Module 4
Networking Basics

Ansh Bhawnani

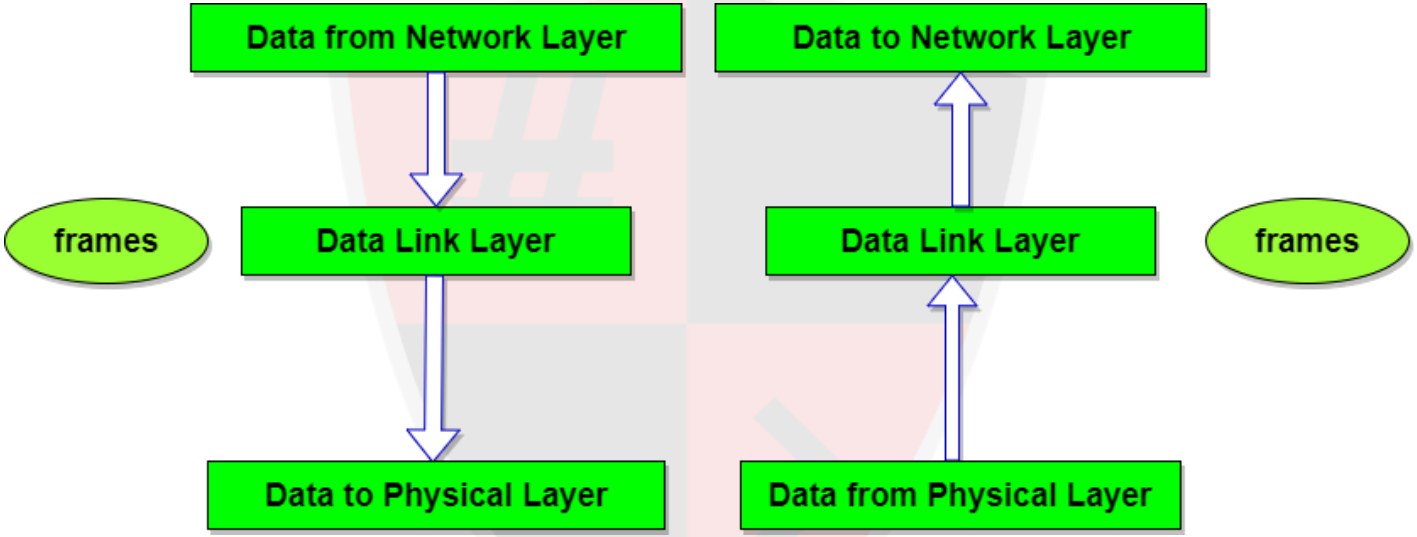
Data Link Layer:
MAC Addresses

Module 4

Data Link Layer

- Data link layer works between two hosts which are directly connected in some sense, point to point or broadcast
- Responsible for converting data stream to signals bit by bit and to send that over the underlying hardware
- At the receiving end, it picks up data from hardware as electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data Link Layer



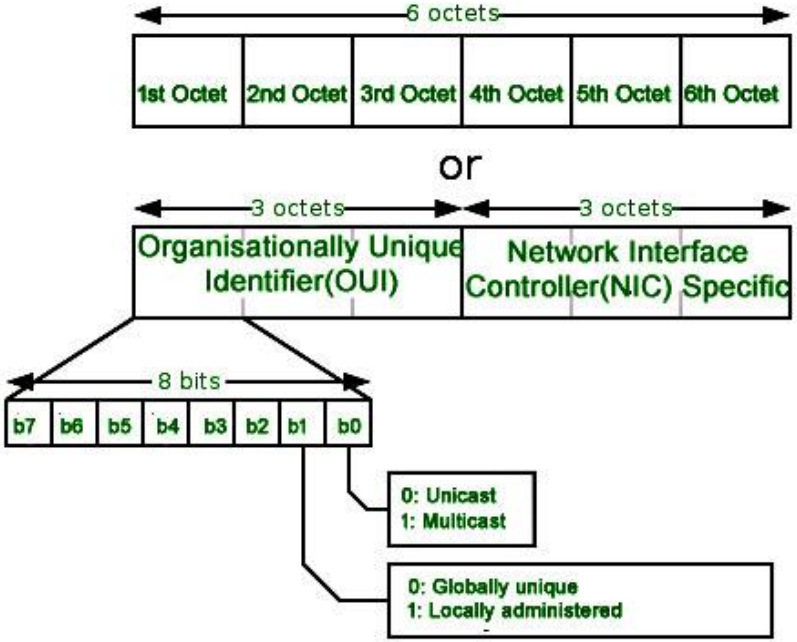
MAC Addresses

- Media Access Control
- In order to communicate or transfer the data from one computer to another computer we need MAC Address.
- MAC Addresses are unique **48-bits** hardware number, embedded into network card (known as **Network Interface Card**)
- World wide unique

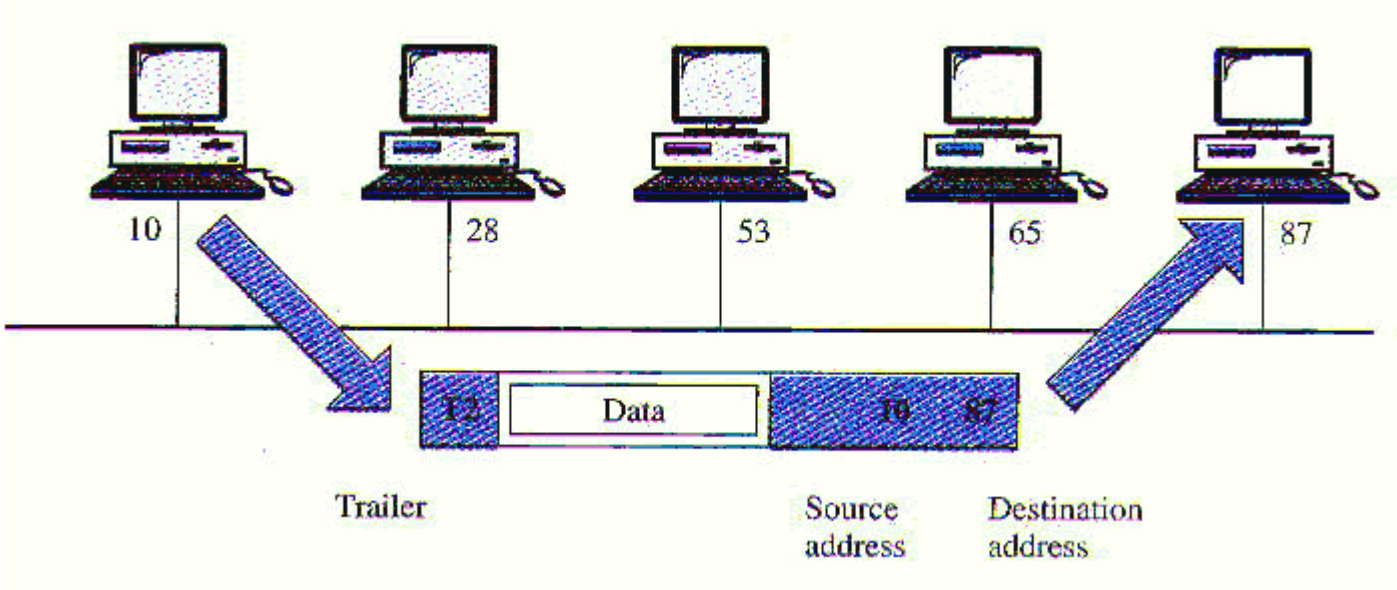
MAC Addresses

- Format of MAC Address:
  - 12-digit hexadecimal number (6-Byte binary number)
  - First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**), assigned by IEEE.
  - The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.
  - E.g. 01-80-C2-FF-E5-A1

MAC Addresses



Node to Node delivery

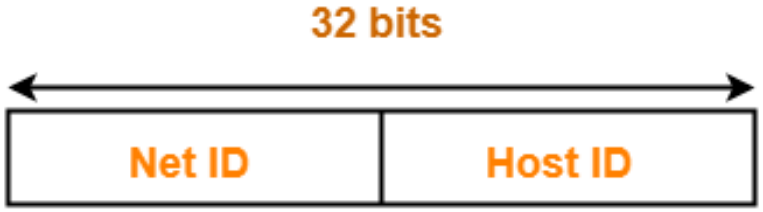


Network Layer: Types of IPv4 Addresses

Module 4

Types of IPv4 Addresses

- There are two parts of an IP Address:
  - Network Part
  - Host part



Format of an IP Address

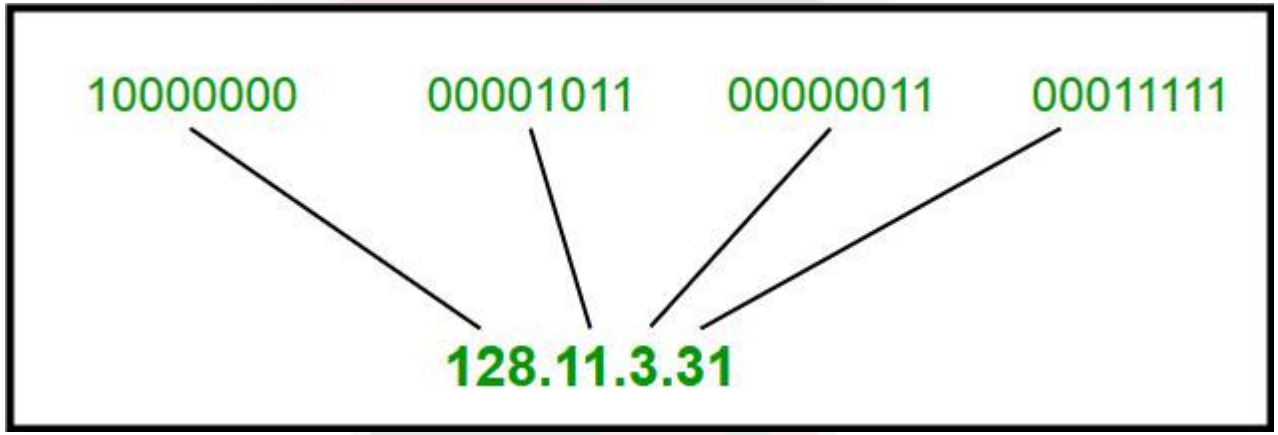
Types of IPv4 Addresses

- **Network Part**
  - Contains the **network ID**
  - Identifies which network you're on
- **Host Part**
  - Used to identify hosts (any device requiring a Network Interface Card, such as a PC or networked printer) on the network

Types of IPv4 Addresses

- **An IP Address can be represented as**
  - Dotted decimal notation: 192.168.1.1
  - Binary Notation: 11000000.10101000.00000001.00000001
  - Hexadecimal Notation: C0A80101
- With 32 bits, we have an address space of 2^32=4,294,967,296
- We separate and allocate some bits to the network part and remaining to the host part

Types of IPv4 Addresses



Classful Addressing

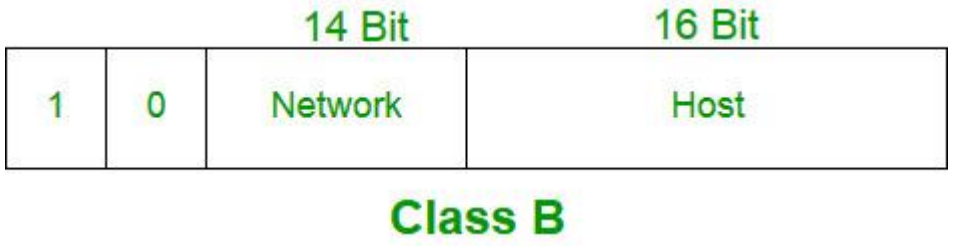
Class A

- Net ID: 8 bits
- Host ID: 24 bits
- First bit of first octet always set to 0
- Number of networks: 2^7-2 = 126
- Number of hosts: 2^24-2 = 16,777,214
- Used by very large organizations or government

Classful Addressing

Class B

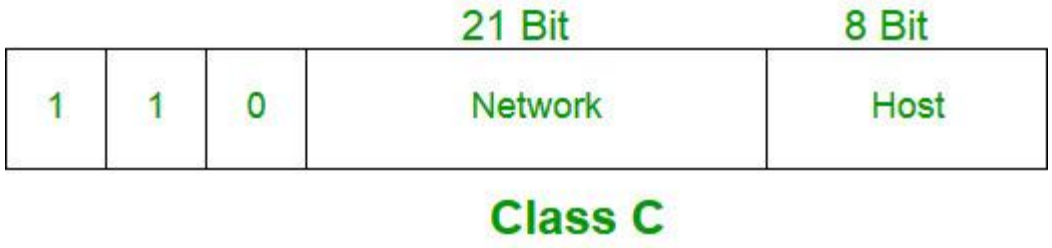
- Net ID: 16 bits
- Host ID: 16 bits
- First two bit of first octet are 10
- Number of networks: 2^14 = 16384
- Number of hosts: 2^16-2 = 65534
- Used by large or medium sized companies



Classful Addressing

Class C

- Net ID: 24 bits
- Host ID: 8 bits
- First three bit of first octet are 110
- Number of networks: 2^21 = 2097152
- Number of hosts: 2^8-2 = 254
- Used by small companies or domestic

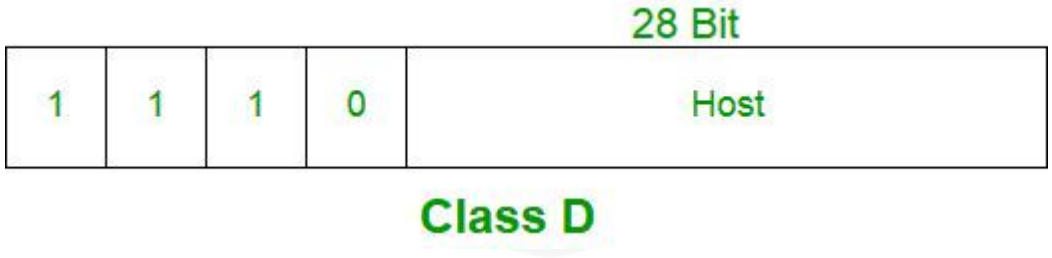


Class C

Classful Addressing

Class D

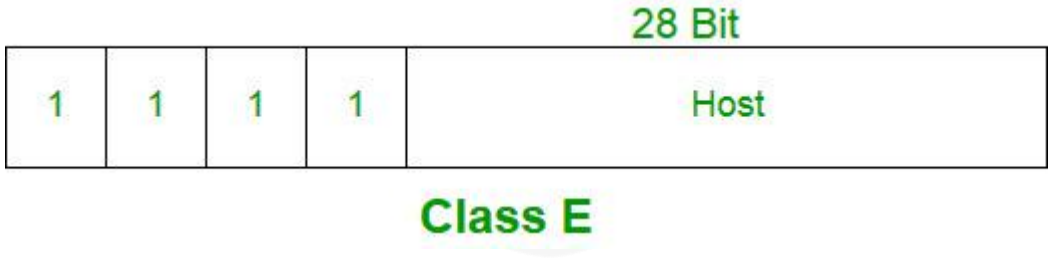
- Reserved for multicasting
- Network and host IDs not applicable
- First four bit of first octet are 1110
- Range: 224.0.0.0 – 239.255.255.255.



Classful Addressing

Class E

- Reserved for experimental and research purposes
- Network and host IDs not applicable
- First four bit of first octet are 1111
- Range: 240.0.0.0 – 255.255.255.254.



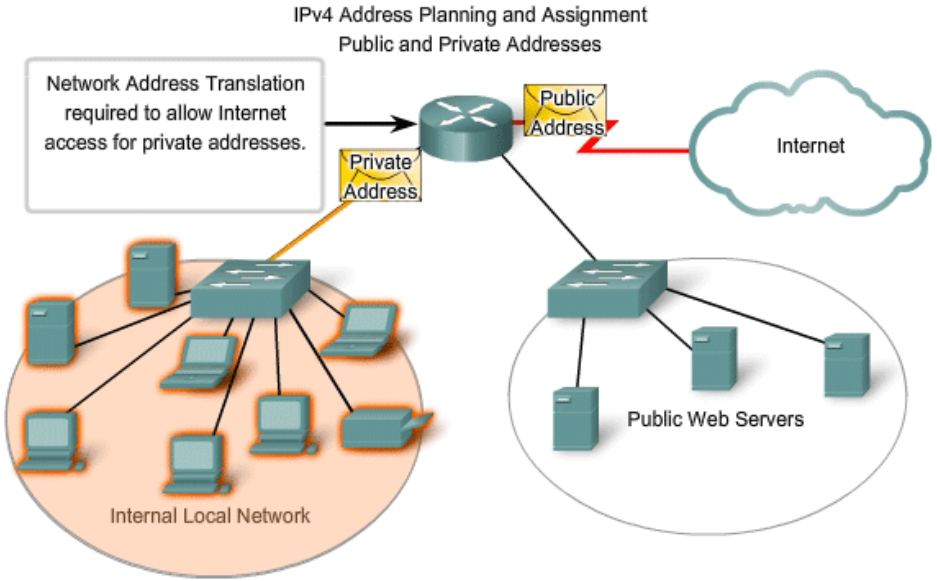
Classful Addressing

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Classful Addressing

- **Private IP blocks**
  - IANA has reserved some blocks to be used in private networks
  - Private IPs are non-routable.
- Class C: **192.168.0.0 - 192.168.255.255** (65,536 IP addresses)
- Class B: **172.16.0.0 - 172.31.255.255** (1,048,576 IP addresses)
- Class A: **10.0.0.0 - 10.255.255.255** (16,777,216 IP addresses)

Types of IPv4 Addresses



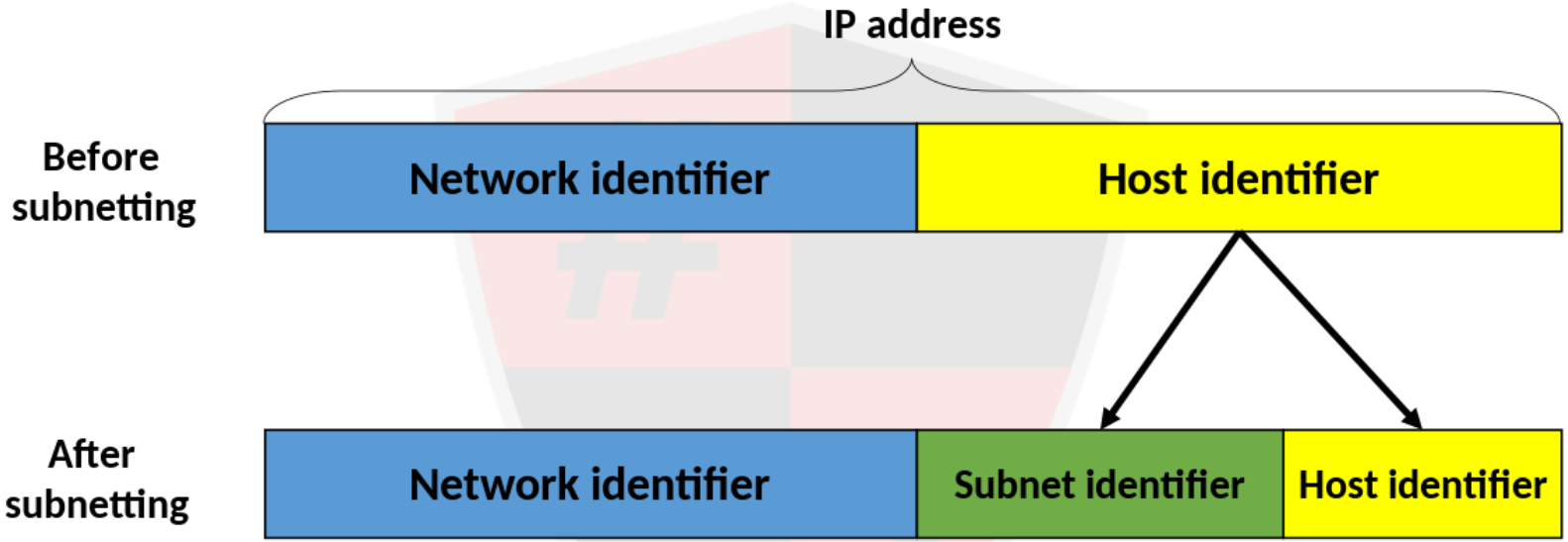
Types of IPv4 Addresses

- **Other special addresses**
  - **169.254.0.0 – 169.254.0.16** : Link local addresses
  - **127.0.0.0 – 127.255.255.255** : Loop-back addresses
  - **0.0.0.0 – 0.0.0.8** : used to communicate within the current network.

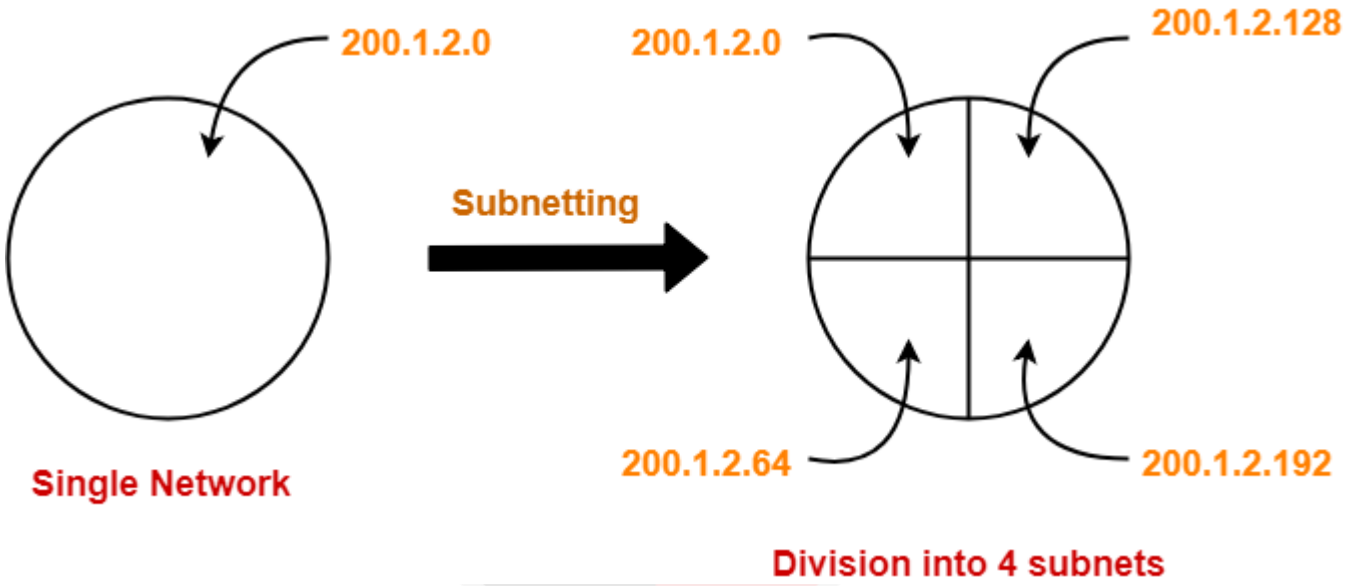
Classless Addressing

- To reduce the wastage of IP addresses in a block, we use sub-netting.
- **Subnetting:** Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks.
- We use host id bits as net id bits of a classful IP address.
- We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28
- For e.g., put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.
- **Subnet address** : AND result of subnet mask and the given IP address

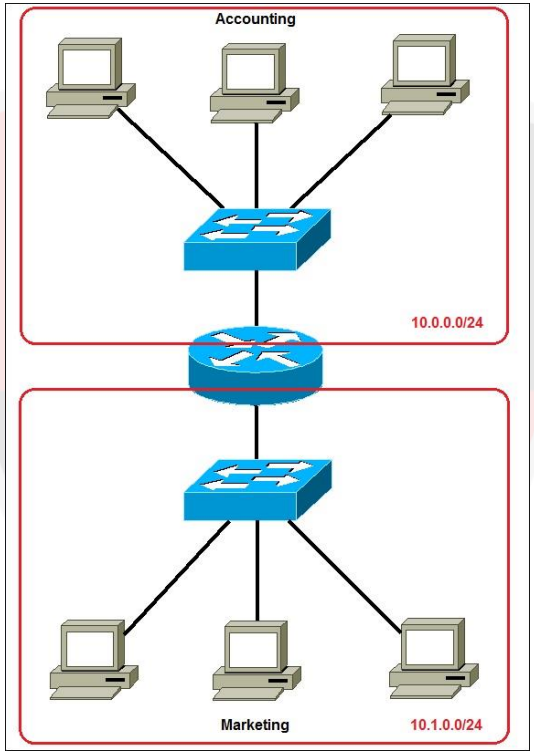
Classless Addressing



Classless Addressing



Classless Addressing



Host to Host Delivery

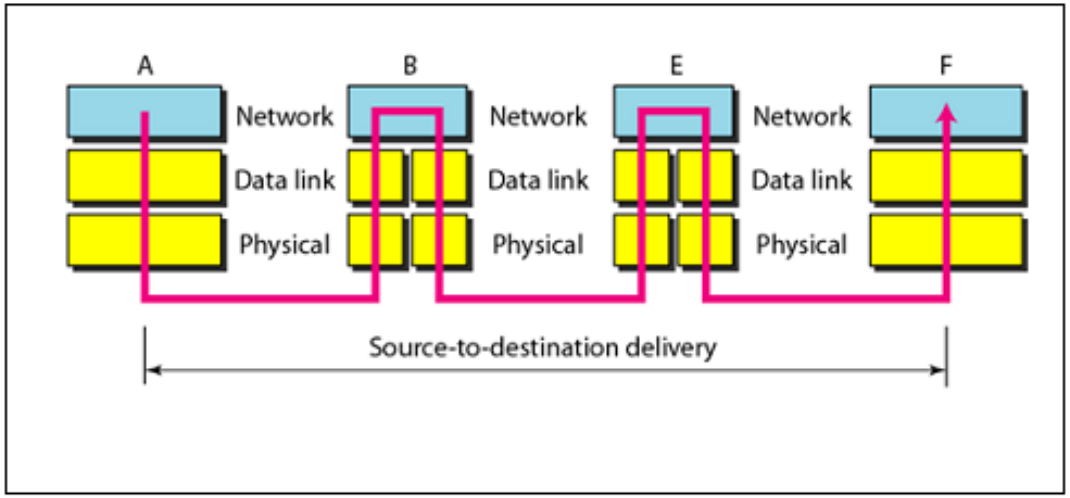


Fig: Data Transfer through Intermediate nodes

Transport Layer:
Port Addressing

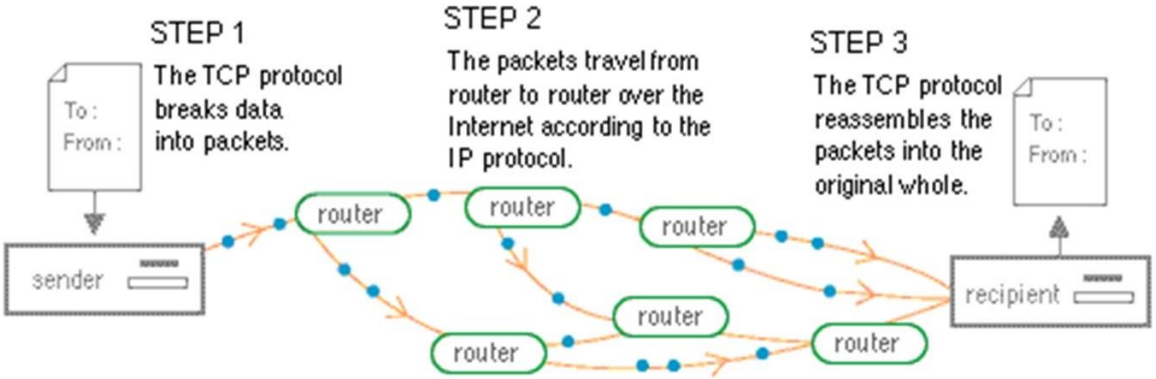
Module 4

Transport Layer Protocol (TCP)

- **TCP:**
  - Connection-oriented protocol.
  - Reliable as it guarantees delivery of data to the destination router.
  - Extensive error checking mechanisms
  - Comparatively slower than UDP
  - Common services that use TCP: HTTP, HTTPS, SSH, Telnet, SMTP, FTP, etc.

Transport Layer Protocol (TCP)

How TCP/IP Works



User Datagram Protocol (UDP)

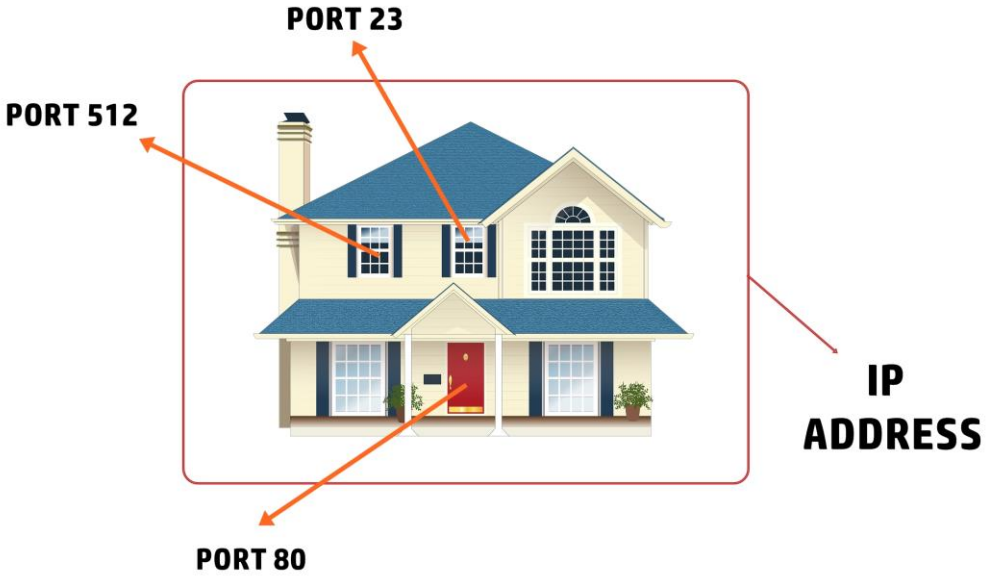
UDP:

- Connection-less protocol.
- Delivery of data to the destination cannot be guaranteed in UDP.
- Has only the basic error checking mechanism using checksums.
- No sequencing of data in UDP.
- Comparatively faster than TCP.
- No retransmission of lost packets
- Common services that use UDP: DNS, DHCP, SNMP, RIP, VoIP

Port Addressing

- **Port**:
  - A process identifier
  - A port number is the logical address of each application or process that uses a network or the Internet to communicate.
  - 16-bit integer port number, so the range is from: 0 to 65535.
  - Assigned automatically by the OS, manually by the user or is set as a default for some popular applications.
  - A complete URL looks like:
    - protocol://ip-address:port-number/path-of-the-resource

Port Addressing



Port Addressing

packetlife.net

Common Ports

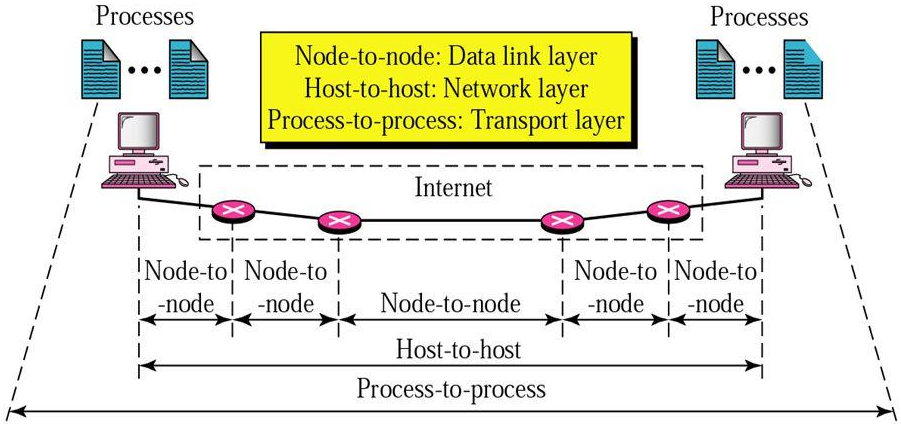
packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin

Process to Process delivery

Process-to-process Communication



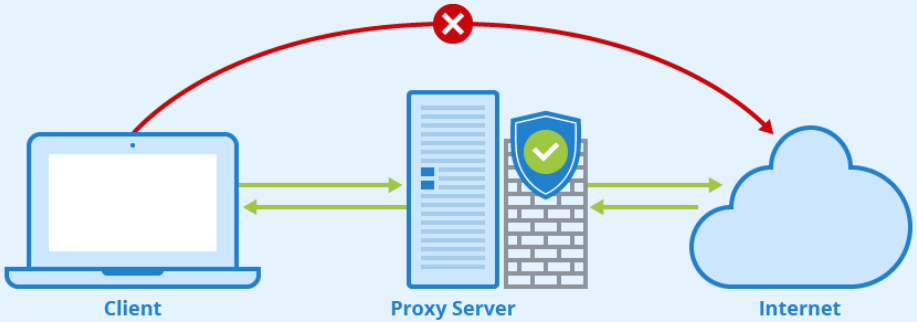
Proxies and Proxy Servers

Module 4

Proxies and Proxy Servers

- **Proxy**:
  - **Proxy server** is an intermediary server between client and the internet.
  - Indirect network connection to other locations and services with your PC or mobile device
  - Maybe an application or a separate system (PC).
  - Can be considered as an extra network hop.

Proxies and Proxy Servers



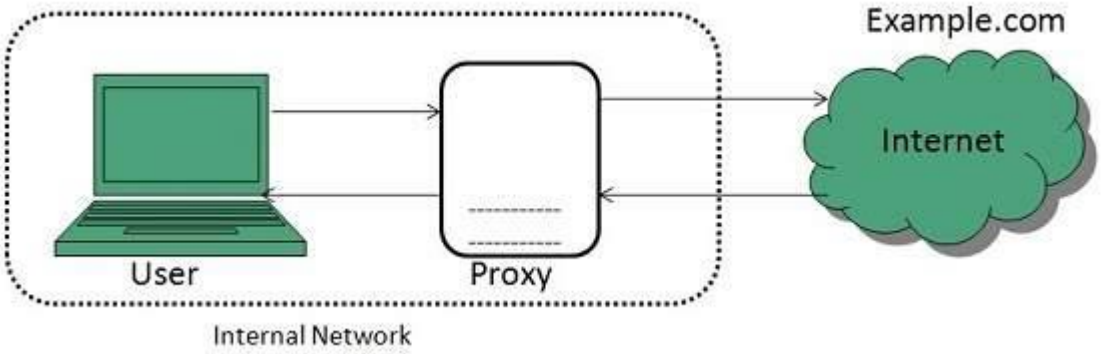
Proxies and Proxy Servers

- **Applications (Uses)**:
  - Monitoring and Filtering
  - Improving performance
  - Translation
  - Accessing services anonymously
  - Security

Proxies and Proxy Servers

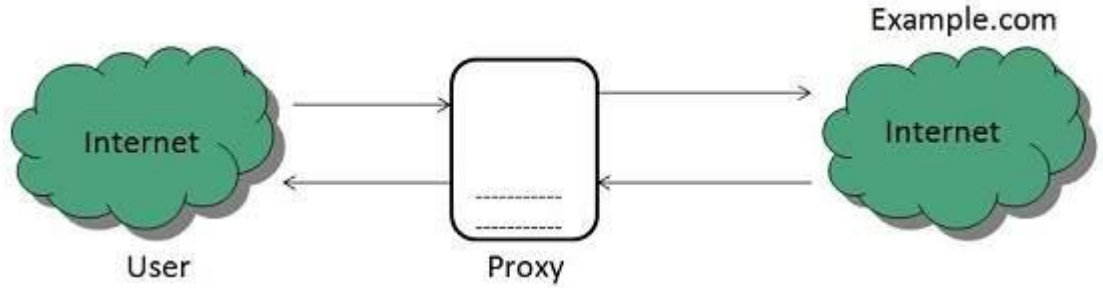
Types of Proxies

- Forward Proxies: Client requests its internal network server to forward to the internet.



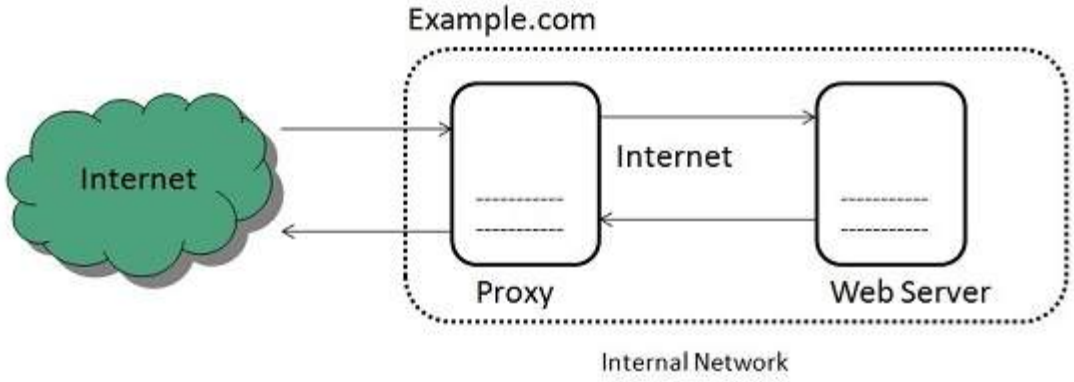
Proxies and Proxy Servers

- Open Proxies: Open Proxies helps the clients to conceal their IP address while browsing the web.



Proxies and Proxy Servers

- Reverse Proxies: Requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original Server.



Proxies and Proxy Servers

Types of Proxy Servers:

- SSL Proxy: Intervenes in the connection between the sender and the receiver and creates the connection over SSL which prevents hackers from attacking the network
- HTTP Proxy: Provides for the caching and content filtering of web pages and files which allows you to access them faster.

Proxies and Proxy Servers

Types of Proxy Servers:

- SOCKS Proxy: General purpose proxies used to access restricted content from behind a firewall, and doesn't interpret any traffic. ***SOCKS*** Version 5 adds additional support for security and UDP.
- Anonymous Proxy: Protects your privacy by hiding your IP (Internet Protocol) address from website owners, eavesdroppers, and other sources that exploit your identity., also capable of eliminating cookies which track your activity

TOR (The Onion Routing)

Module 4

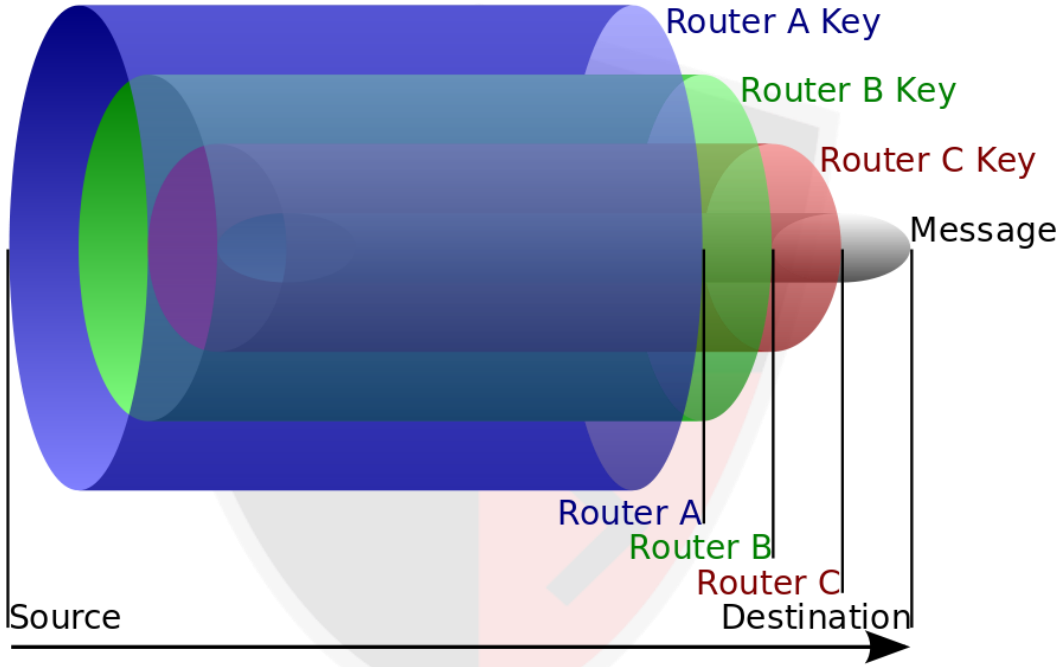
Onion Routing

- A technique for anonymous communication over a computer network.
- Messages are encapsulated in layers of encryption, analogous to layers of an onion.
- An advanced security measure in case you are still not satisfied with single encryption!
- Data is transmitted through a series of network nodes called **onion routers**, each of which "peels" away a single layer

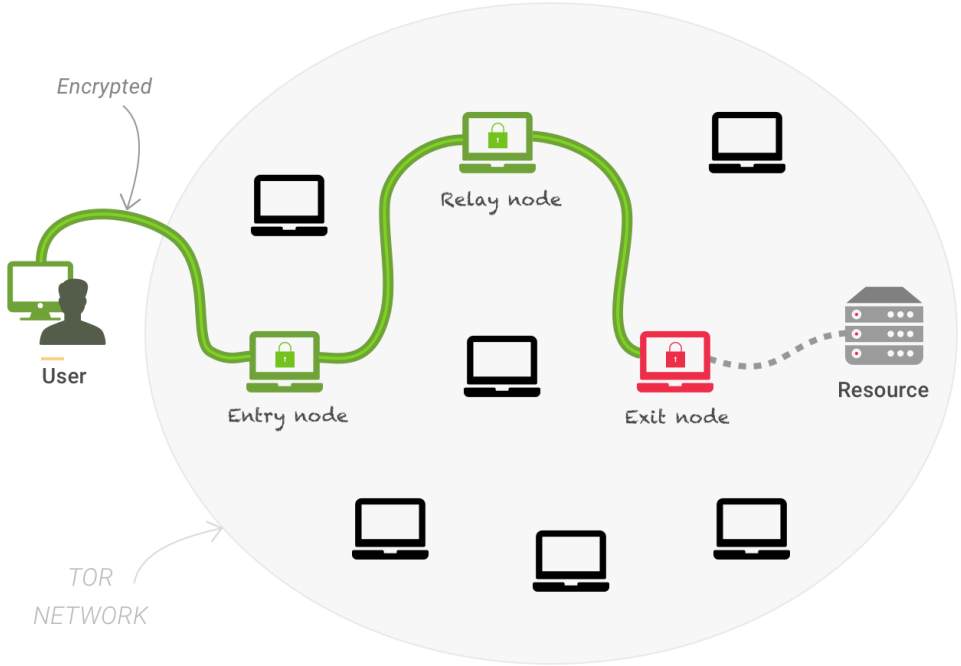
Onion Routing

- **Working**:
  - Connection is maintained between different nodes i.e. the connection hops from one server to another and when it reaches the last server, the destination server.
  - The message we send and the responses we receive are encrypted with different keys, with a unique key for encryption for every different hop or server visit.
  - Client has access to all the keys but the servers only have access to the keys specific for encryption/decryption to that server.

Onion Routing



Onion Routing

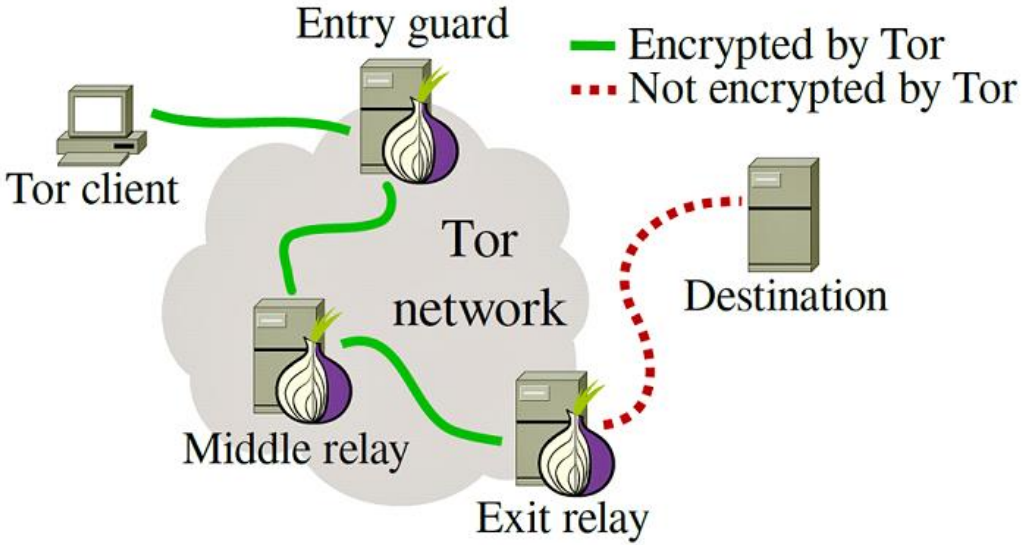


Onion Routing

The TOR Network:

- Free and open-source software for enabling anonymous communication using onion routing.
- Directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays.
- Makes it more difficult for network surveillance and traffic analysis.
- The U.S. Naval Research Laboratory sponsored the development of onion routing in the 1990s, and Tor itself was developed by Navy and independent researchers in 2002, and still funded by US Government.

Onion Routing



Onion Routing

Advantages of TOR:

- Open Source, reduces the risk of malicious backdoors.
- Multi proxy security (proxychaining)
- Supports .onion sites, etc. which are impossible to open otherwise
- Hides your IP address from which you are accessing the deep or dark web
- It supports all major operating system.
- TOR with VPN doubles the security

Onion Routing

Disadvantages of TOR:

- Bandwidth speeds are reduced when using Tor.
- Higher authorities or law can monitor and track
- Any relay within your TOR circuit can still read your data, especially the exit node.
- Tor browser uses apps which are not protected and doesn't provide anonymity.
- It can still reveal your IP address.

VPN (Virtual Private Networks)

Module 4

Virtual Private Networks

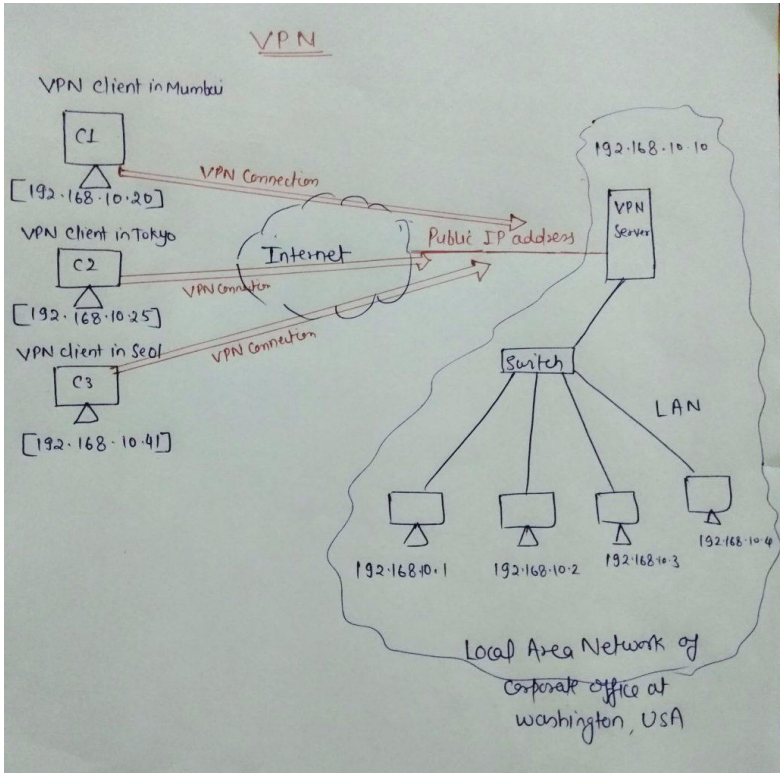
- Technology that creates a safe and encrypted connection over a less secure network, such as the internet.
- Way to extend a private network using a public network such as internet
- Users at one location ,e.g., home or office can connect in a secure fashion to a remote corporate server
- Uses tunneling which creates a point-to-point connection that cannot be accessed by unauthorized users

Virtual Private Networks

What is VPN Tunneling?

- Two-fold process of data encapsulation and data encryption.
- **Data encapsulation:** Encapsulation is the process of wrapping an internet data packet inside of another packet. You can think of this as like putting a letter inside of an envelope for sending.
- **Data encryption:** However, just having a tunnel isn't enough. Encryption scrambles and locks the contents of the letter, i.e. your data, so that it can't be open and read by anyone except the intended receiver.

Virtual Private Networks



Virtual Private Networks

Protocols implementing VPN?

- Internet Protocol Security (IPsec)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Secure Socket Tunneling Protocol (SSTP)
- Secure Socket Layer (SSL)

Virtual Private Networks

Advantages of VPN:

- Hides Your Online Identity
- Helps You Bypass Geo-Blocks
- Secures Your Online Transactions
- Prevents Bandwidth Throttling
- Can Bypass Firewalls
- Makes Online Gaming Better

Virtual Private Networks

Disadvantages of VPN:

- Can Sometimes Slow Down Your Online Speeds
- Wrong VPN Can Put Your Privacy in Danger
- Quality VPNs Will Cost Money
- Not All Devices Natively Support VPNs

Virtual Private Networks

Types of VPN:

- **Remote Access VPN:** Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely.
- **Site to Site VPN:** A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies, with branch offices in different locations, use Site-to-site VPN.
  - Intranet based VPN
  - Extranet based VPN

Remote Login: SSH and Telnet

Module 4

Remote Login

- Technology that allows an authorized user to login to other computer machines (hosts) on same or remote network
- Appears as if the user terminal were directly connected to that host computer
- The user can do anything that the host has given permission for, such as read, edit, or delete files.
- VPN provides access to a network, remote login provides access to a host within that network.
- VPN localizes your computer, while remote login localizes you.

Remote Login

- **Telnet**:
  - Network protocol that allows a user to communicate with a remote device.
  - Virtual terminal protocol used mostly by network administrators to remotely access and manage devices
  - Uses TCP port 23 by default
  - Telnet client and server must be running
  - Disadvantage: Clear text data transmission
  - Usage: telnet [hostname] [port]

Remote Login

- **SSH (Secure Shell)**:
  - Network protocol like telnet, with encryption.
  - Uses public key encryption to prevent eavesdropping
  - SSH client and server must be running
  - Usage: ssh [username]@[hostname] [commands]

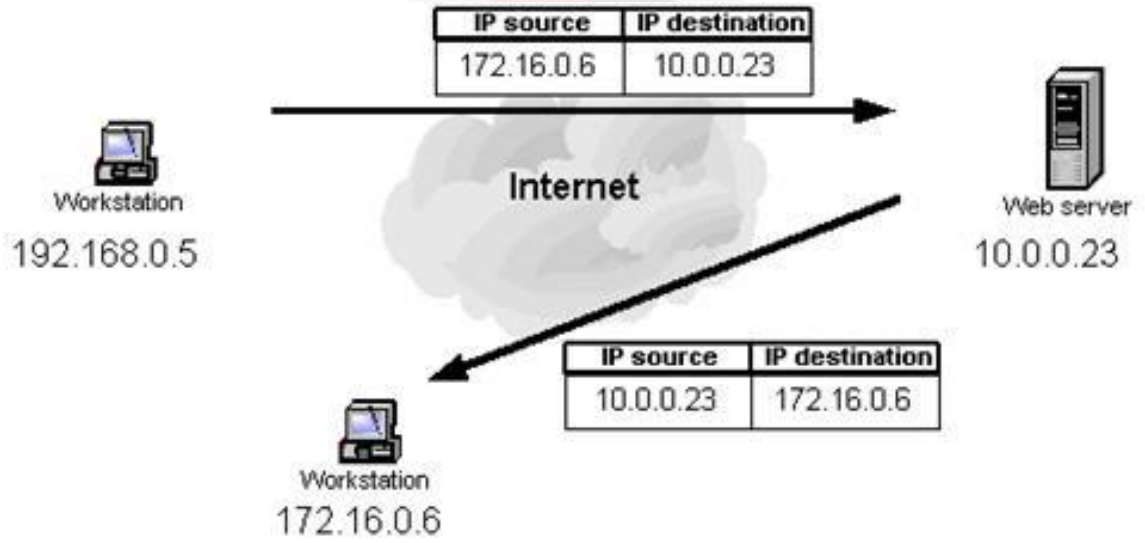
IP Spoofing

Module 4

IP Spoofing

- Creation of Internet Protocol (IP) packets which have a modified source address
- To either hide the identity of the sender or to impersonate another entity
- Done by modifying the packet header's source IP address and header checksum.

IP Spoofing


IP source
IP destination
172.16.0.6
10.0.0.23
Workstation
192.168.0.5
Internet
Web server
10.0.0.23
IP source
IP destination
10.0.0.23
172.16.0.6
Workstation
172.16.0.6

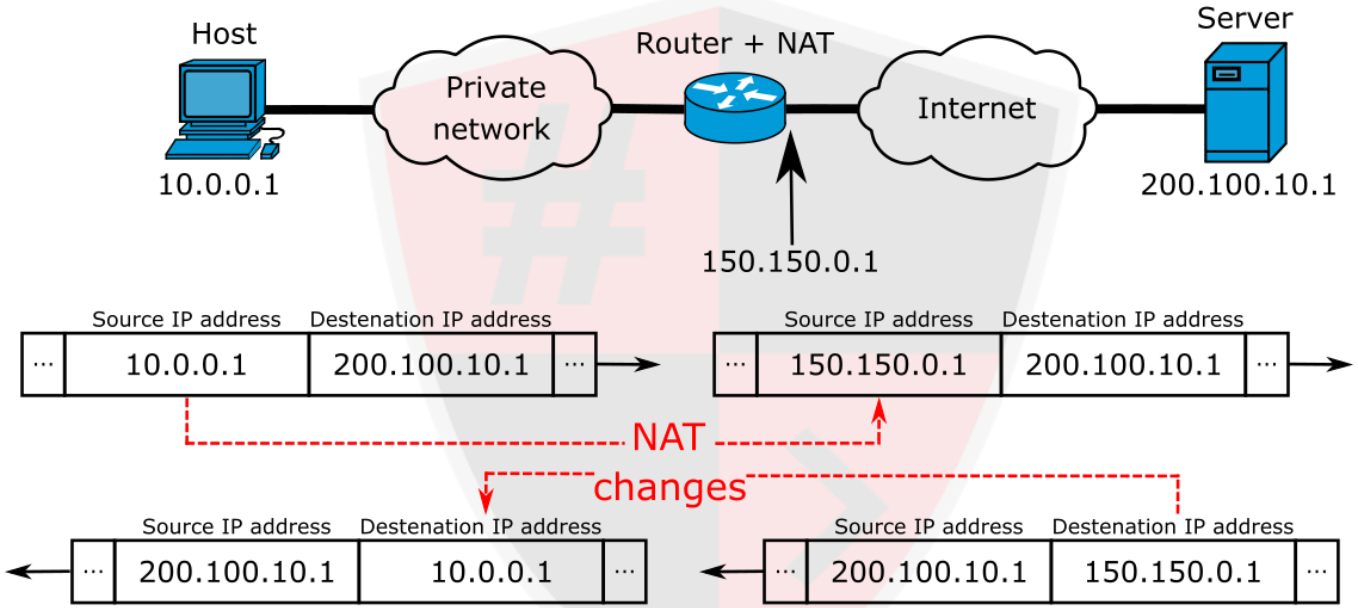
IP Spoofing

- **Attacks with IP Spoofing**:
  - Avoid being discovered and implicated by the authorities
  - Bypass security scripts, devices and services
  - Gain access to an internal private network
  - Perform Man-In-The-Middle attacks
  - Perform DDoS attacks, with amplification
  - ARP Poisoning
  - DNS Spoofing

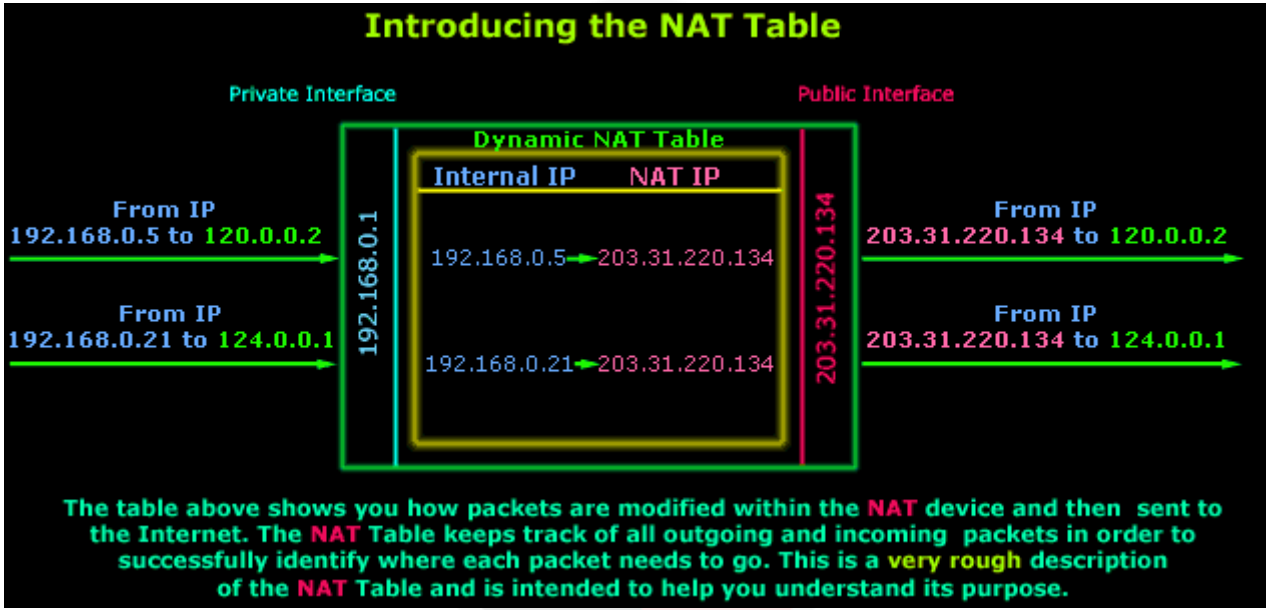
Port Forwarding

Module 4

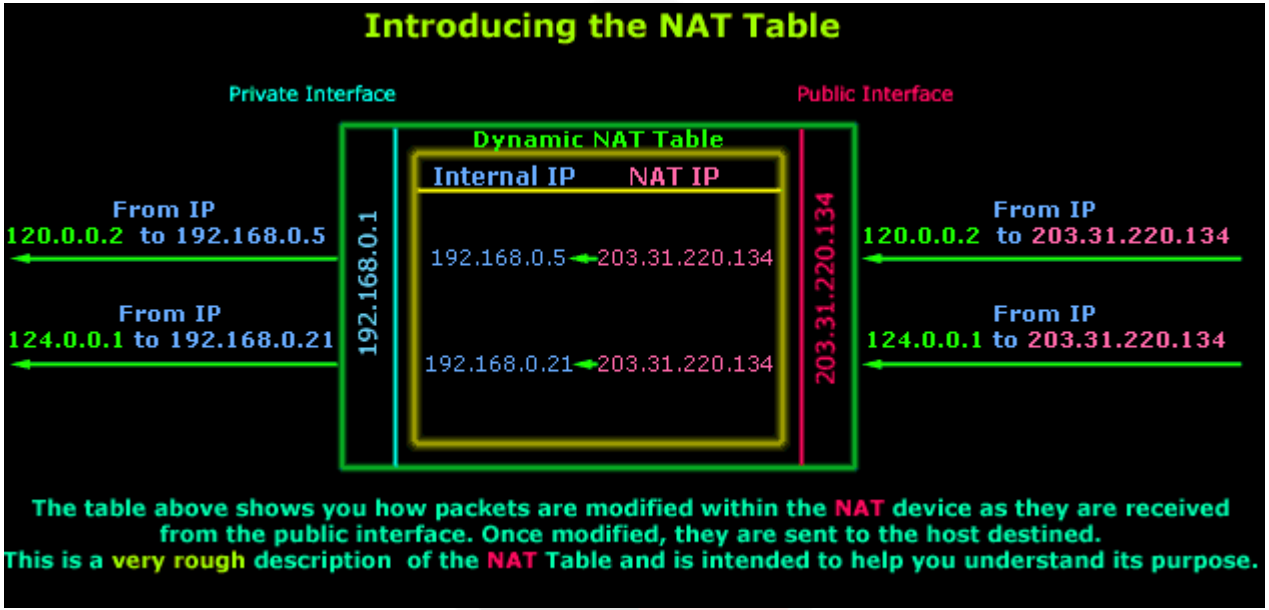
Working of NAT



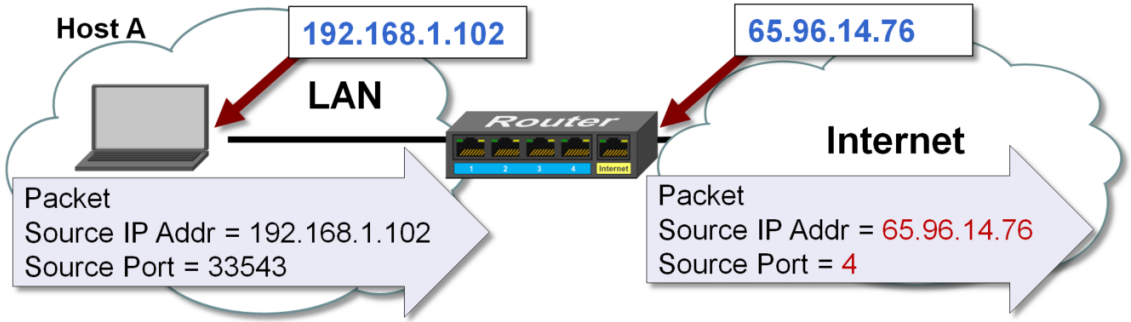
NAT Table


Introducing the NAT Table
Private Interface
Public Interface
Dynamic NAT Table
Internal IP
NAT IP
From IP
192.168.0.5 to 120.0.0.2
From IP
192.168.0.21 to 124.0.0.1
192.168.0.1
192.168.0.5 203.31.220.134
192.168.0.21 203.31.220.134
203.31.220.134
From IP
203.31.220.134 to 120.0.0.2
From IP
203.31.220.134 to 124.0.0.1
The table above shows you how packets are modified within the NAT device and then sent to the Internet. The NAT Table keeps track of all outgoing and incoming packets in order to successfully identify where each packet needs to go. This is a very rough description of the NAT Table and is intended to help you understand its purpose.

NAT Table


Introducing the NAT Table
Private Interface
Public Interface
Dynamic NAT Table
Internal IP
NAT IP
From IP
120.0.0.2 to 192.168.0.5
From IP
124.0.0.1 to 192.168.0.21
192.168.0.1
192.168.0.5 ◄ 203.31.220.134
192.168.0.21 ◄ 203.31.220.134
203.31.220.134
From IP
120.0.0.2 to 203.31.220.134
From IP
124.0.0.1 to 203.31.220.134
The table above shows you how packets are modified within the NAT device as they are received from the public interface. Once modified, they are sent to the host destined.
This is a very rough description of the NAT Table and is intended to help you understand its purpose.

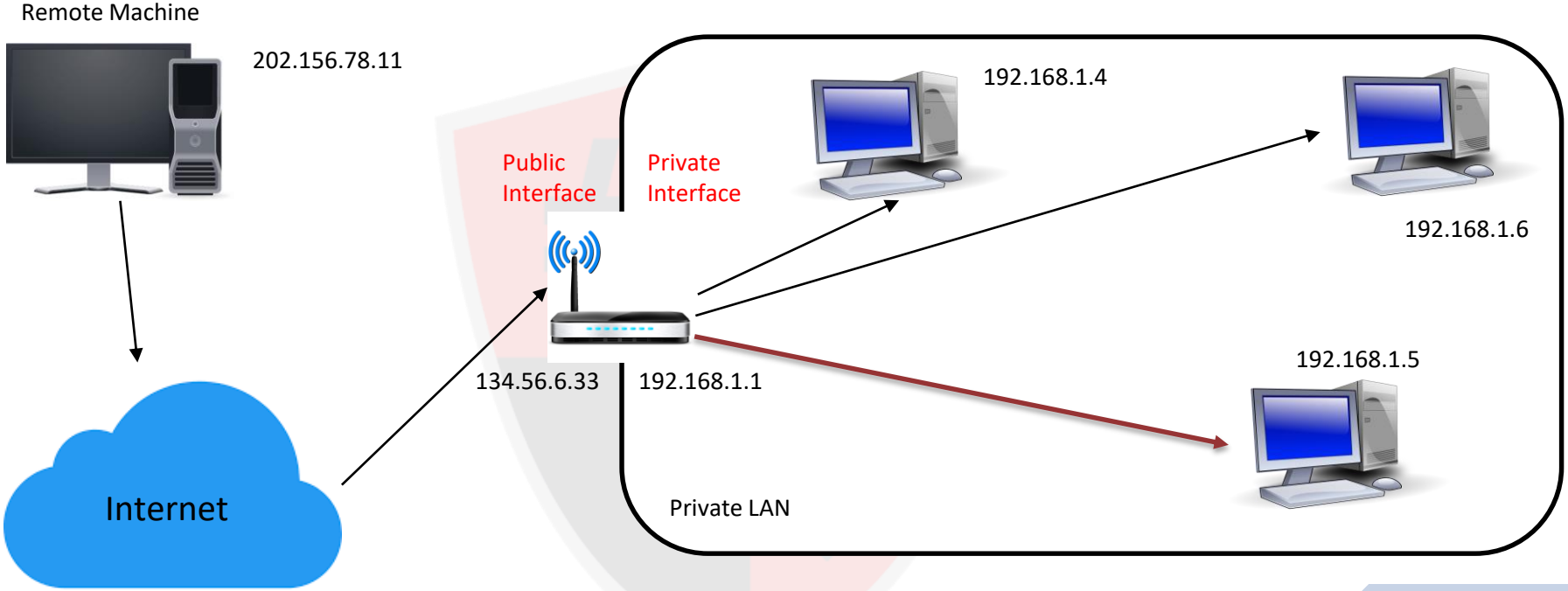
NAT Table



NAT Translation Table

	Local IP Address	Source Port #		Internet IP Address	Source Port #
process X, Host A →	192.168.1.101	54,847	=	65.96.14.76	1
Host B →	192.168.1.103	24,123	=	65.96.14.76	2
process Y, Host A →	192.168.1.101	42,156	=	65.96.14.76	3
Host C →	192.168.1.102	33,543	=	65.96.14.76	4

Destination		Forward to..	
IP	PORT	IP	PORT
134.56.6.33	8080	192.168.1.5	8080



HACKING

Is an art, practised through a creative mind.