

Intro to Computer Networking

Computer Networking Flashcards: <https://www.cram.com/flashcards/black-tower-network-terms-12714098>

What is computer network: “Computers interconnected together with the purpose of sharing resources.”

BASE NUMBERING SYSTEMS, [Base-2 Binary](#) IPv4 Addresses, Subnet Masking, Data Transmission, Bitwise Operations, Routing Tables, Much More*

[Base-10 Decimal](#) Numbers and information presented to end users are presented this way.

[Base-16 Hexadecimal](#) Concise way of representing binary, Physical / MAC Addresses, Ethernet Frame Types, IPv6 Addresses, Website Certificates, File Signatures, PCAPs, Color Codes for Websites, More*

[Base-62](#) are used in [URL Shorteners](#), Unique IDs, Data Compression, Obfuscation of data.

[Base-64](#) are used in Emails, URL encoding, Data, Basic Authentication, Encoding Private/Public Keys, and Obfuscation of data.

The [client-server model](#) is a computing architecture where one computer (the server) provides resources, services, or data to other computers (the clients) upon request. The server waits for requests from clients, processes those requests, and then sends the appropriate data or response back to the clients.

[Nodes](#) - A device connected to a network. Could be an Endpoint or a network redistribution point.

[Endpoint](#) -

[Gateway](#) - A node that acts as an interface between networks, this has a blended definition with the term Router.

[Host](#) - A node that is typically a device which runs applications, such as computers, smartphones, or server.

<OSI MODEL – Open Systems Interconnection Model>

- Layer 1 - Physical
- Layer 2 - Data Link
- Layer 3 - Network
- Layer 4 - Transport
- Layer 5 - Session
- Layer 6 - Presentation
- Layer 7 – Application

Computer Network Media uses the following to transfer information: Low Voltage Electrical, Light and Laser, Radio Frequency Signal, Sound, Vibration, Magnetism.

The Internet Engineering Task Force ([IETF](#)) is an open, international organization responsible for developing and promoting voluntary Internet standards.

Public IP addresses are unique globally and are used for external network communication, while private IP addresses are used and reused over and over again within local networks and aren't routable on the global internet.

Private IP ([IPv4](#)) addresses are reserved for use within private networks and are not routable on the public internet. These addresses are specified by the Internet Assigned Numbers Authority (IANA) and are typically used in local area networks (LANs) in residential, office, and enterprise environments.

1. **10.0.0.0 to 10.255.255.255**

- A single class A address block.
- Provides 16,777,216 private IP addresses.

2. **172.16.0.0 to 172.31.255.255**

- Consists of 16 contiguous class B address blocks.
- Provides 1,048,576 private IP addresses.

3. **192.168.0.0 to 192.168.255.255**

- Consists of 256 contiguous class C address blocks.
- Provides 65,536 private IP addresses.

[NAT – Network Address Translation](#)

To leave the private LAN that you are on, and go out to the Internet, one must use **Network Address Translation (NAT)**. Basically, NAT will map all of your local **Private IP Addresses** with a **Public IP Address**.

NAT conserves global IP address space by allowing multiple devices in a private network to share a single public IP address for accessing resources on the internet.

The Network Equipment that does the NAT function are **Routers**.

Remember that Routers have a minimum of two Network Interfaces, one for the LAN and one for another Network.

[In most situations, the 'other' network will be the Internet.] Each Network Interface will have an IP Address appropriate to the Networks that it is on. The [LAN](#) Interface will have a Private Address and the [WAN](#) Interface will have a Public IP Address.

[Network ports](#) are software-based constructs that allow applications and services on a computer to share the same physical network interface without interfering with one another.

Each IP address has 65,536 ports for both TCP ([Transmission Control Protocol](#)) and UDP ([User Datagram Protocol](#)). These ports enable multiple services to run on a single machine. For instance, web servers typically run on port 80 for HTTP and port 443 for HTTPS.

Administrative Ports (Well-Known Ports):

Range: 0-1023

Description: These ports are reserved for standard services.

Registered Ports:

Range: 1024-49151

Description: These ports are not reserved but are registered for specific applications. For instance, while not as universal as well-known ports, many applications will default to a port in this range.

Ephemeral Ports (Dynamic/Private Ports):

Range: 49152-65535

Description: These ports are not registered or reserved.

They are used for temporary and dynamic purposes, especially for the client-side of the client-server communication.

[Well Known or Common Port Numbers](#) such as 80 for HTTP or 443 for HTTPS

The purpose of standard network protocols is to define rules and conventions for communication between devices in a network. This includes interoperability, Data Integrity, Efficiency, Routing and Delivery to the other end of the connection, Security. By having standardized protocols, developers, engineers, and manufacturers have a common framework to design and develop their products, ensuring a consistent user experience.

A default gateway is the device that directs network traffic from a local network to other networks or the internet. It acts as the "exit point" for local devices seeking to communicate outside their immediate network.

In home networks, it is typically your Internet Router / Gateway / Modem if it is all combined into a single device.

Protocol Acronym	Protocol Name	Transport Protocol	Concept	Port(s)	RFP (For Reference)
DHCP	Domain Host Configuration Protocol	UDP	DHCP provides Dynamic Addresses to Clients that wish to join a Computer Network	67/68	RFC 2131
DNS	Domain Name Service	TCP/UDP	Translates domain names into IP addresses to ensure proper routing.	53	RFC 1034 / RFC 1035
HTTP	Hypertext Transfer Protocol	TCP	The main protocol to transfer HTML Code from Server to Client Browser so End Users can view Web Pages.	80	RFC 2616
HTTPS	Hypertext Transfer Protocol over SSL/TLS	TCP	HTTPS works with HTTP to deliver HTML Code securely using the SSL / TLS Protocols.	443	RFC 2618

Telnet	Teletype over Network Protocol	TCP	A deprecated method that shouldn't be used to manage Network Devices & Unix/Linux Systems via a text-based Shell. (Not Encrypted)	23	RFC 15 RFC 854
SSH	Secure Shell	TCP	The primary method used to manage Network Devices & Unix/Linux Systems via a text-based Shell. (Encrypted)	22	RFC 4250-4256