (Internet Exchange Point)** → ISPs interconnect হয়

ARP Protocol — Deep Explanation

ARP কী করে?

LAN-এর মধ্যে IP → MAC পাওয়ার একমাত্র উপায়।

ARP Message Types:

1. **ARP Request (Broadcast)**
   → Everyone listen! Who has 192.168.1.10?
2. **ARP Reply (Unicast)**
   → I am 192.168.1.10, my MAC is AA:BB:CC:DD:EE:FF

ARP Cache/Table:

OS এর RAM-এ নিচের মত স্টোর হয়:

192.168.1.1 -> 00:11:22:33:44:55 (valid 60 sec)

ARP Spoofing (Attack)

Attackers fake ARP Reply পাঠায়:

- Router's IP → Attacker's MAC
- Result = MITM attack
- Wireshark-এ দেখা যায়

ICMP Protocol — Deep Explanation

ICMP কোন Layer?

- **Layer 3 (Network Layer)**
- IP-এর ভিতরে encapsulated হয়

ICMP কিসের জন্য?

- Error reporting
- Network testing
- Diagnostic

Common ICMP Messages:

ICMP Type	Meaning
0	Echo Reply (ping reply)
8	Echo Request
3	Destination Unreachable
11	Time Exceeded
5	Redirect

ICMP Security Note:

অনেক firewall ICMP block করে:

- DoS attack হতে পারে
- Ping flood
- Smurf attack

IGMP Protocol — Deep Explanation

IGMP = Multicast Membership Management

Multicast IP range:
224.0.0.0 – 239.255.255.255

কেন multicast দরকার?

Unicast → 1:1
Broadcast → সবাই
Multicast → গ্রুপ-ভিত্তিক (efficient)

IGMP versions:

- **IGMPv1** – Basic join
- **IGMPv2** – Leave message
- **IGMPv3** – Source-specific multicast (SSM)

উদাহরণ:

IPTV → Channel join/leave
Video conference → group video

QUIC Protocol — Deep Explanation

QUIC = Fast Reliable connection over UDP

UDP ব্যবহার করে কিন্তু TCP-এর ফিচারগুলা রাখা হয়েছে।

QUIC-এর Features:

1. **Zero-RTT connection**
2. **Built-in TLS 1.3**
3. **No Head-of-Line Blocking**
4. **Connection migration**
   (WiFi → Mobile data switch হলেও connection break হয় না)

QUIC ব্যবহারকারীরা:

- HTTP/3 এ QUIC ব্যবহার বাধ্যতামূলক
- Google, Facebook, Cloudflare, YouTube

Ping Protocol — Deep Explanation

Ping = ICMP Echo Request/Reply.

Ping কি মাপতে পারে?

- RTT (Round Trip Time)
- Jitter
- Packet loss
- DNS resolution
- Network reachability

Example Output:

64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=32.1 ms

MAC Address — Deep Explanation

MAC structure (48-bit)

- 1st 24-bit → Manufacturer (OUI)
- Last 24-bit → Device serial

Example:

FC:FB:FB:01:02:03

- FC:FB:FB → Apple
- Rest → Device specific

MAC Filtering:

WiFi security → Allow list / Block list

MAC Spoofing:

Kali Linux:

```
ifconfig wlan0 down
macchanger -r wlan0
ifconfig wlan0 up
```

Network Devices — Full Deep Explanation

Hub

- Pure physical layer device (Layer 1)
- Broadcasts all data
- No MAC table
- Collision domain = 1
- Very insecure
- Uses CSMA/CD

Switch

Layer 2 device (sometimes Layer 3)

Switch Features:

- MAC table
- VLAN
- STP (Spanning Tree Protocol)

- Trunking (802.1Q)
- EtherChannel (Port aggregation)
- QoS
- ARP Inspection
- DHCP Snooping

Switch frames forwarding:

1. Reads MAC
2. Checks table
3. Forward/Filter/Flood

Router

Layer 3 device।

Router Features:

- Routing (static/dynamic)
- NAT/PAT
- DHCP server
- Firewall
- VPN termination
- Inter-VLAN routing

Routing Protocols:

- **IGP**: OSPF, EIGRP, RIP
- **EGP**: BGP

Bridge

Switch-এর পুরনো ভার্সন।

কাজ:

- Collision domain ভাগ করে
- MAC filtering
- Slow, replacing by switches

Repeater

Layer 1 device
Signal regenerate করে
Range বাড়ায়
Used in fiber, WiFi boosters

Gateway

Protocol converter:

উদাহরণ:

- VoIP gateway (SIP → PSTN)
- Payment gateway
- IoT gateway

Access Point

WiFi network তৈরি করে।

Types:

- Standalone AP
- Controller-based AP
- Mesh AP

Features:

- WPA2/WPA3 encryption
- WiFi 6/6E
- SSID broadcasting

- Channel selection
- Band steering
- Load balancing

Modem

Modulator + Demodulator
ISP line → Router

Types:

- DSL modem
- Cable modem
- Fiber ONT (GPON, EPON)

Synchronous & Asynchronous Data Transmission

🔹 **Synchronous Transmission**

ডাটা পাঠানো হয় **clock signal অনুযায়ী**, অর্থাৎ sender–receiver-এর মধ্যে timing match থাকে।

বৈশিষ্ট্য:

- Continuous data stream
- Fast transmission
- Clock sync প্রয়োজন
- Used in: LAN, High-speed networks, DDR RAM, USB

Diagram (Conceptual):

Clock: | | | | | | |

Data : 1 0 1 1 0 0 1

- **Asynchronous Transmission**

ডাটা পাঠানো হয় **bit-by-bit** ভিত্তিতে।
Start bit + Stop bit দিয়ে ডাটা বোঝায়।

বৈশিষ্ট্য:

- No clock sync needed
- Slower
- Low-cost
- Used in: Keyboard, Mouse, Serial comm (RS-232)

Diagram:

Start | Data Bits | Stop

0 10101 1

- **Difference Table**

Feature	Synchronous	Asynchronous
Clock	Required	Not required
Speed	Fast	Slow
Cost	High	Low
Data flow	Stream	Byte-by-byte
Examples	USB, DDR, LAN	Keyboard, Serial port

Simplex, Half Duplex, Full Duplex

- **Simplex**

ডাটা শুধু **এক দিক** দিয়ে যায়।

উদাহরণ:

- TV broadcasting
- Fire alarm system

Diagram:

A → B

🔹 **Half Duplex**

ডাটা দুই দিকেই যায়, কিন্তু **একসময় এক দিক**।

উদাহরণ:

- Walkie-Talkie
- Old wireless systems

Diagram:

A ↔️ B (not simultaneously)

🔹 **Full Duplex**

ডাটা দুই দিকেই যায় **একসাথে**।

উদাহরণ:

- Phone call
- Modern Computers
- Ethernet switches

Diagram:

A ⇄ B (simultaneously)

- **Difference Table**

Mode	Direction	Example
Simplex	One-way	TV
Half Duplex	Both-way (not same time)	Walkie-talkie
Full Duplex	Both-way (same time)	Phone call

IP Addressing (IPv4 & IPv6)

- **IPv4 (32-bit)**
  - Length: **32-bit**
  - Format: Decimal
  - Example: **192.168.1.10**
  - Total addresses: 4.3 billion

IPv4 Classes:

Class	Range	Use
A	1–126	Large networks
B	128–191	Medium networks
C	192–223	Small networks
D	224–239	Multicast
E	240–255	Experimental

- **IPv6 (128-bit)**
  - Length: **128-bit**
  - Format: Hexadecimal
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- Total addresses: **340 undecillion**
- Auto-configuration supported (SLAAC)

Features of IPv6:

- No NAT required
- Built-in IPsec
- Hierarchical addressing
- Faster routing
- No broadcast (only multicast & anycast)

Subnetting — Full Explanation

Subnetting = বড় নেটওয়ার্ককে ছোট ছোট নেটওয়ার্কে ভাগ করা।

কেন Subnetting করা হয়?

- IP save করা
- Network management সহজ
- Security বাড়ে
- Network performance বাড়ে

Subnetting Example:

Given:
192.168.1.0/24 → 256 total IPs

If you divide into 2 subnets:

1. 192.168.1.0/25
2. 192.168.1.128/25

Each subnet contains:

- 128 IP
- Usable = 126
- Broadcast = last IP

Supernetting — Full Explanation

Supernetting = ছোট network → বড় network combine করা।
Also called **Route Aggregation**.

Used by ISPs, BGP routing.

Example:

Combine:

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

→ Supernet becomes:
192.168.0.0/22

CIDR Notation — Full Explanation

CIDR = Classless Inter-Domain Routing
Format → **IP/prefix**

Example:

- 192.168.1.0/24
- 10.0.0.0/8

Prefix length says how many bits = network portion.

Some Important CIDR blocks:

CIDR	Total IP	Usable
/8	16,777,216	huge
/16	65,536	medium
/24	256	small
/30	4	point-to-point
/32	1	host route

OSI Model — Full Explanation

OSI = Open Systems Interconnection

Total: **7 Layers**

Layer	Name	Function	Example
7	Application	User interface	HTTP, DNS
6	Presentation	Data format, encryption	SSL/TLS
5	Session	Connection control	Session keys
4	Transport	Reliable delivery	TCP/UDP
3	Network	Routing	IP
2	Data Link	MAC addressing	Switch
1	Physical	Bits, signals	Cable, Hub

TCP/IP Model — Full Explanation

4-layer model:

TCP/IP Layer	OSI Equivalent	Examples
Application	5,6,7	HTTP, FTP, DNS
Transport	4	TCP, UDP
Internet	3	IP, ICMP
Network Access	1,2	Ethernet, WiFi

Well-Known Ports and Their Works

এগুলো হলো Standard Ports যেগুলো নির্দিষ্ট সার্ভিসের জন্য ব্যবহৃত হয়।

Most Important Ports (Table)

Port	Protocol	Service	কাজ
20/21	TCP	FTP	File transfer
22	TCP	SSH	Secure remote login
23	TCP	Telnet	Unsecure remote login
25	TCP	SMTP	Email sending
53	TCP/ UDP	DNS	Name resolution
67/68	UDP	DHCP	IP assign করা
69	UDP	TFTP	Simple file transfer
80	TCP	HTTP	Web browsing
110	TCP	POP3	Receive email
123	UDP	NTP	Time sync
143	TCP	IMAP	Email retrieve
161/162	UDP	SNMP	Network monitoring
389	TCP/ UDP	LDAP	Directory services
443	TCP	HTTPS	Secure browsing
445	TCP	SMB	File sharing (Windows)
514	UDP	Syslog	Logging
5060	UDP/ TCP	SIP	VoIP
8080	TCP	HTTP Proxy	Web proxy

TCP & UDP Protocol (When, Where, How They Send Data)

🔹 **TCP (Transmission Control Protocol)**

✔️ **TCP কোথায় ব্যবহার হয়?**

যেখানে **reliable**, **error-free**, **ordered** data দরকার:

- Web browsing (HTTPS)
- Email
- File transfer (FTP)
- Remote login (SSH)
- Database communication

✔️ **TCP কিভাবে ডাটা পাঠায়?**

- Connection-oriented
- 3-way handshake দিয়ে শুরু
- Ordered delivery
- Lost packet retransmit করে
- Flow control (Windowing)
- Congestion control

TCP ensures:
➡️ Data MUST reach
➡️ Data MUST be in order
➡️ No corruption allowed

🔹 **UDP (User Datagram Protocol)**

✔️ **UDP কোথায় ব্যবহার হয়?**

যেখানে **speed গুরুত্বপূর্ণ**, reliability না:

- Video streaming
- Online gaming
- VoIP call
- DNS
- Live broadcasting

✔️ **UDP কিভাবে ডাটা পাঠায়?**

- Connectionless
- No handshake
- No guarantee
- Very fast
- Lightweight packets

UDP ensures:
➡️ Speed
➡️ Low latency
➡️ Broadcasting possible

🔹 **Difference Table**

Feature	TCP	UDP
Connection	Yes	No
Speed	Slow	Fast
Reliability	High	Low
Ordering	Guaranteed	Not guaranteed
Use cases	Web, Email	Gaming, Live stream

TCP 3-Way Handshake (Connection Establishment)

TCP connection establish করার জন্য তিনটি ধাপ থাকে:

Client ---- SYN ---> Server

Client <--- SYN/ACK --- Server

Client ---- ACK ---> Server

- **Step-by-step:**
  1. **SYN**
     Client বলে: “I want to connect.”
  2. **SYN + ACK**
     Server বলে: “I’m ready. You can connect.”
  3. **ACK**
     Client বলে: “Okay, connection established.”

এটাই secure, reliable TCP connection শুরু হওয়ার পদ্ধতি।

TCP 4-Way Handshake (Connection Termination)

TCP connection বন্ধ করার ৪ ধাপ থাকে:

Client ---- FIN ---> Server

Client <--- ACK ---- Server

Client <--- FIN ---- Server

Client ---- ACK ---> Server

- **Step-by-step:**
  1. Client → FIN
  2. Server → ACK
  3. Server → FIN
  4. Client → ACK

Connection closes from both sides.

TCP Flags (SYN, ACK, FIN, RST, PSH, URG)

TCP packet header-এ 6টি main flags থাকে।

Flag	Meaning	কাজ
SYN	Synchronize	Connection start
ACK	Acknowledgement	Packet received confirm
FIN	Finish	Connection close
RST	Reset	Forcefully close
PSH	Push	Urgent send (buffer bypass)
URG	Urgent	High priority packets

Example:

- SYN = handshake start
- SYN + ACK = handshake accept
- FIN = close request
- RST = sudden termination

HTTP Methods (GET, POST, PUT, PATCH, TRACE, HEAD, OPTIONS)

এগুলো ওয়েব সার্ভারে বিভিন্ন উদ্দেশ্যে request পাঠায়।

Table with Full Explanation

Method	Use	Works
GET	Data read	URL-এ ডাটা দেখা যায়
POST	Data submit	Form submission, login
PUT	Replace data	Full update
PATCH	Partial update	ছোট অংশ modify
DELETE	Remove data	Record delete
HEAD	Headers only	Resource exists কিনা দেখা
OPTIONS	Allowed methods	Server কোন HTTP methods সাপোর্ট করে
TRACE	Loopback test	Debugging request path

🔹 **Short Explanation:**

GET

- Only retrieve data
- Visible in URL
- Not secure for passwords

POST

- Secure
- Body-তে data যায়
- Login, signup, upload

PUT

- Entire record replace করে

PATCH

- Only selected fields modify

HEAD

- GET এর মতো কিন্তু body ছাড়া

OPTIONS

- Check allowed methods (CORS)

TRACE

- Security risk, often disabled

DNS (Domain Name System)

DNS হলো **ইন্টারনেটের ফোনবুক**।
এটি **ডোমেইন নাম → IP address**-এ রূপান্তর করে।

উদাহরণ:

google.com → 142.250.190.78

facebook.com → 157.240.200.35

DNS কাজের ধাপ

1. User টাইপ করে: google.com
2. Browser sends DNS query
3. Resolver → Root server
4. Root → TLD server (.com)
5. TLD → Authoritative DNS
6. Authoritative DNS IP পাঠায়
7. Browser সার্ভারে connect করে

DNS Record Types:

Type	কাজ
A	IPv4 address
AAAA	IPv6 address
CNAME	Alias name
MX	Mail server
TXT	Verification
NS	Nameserver
PTR	Reverse DNS

DHCP (Dynamic Host Configuration Protocol)

DHCP স্বয়ংক্রিয়ভাবে ডিভাইসকে নেটওয়ার্ক সেটিং দেয়।

DHCP দেয়:

- IP Address
- Subnet Mask
- Gateway
- DNS Server
- Lease Time

DHCP কাজের চার ধাপ (DORA):

1. Discover
2. Offer
3. Request
4. Acknowledge

FTP, TFTP, SFTP, SCP

- FTP (File Transfer Protocol)
  - Port: 20/21
  - Unsecure
  - File upload/download
  - Used in legacy systems
- TFTP (Trivial FTP)
  - Port: 69
  - No authentication
  - Fast & lightweight
  - Used in: Booting routers, PXE boot
- SFTP (SSH File Transfer Protocol)
  - Port: 22
  - Secure (SSH-based)
  - Used in: Secure file transfers
- SCP (Secure Copy Protocol)
  - Port: 22
  - Works over SSH
  - Very fast secure copy

SSH & Telnet

- **Telnet**
  - Port: 23
  - Plain text
  - Not secure
  - Used only for testing
- **SSH (Secure Shell)**
  - Port: 22
  - Encrypted remote login
  - Used by admins, hackers, servers

SSH = Most secure remote control method.

SMTP, POP3, IMAP

- **SMTP (Simple Mail Transfer Protocol)**
  - Port: 25
  - Emails **send** করতে ব্যবহৃত হয়।
- **POP3 (Post Office Protocol v3)**
  - Port: 110
  - Email **download** করে device-এ রাখে
  - Server থেকে mail delete হয় (mostly)
- **IMAP (Internet Message Access Protocol)**
  - Port: 143
  - Emails sync করে
  - Server-এ কপি থাকে
  - Used in modern devices

SNMP (Simple Network Management Protocol)

Network monitoring-এর জন্য ব্যবহৃত হয়।

SNMP কী মনিটর করে?

- Router status
- CPU usage
- Bandwidth
- Interface up/down
- Errors
- Traffic graphs

SNMP Ports:

- **161** → Queries
- **162** → Traps (alerts)

NTP (Network Time Protocol)

- Port: **123 (UDP)**
- Time synchronization করে
- সব সার্ভার/ডিভাইসকে একই সময় দেয়

Example:
Google NTP → time.google.com

SMB, LDAP, RDP

🔹 **SMB (Server Message Block)**

- Port: **445**
- Windows File Sharing

- Used for:
    - File share
    - Printer share
    - Windows AD communication
- Attacks: EternalBlue, WannaCry

🔹 **LDAP (Lightweight Directory Access Protocol)**

- Port: **389**
- Directory data store & authentication
- Used by Active Directory (AD)

🔹 **RDP (Remote Desktop Protocol)**

- Port: **3389**
- Windows remote access
- Graphical remote control
- Used by admins & attackers

NAT & PAT (Network and Port Address Translation)

🔹 **NAT (Network Address Translation)**

Private IP → Public IP
Used in routers.

উদাহরণ:

192.168.1.10 → 203.0.113.5

🔹 **PAT (Port Address Translation)**

Many private devices → One public IP
But mapped by **port**.

Example:

192.168.1.10:5050 → 203.0.113.5:30001

192.168.1.11:5050 → 203.0.113.5:30002

PAT = NAT Overload

Used in home routers.

Firewalls & CDN

🔹 **Firewall**

Firewall traffic ফিল্টার করে।

Firewall filters:

- IP
- Port
- Protocol
- Application
- URL
- Content

Types:

- Packet filtering
- Stateful firewall
- Proxy firewall
- Next-generation firewall (NGFW)

🔹 **CDN (Content Delivery Network)**

CDNs world-wide content দ্রুত পৌঁছায়।

কাজ:

- Caching
- DDoS protection
- Load balancing
- Low latency

Examples:

- Cloudflare
- Akamai
- Fastly

VPN (SSL, IPsec, PPTP, L2TP)

- **SSL VPN**
  - Works through HTTPS (443)
  - User-friendly
  - Used for remote workers
- **IPsec VPN**
  - Most secure
  - Works at network layer
  - Used for site-to-site VPN
- **PPTP**
  - Old
  - Weak encryption
  - Not recommended
- **L2TP/IPsec**
  - Combination of L2TP + IPsec
  - Secure + stable
  - Used widely in enterprises

TLS (Transport Layer Security)

TLS = HTTPS নিরাপত্তার মূল প্রযুক্তি।

TLS কী করে?

- Data encrypt করে
- Authentication দেয়
- Integrity নিশ্চিত করে
- Man-in-the-middle আক্রমণ ঠেকায়

TLS versions:

- TLS 1.0 → Deprecated
- TLS 1.2 → Standard
- TLS 1.3 → Fastest + Most Secure

Netstat & Traceroute

🔹 **Netstat**

Netstat = "Network Statistics"
এটি দিয়ে সিস্টেমে কি কি connections active আছে তা দেখা যায়।

Netstat কী দেখায়?

- Active TCP/UDP connections
- Listening ports
- Established connections
- Routing table
- Network interfaces

Common netstat outputs:

netstat -tulnp

Flag	Meaning
-t	TCP
-u	UDP
-l	Listening ports
-n	Show numeric IP/ports
-p	Show process using the port

- **Traceroute**

Traceroute দেখায় **একটি packet গন্তব্যে পৌঁছাতে কতগুলি রাউটার (hop) পেরোয়**।

Traceroute কীভাবে কাজ করে?

Traceroute ICMP ব্যবহার করে TTL (Time To Live) বাড়াতে বাড়াতে packet পাঠায়:

- TTL=1 → 1st router reply
- TTL=2 → 2nd router reply
- TTL=3 → 3rd router reply

এভাবে পুরো পথ দেখা যায়।

Command:

traceroute google.com

Encryption Protocols (WEP, WPA, WPA2, WPA3)

- **WEP (Wired Equivalent Privacy)**
  - খুব দুর্বল
  - RC4 encryption
  - সহজে ভাঙা যায়
  - এখন আর ব্যবহার হয় না

- **WPA (Wi-Fi Protected Access)**
  - WEP থেকে ভালো
  - TKIP ব্যবহার করে
  - দুর্বল, WPS আক্রমণে ভাঙা যায়
- **WPA2**
  - সবচেয়ে বেশি ব্যবহৃত
  - AES-CCMP encryption
  - শক্তিশালী নিরাপত্তা
- **WPA3**
  - নতুন স্ট্যান্ডার্ড
  - SAE (Simultaneous Authentication of Equals)
  - KRACK থেকে immune
  - বেশি security, harder to crack

3. Wireless Authentication (PSK, Enterprise)

- **WPA/WPA2 PSK (Pre-Shared Key)**
  - Password দিয়ে WiFi connect হয়
  - Home networks-এর জন্য
  - Everyone uses same key
- **WPA Enterprise (802.1X)**
  - Username + password required
  - RADIUS server authentication
  - Corporate/office network-এ ব্যবহৃত

PSK vs Enterprise Table:

Feature	PSK	Enterprise
Key	Shared	Per-user
Security	Medium	High
Use	Home	Company

Wireless Attacks (Deauth, Evil Twin, KRACK)

- **1) Deauthentication Attack**
  - WiFi থেকে ইউজারকে ডিসকানেক্ট করে
  - Attack tool: aireplay-ng
  - Purpose: Handshake capture (WPA/WPA2 cracking)
- **2) Evil Twin Attack**
  - Fake WiFi access point তৈরি করা
  - Victim connect হলে তার ট্রাফিক attacker দেখে
  - Used for: MITM, credential stealing
- **3) KRACK Attack**
  - WPA2 handshake vulnerability
  - Replay attack
  - Attacker encrypted ট্রাফিকও পড়তে পারে

ARP Spoofing / ARP Poisoning

ARP Spoofing = attacker নিজের MAC address-কে gateway বা victim-এর IP-এর সাথে bind করে।

ফলাফল:

- MITM attack
- Data sniffing
- Session hijacking
- DNS spoofing possible

Concept:

Attacker: "I am the gateway"

Victim → sends packets to attacker

Tools: ettercap, bettercap, arpspoof

DNS Spoofing

DNS spoofing = attacker fake DNS response পাঠায় যাতে victim ভুল IP-তে যায়।

Example:

facebook.com → 192.168.1.50 (attacker server)

Used for:

- Phishing
- Redirection
- MITM attacks

IP Spoofing

Attacker fake source IP ব্যবহার করে packet পাঠায়।

Uses:

- Hiding identity
- SYN flood attack
- Bypassing IP filtering
- Smurf attack

Since IP spoofing changes source IP, victim reply wrong host.

MAC Flooding

Switch-এর MAC table flood করা হয় random MAC দিয়ে।

Effect:

- Switch becomes full
- Switch turns to **hub mode** (broadcast everything)
- Attacker can sniff traffic

Tool: macof (from Dsniff)

DHCP Starvation

Attacker অনেক fake DHCP requests পাঠায়, DHCP server-এর IP pool শেষ হয়ে যায়।

Result:

- Legit users get no IP
- Attacker starts Rogue DHCP server

Used for:

- MITM
- Redirection attack

Tools: Yersinia

SYN Flood / DoS / DDoS

- **SYN Flood**

Attacker প্রচুর SYN পাঠায় server-এ
Server SYN/ACK পাঠায়
Client ACK কখনো পাঠায় না

Result:

- Server half-open connection table পূর্ণ
- Server freeze / crash

- **DoS**

Single attacker → target down করে।

- **DDoS**

Many attackers → huge traffic → server down
Uses botnets (Mirai, Zeus)

MITM (Man-in-the-Middle)

MITM = attacker দুই পক্ষের মাঝখানে থেকে ডাটা change বা capture করে।

MITM techniques:

- ARP Spoofing
- DNS Spoofing
- Evil Twin
- HTTPS downgrade attack
- SSL stripping

What attacker can do?

- Read traffic
- Modify traffic
- Inject malware
- Hijack sessions

Sniffing & Eavesdropping

- **Sniffing**

Sniffing মানে নেটওয়ার্কের মধ্যে চলাচল করা ডাটা capture করা।

Passive Sniffing

- Network listen করে
- Victim বুঝে না
- Switch networks-এ কঠিন

Active Sniffing

- Attacker actively packet manipulate করে
- ARP Spoofিং
- MAC Flooding
- DHCP Spoofing

Tools:

- Wireshark
- tcpdump
- tshark
- Ettercap / Bettercap

🔹 **Eavesdropping**

Eavesdropping = গুপ্তভাবে কথা শোনা।

নেটওয়ার্কে:

- HTTPS না থাকলে attacker ডাটা পড়তে পারে
- যেমন: username/password

এটা sniffing-এরই কোভার্ট ফর্ম।

Replay Attacks

Attacker কোনো বৈধ প্যাকেট **capture করে** আবার **resend করে**।

উদাহরণ:

- Login request capture → পরে পাঠানো
- Payment request replay
- Authentication token reuse

প্রতিরোধ:

- Time-stamps
- Nonce
- TLS/HTTPS

Session Hijacking

Attacker একটি active session দখল করে নেয়।

ধাপ:

1. Attacker session cookie sniff করে
2. Cookie ব্যবহার করে victim-এর account takeover

Types:

- **Active hijacking:** attacker packet modify করে
- **Passive hijacking:** শুধু session পড়ে
- **Cookie hijacking:** session id চুরি

Tools:

- Burp Suite
- Bettercap
- Wireshark

ICMP Flood / Ping of Death / Smurf Attack

- **ICMP Flood**

Attacker সার্ভারকে অনেক ICMP Echo (ping) পাঠায়।

Result:

- Server CPU overload
- ICMP stack ব্যস্ত হয়ে যায়
- DoS ঘটে

- **Ping of Death**
  - Huge ICMP packet পাঠিয়ে system crash করা
  - Old OS vulnerable ছিল
  - Modern OS patched
- **Smurf Attack**
  - Attacker → broadcast address-এ ICMP পাঠায়
  - Source IP spoof করে victim-এর
  - Network → সব reply victim-এ পাঠায়
  - Victim overloaded হয়ে যায়

VLAN Hopping

Attacker এক VLAN থেকে অন্য VLAN-এ access পায়।

Techniques:

1. **Switch Spoofing**
   - Attacker নিজের ডিভাইসকে Trunk port-এর মতো behave করায়
2. **Double Tagging**
   - Double 802.1Q tag ব্যবহার করে VLAN bypass

Prevent:

- Disable DTP
- Set all ports to access
- Use VLAN pruning

Rogue DHCP & Evil Twin

🔹 **Rogue DHCP**

Attacker fake DHCP server বানায়।

Result:

- Victim wrong gateway পায়
- Traffic attacker-এর কাছে যায়
- MITM possible
- DNS spoofing possible

🔹 **Evil Twin**

Fake WiFi Access Point বানানো।

Works:

- Victim thinks it's real
- Connects
- Attacker sniffs + controls traffic

Routing Attacks

Routing protocol manipulate করার আক্রমণ।

Types:

1) Route Injection

- Fake route advertise করা
- Traffic attacker-এর দিকে reroute

2) Blackhole Attack

- Traffic drop করে

3) Routing Table Poisoning

- Wrong entries দিয়ে routing নষ্ট করা

Protocols targeted:

- OSPF
- BGP
- RIP

SSL Stripping

HTTPS → HTTP করে ফেলা (downgrade attack)।

কাজ:

1. Victim → HTTPS request
2. Attacker intercept করে
3. Server-এর সাথে HTTPS
4. Victim-এর সাথে HTTP
5. Attacker সব data পড়ে + পরিবর্তন করতে পারে

Used in WiFi MITM attacks.

Tools:

- sslstrip
- Bettercap
- Burp Suite

Port Scanning Detection & Prevention

- **Detection:**
  - IDS/IPS (Snort, Suricata)
  - Firewall logs
  - Unusual SYN packets
  - nmap fingerprinting detection
- **Prevention:**
  - Firewall rules tighten
  - SYN cookies enable
  - Port knocking
  - Disable unused ports
  - Rate limiting

Pivoting Through Networks

Pivoting = এক ডিভাইস compromise করার পর সেখান থেকে **অন্য নেটওয়ার্ক/ডিভাইসে প্রবেশ**।

Techniques:

- SSH Tunneling
- Meterpreter pivot route
- SOCKS proxy
- Proxychains
- VPN pivot

Example:

Attacker → Compromised PC → Internal Servers

Used in post-exploitation.

Traffic Redirection & Tunneling

🔹 Traffic Redirection

Attacker network traffic অন্য জায়গায় পাঠায়:

- DNS Spoofing
- ARP Poisoning
- Route Injection

🔹 Tunneling

এক প্রোটোকলের ভিতরে আরেক প্রোটোকল লুকানো।

Examples:

- SSH Tunnel
- HTTP Tunnel
- ICMP Tunnel
- DNS Tunnel

Used to bypass firewalls.

Reverse Shells & Bind Shells

🔹 Reverse Shell

Victim attacker-কে connect করে।
(Easiest to bypass firewall)

Victim → Attacker listener

Used in:

- Metasploit
- Netcat
- Python payloads

- **Bind Shell**

Victim machine একটি port খুলে, attacker সেখানে connect করে।

Attacker → Victim open port

Harder to bypass firewall (needs open port).