

## NETWORK

### INTERNET

#### OSI MODEL (OPEN SYSTEMS INTERCONNECTION MODEL)

Developed in the 1980s...

Standard reference model created by the International Organization for Standardization

Conceptual model that characterizes and standardizes communication between network and user, by dividing all the operations related to data transmission into different layers

Describes how computers communicate with one another over a network

Describes how different software and hardware components involved in a network communication should divide labor and interact with one another

Goal is interoperability of diverse communication systems with standard protocols

Defines networking framework to implement protocols in terms of a vertical stack of seven layers

A layer serves the layer above it and is served by the layer below it

Protocols are common sets of rules for transmitting and receiving packets of data between two endpoints and are fundamental for communication

All data that goes over a network connection passes through each of the seven layers, going from the upper level software oriented services to the lower level more hardware oriented functions

#### LAYERS

- Layer 7: Application Layer (Protocols: HTTP/FTP/TELNET/SSH/SMTP/POP3/DNS)
- Layer 6: Presentation Layer
- Layer 5: Session Layer
- Layer 4: Transport Layer (Protocols: TCP/UDP)
- Layer 3: Network Layer (Protocols: IP)
- Layer 2: Data Link Layer
- Layer 1: Physical Layer

#### TCP/IP MODEL (TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL)

Developed in the 1970s...

Another name for it is "Internet Protocol Suite" since more protocols are used in addition to TCP and IP

TCP defines how applications can create reliable channels of communication across a network and IP defines addressing and routing

Protocols by which data is sent from one computer to another on the Internet, organized into four abstraction layers which specifies how data should be packetized, addressed, transmitted, routed, and received

Each computer/host on the Internet has one IP address that uniquely identifies it from all other computers on the Internet

When data is sent or received, it gets divided into packets, containing both the sender's and the receiver's IP address

During transmission, each layer adds a header to the data that directs and identifies the packet

#### LAYERS

- Layer 4: Application layer
  - Provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data
  - The application layer contains the higher level protocols used by most applications for network communication
  - Data coded according to application layer protocols are encapsulated into a transport layer protocol (TCP / UDP) which in turn use lower layer protocols to do the actual data transfer

Application layer protocols generally treat the transport layer and lower protocols as black boxes which provide a stable network connection across which to communicate

- Layer 3: Transport layer  
Responsible for providing Application layer with session and datagram communication services  
The transport layer establishes host-to-host connectivity and transmits the data by sending packages  
Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers)
- Layer 2: Internet layer  
Responsible for addressing, packaging, and routing functions  
Provides logical addressing so data can pass among subnets of different types  
Provides packet routing, the task of sending packets of data (datagrams) from source to destination by sending them to the next network node (router) closer to the final destination  
Relates physical addresses (used at the Network Access layer) to logical addresses
- Layer 1: Network layer  
Responsible for sending and receiving TCP/IP packets on the network  
Involves encapsulation of IP packets into frames for transmission, mapping IP addresses to physical hardware addresses (MAC Addresses) and physical transmission of data

---

## CONCEPTS & TERMS

### Protocols

Standards / policies, consisting of rules, procedures and formats for how devices communicate with each other over networks

### Ports

Endpoints of communication identified by numbers, referred to as port numbers

A port number is a 16-bit unsigned integer that ranges from 0 to 65535

The port numbers that range from 0 to 1023 are known as well-known port numbers and these are used by standard server processes, such as HTTP, SSH, FTP, SMTP and Telnet

Any networking process uses a specific network port to transmit and receive data to a certain IP address

### Network interface controller

Point of interconnection between a computer and a private or public network

Interface between two pieces of equipment

Computer <-> Switch

Router <-> Switch

Typically, a network card

A network interface controller will usually have some form of network address

Network interfaces provide standardized functions such as passing messages, connecting and disconnecting

### Switch

Switches create networks

Operates on the data link layer

Sends data in the form of frames

Connects devices together on network by using packet switching to receive, process, and forward data to the destination device

### Router

Routers connect networks

Operates on the network layer

Sends data in the form of packets

Networking device that forwards data packets between computer networks

Routers perform the traffic directing functions on the Internet

Routers are located at gateways, the places where two or more networks connect

A data packet is typically forwarded from one router to another router through the networks until it reaches its destination node

### LAN (Local area network)

Network that interconnects a group of computers within a limited area such as a residence, school, laboratory, university campus or office building

### WAN (Wide area network)

Network that spans a large geographic area such as across cities, states, or countries  
Connects several LANs together

### MAC Addresses (Media Access Control)

Kind of serial number assigned to every network interface controller

MAC addresses are assigned at the time hardware is manufactured

Each network interface controller has one, including wired and wireless interfaces

A network node may have multiple network interface controllers which all have a unique MAC address

Used to direct packets from one device to the next as data travels on a network

MAC addresses travel the network only until the next device along the way

### IP Addresses (Internet Protocol)

Numerical label

Numbers are used by routers and servers to direct requests and get correct responses

IP addresses are assigned as part of connecting to a network

IP address is assigned to every device on a network, so that device can be located on that network

Each ISP or private network administrator assigns an IP address to each device connected to its network, on either static or dynamic basis (*static IP address / dynamic IP address*)

An IP address has two parts, the network address and the host address

IP address: 192.168.123.132  
(192.168.123) Network address      192.168.123.0 Network address  
(132) Host address      0.0.0.132 Host address

IPv4      Defines a 32-bit numeric IP address  
(172.160.254.100)      Decimal notation  
4 \* 8 bits  
4 octets  
Decimal values ranging from 0 - 255  
Number of IPv4 addresses  
 $2^{32} = 4,294,967,296$

IPv6      Defines a 128-bit hexadecimal IP address  
(2001:0db8:85a3:0000:0000:8a2e:0370:7334)      Hexadecimal notation  
8 \* 16 bits  
16 octets  
Number of IPv6 addresses  
 $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$   
  
340 undecillion, 282 decillion, 366 nonillion, 920 octillion, 938 septillion, 463 sextillion, 463 quintillion, 374 quadrillion, 607 trillion, 431 billion, 768 million, 211 thousand and 456

## Public addresses

Globally routable unicast IP address

If directly connected, a computer will have an IP address that can be reached from anywhere on the internet

## Private addresses

Used internally on private networks

If behind a router, router will have the internet-visible IP address, but it will then set up a separate, private network to which the computer is connected, assigning IP addresses out of a private range, that is not directly visible on the internet.

Any internet traffic a computer generates must go through the router and will appear on the internet to have come from the router

Three non-overlapping ranges of IPv4 addresses reserved for private networks

	Start	End	No. of addresses
24-bit block	10.0.0.0	10.255.255.255	16777216
20-bit block	172.16.0.0	172.31.255.255	1048576
16-bit block	192.168.0.0	192.168.255.255	65536

Multiple client devices can appear to share an IP address, either because they are part of a shared hosting web server environment or because an IPv4 network address translator (NAT) or proxy server acts as an intermediary agent on behalf of the client

## Loopback Address

Localhost is a hostname that means “this computer” used to access and test the network services that are running on the host

Range of IPv4 addresses reserved for loopback addresses

	Start	End	No. of addresses
20-bit block	172.0.0.0	172.255.255.255	1048576

## Default gateway

The node that is assumed to know how to forward packets on to other networks

Serves as an access point to others network if nothing else is specified

Each network has a default gateway, through which all data bound for other networks passes, thereby making communication between subnets possible

Either routers or gateway computers can be used to network local subnets

## Subnet mask

Enables network administrator to further divide the host part of the address into two or more subnets

Subnet mask is a mask used to determine what subnet an IP address belongs to and if it is on a local subnet or a remote network

A subnet mask neither works like an IP address nor exist independently of them, instead subnet masks accompany an IP address and the two values work together

With a subnet mask the network and host portions of an IP address can be separated

IP address:	192.168.123.132	11000000.10101000.01111011.10000100
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
Network address:	192.168.123.0	11000000.10101000.01111011.00000000
Host address:	000.000.000.132	00000000.00000000.00000000.10000100

Subnet mask can be used to determine if network addresses matches

IP address:	192.168.123.155	11000000.10101000.01111011.10011011
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
Network address:	192.168.123.0	11000000.10101000.01111011.00000000

Examples of other subnet masks

255.255.240.0	11111111.11111111.11110000.00000000
255.255.255.192	11111111.11111111.11111111.11000000
255.255.255.224	11111111.11111111.11111111.11100000

### **DHCP (Dynamic Host Configuration Protocol)**

Dynamically distributes IP addresses, subnet masks and default gateway, eliminating the need for an administrator to manually assign IP addresses to all network devices

- When a DHCP-configured client connects to a network, it sends a broadcast query requesting necessary information to a gateway enabled to act as DHCP server
- The DHCP server manages a pool of IP addresses and information about default gateway, domain name and similar
- On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), subnet mask and default gateway
- The query is typically initiated immediately after booting and must complete before the client can initiate IP-based communication with other hosts
- Upon disconnecting, the IP address is returned to the pool for use by other clients

### **NAT (Network address translation)**

Enables a network to use one set of IP addresses for internal traffic and a second set of addresses for external traffic

The way that the router translates the IP addresses of packets that cross the remote/local network boundary

Method of remapping one IP address space into another by modifying network address information

Allows a single device, such as a router, to act as an agent between the remote (public network) and a local (private) network

This means that only a single, unique IP address is required to represent an entire group of computers

1. Local machine sends package
2. Router sees package and replaces source IP with the router's own IP
3. Remote host replies to router
4. Router sees reply and replaces destination IP with source IP

### **DNS (Domain Name System)**

Hierarchical decentralized naming system used by the Internet since 1985

The way that internet domain names are located and translated into IP addresses

Better to use names instead of numbers for Internet addresses

Globally distributed, scalable, reliable, dynamic database, used to map between hostnames and IP addresses, and to provide electronic mail routing information

TechnologySite.com <=> 165.23.43.66

DNS mapping is distributed throughout the Internet

DNS is a worldwide network that collectively forms a global database of domain names and IP addresses

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain

Access providers, enterprises, governments, universities and other organizations, typically have their own assigned ranges of IP addresses, an assigned domain name and run DNS servers to manage the mapping of those names to those addresses

The top hierarchy of the Domain Name System is served by the root name servers and top level domain name servers

The root domain contains all top level domains of the Internet and it does not have a formal name, but is just labeled as an empty string in the DNS hierarchy

google.com. / yahoo.com. / dr.dk. / ...

There are thirteen root server networks, consisting of hundreds of servers spread out in countries all over the world, maintained by 12 different organizations A-M (Verisign / University of Maryland / Netnod / ...)

The root zone is supervised by IANA, which is a part of ICANN

The root zone has a list of the authoritative servers for each of the 1500+ top level domains

.com / .org / .dk / .uk / .london / .eco / .google / ...

Each one of the top level domains authoritative name servers knows about the authoritative name servers for the second level domains under them

news.com / news.org / news.dk / news.uk / news.london / news.eco / news.google / ...

### DNS Servers

Authoritative DNS server

Satisfies queries from its own data without needing to reference another source

Responsible for providing mapping answers to recursive DNS servers

Recursive DNS server

Answers queries by asking other name servers

Assigned with task of finding IP addresses for domain names

If nothing is cached authoritative DNS hierarchy is asked for answers

DNS servers answer questions from both inside and outside their own domains

When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer

When a server receives a request from inside its own domain for information about a name or address outside that domain, it passes the request out to another server

The major task carried out by a DNS server is to respond to local and remote queries

A DNS client queries a DNS server to resolve a host name into an IP address

### DNS Requests

There are three types of queries defined for DNS:

- Recursive:  
Return either resolved host name or error message perhaps querying other DNS servers
- Iterative:  
Return either resolved host name or referral to different DNS server without querying other DNS servers
- Inverse:  
Return resolved host name associated with a IP address

### DNS Records

DNS records are instructions that live in authoritative DNS servers and provide information about a domain

DNS records are used to control the location of resources on the Internet and each record has a name, type and time to live (TTL)

DNS records are defined in a text file called the DNS zone file

Many different types of DNS records can be created for a domain with different purposes

- |  |                                     |
|--|-------------------------------------|
| - Address Mapping records (A)          | Map domain name to IPv4 address     |
| - IP Version 6 Address records (AAAA)  | Map domain name to IPv6 address     |
| - Canonical Name records (CNAME)       | Map domain name to domain name      |
| - Mail exchanger record (MX)           | Direction of mail                   |
| - Name Server records (NS)             | Specify name servers used by domain |
| - Reverse-lookup Pointer records (PTR) | Map IP address to domain name       |

---

## COMMANDS & SITES

### ipconfig / ifconfig (Internet Protocol Configuration)

Displays the IP address, subnet mask, and default gateway for all adapters

Displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings

Ipconfig /all gives more detailed information

An important additional feature is to force refreshing of the DHCP IP address of the host computer to request a different IP address

ipconfig /release is executed to force the client to immediately give up its lease by sending the server a DHCP release notification which updates the server's status information and marks the old client's IP address as "available"

ipconfig /renew is executed to request a new IP address

Example: ipconfig /all

### ping

Tests the ability of the source computer to reach a specified destination computer

Verifies that a computer can communicate over the network with another computer or network device

Operates by sending messages to destination computer and waiting for a response

How many responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides

Also gives destination public ip address

Example: ping google.com

### tracert / traceroute

Used to show details about the path that packets take from host to destination

Displays route (path) and measure transit delays of packets across network

Identifies network devices all the way to destination, plus delays and packet loss at each stop (hop)

Round-trip time is time that it takes for a packet to get to a hop and back (in milliseconds)

Example: tracert google.com

### pathping

Combination of ping and tracert

Example: pathping google.com

### netstat (Network statistics)

Lists opened connections (sockets) on your machine

Displays network connections, both incoming and outgoing, plus routing tables

-ab Shows listeners (Run as administrator)

Example: netstat

Example: netstat -ab

### nslookup (Name server lookup)

Used to obtain information about internet servers

Finds name server information for domains by querying the Domain Name System (DNS)

Can identify which DNS server that the host is currently configured to use for its DNS lookups

A non-authoritative answer referring to DNS record kept on third-party DNS servers

An authoritative address lookup can be performed by specifying one of the domain's registered name servers

set type=a Specifies a computer's IP address

set type=ns Specifies a DNS name server for the named zone

set type=any Specifies all types of data

Example: nslookup -> set type=ns -> google.com

### whois

Search domain name registration records

<https://www.whois.com/whois/>

### whatismyip

Google ip

<https://whatsmyip.com/>

## HTTP (HYPERTEXT TRANSFER PROTOCOL)

Basic underlying protocol of the World Wide Web

Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands

Stateless application-level protocol

Request / Response

Initiated by a request / Replied with a response

### Messages

- Request line / Status line
  - o Request line: Method / URI / Version  
Request: GET /logo.gif HTTP/1.1
  - o Status line: Version / Status code / Status text  
Response: HTTP/1.1 200 OK
- Headers
  - Simple key-value pairs
- Empty line (<CR><LF>)
  - The request / status line and headers must end with <CR><LF>
- Message
  - Optional message body

### Methods

GET	Requests a representation of the specified resource Requests using GET should only retrieve data and should have no other effect
POST	Requests that the server accept the entity enclosed in the request as a new subordinate of the resource identified by the URI
HEAD	Asks for the response identical to the one that would correspond to a GET request, but without the response body
PUT	Requests that the enclosed entity be stored under the supplied URI. If the URI refers to an already existing resource, it is modified; if the URI does not point to an existing resource, then the server can create the resource with that URI
DELETE	Deletes the specified resource
TRACE	Echoes back the received request so that a client can see what (if any) changes or additions have been made by intermediate servers
OPTIONS	Returns the HTTP methods that the server supports for specified URL This can be used to check the functionality of a web server

### Status codes

5 different categories with many different sub codes

1xx	Informational
2xx	Successful
3xx	Redirection
4xx	Client error
5xx	Server error

### Caching

Performance of web sites and applications can be significantly improved by reusing previously fetched resources, thereby reducing latency and network traffic

Set expiration time, revalidation and other caching policies in header

### Sessions

Each request is discrete and unrelated to preceding or following requests

The core HTTP protocol itself is stateless, but web applications built on top of HTTP do not have to be stateless

Different ways to introduce state

Query strings

/index.html?user=jimmy&password=1234

Hidden form variables



Cookies  
Local storage  
Session storage

### **Cookies**

Small piece of data that a website asks your browser to store on your computer or mobile device

Supported by most browsers, but users can set their browsers to decline them and delete them whenever they like

Used for many different purposes such as authentication, personalization, tracking and advertising

- Session
  - Users sessions for a website exists in temporary memory only while users are navigating the website
  - Web browsers normally delete session cookies when users close their browsers
- Persistent
  - Persistent cookies can be created to outlast user sessions
- Secure
  - Has the secure attribute enabled
  - Only used for HTTPS
  - Encrypted when transmitting from client to server
  - Less likely to be exposed to cookie theft via eavesdropping
- HttpOnly
  - Supported by most modern browsers
  - Used only when transmitting HTTP/HTTPS requests, restricting access from other non HTTP APIs
- ThirdParty
  - First-party cookies are cookies created by the visited domain
  - Third-party cookies are cookies created by other domains than the visited domain

### **EU legislation**

Web sites must follow the Commission's guidelines on privacy and data protection and inform users that cookies are used to store information, the law however is not only restricted to cookies, but involves all information storing technologies

**POSTMAN**     <https://www.getpostman.com/apps>

### **Browser developer tools**

Browser developer tools (F12 / Ctrl + Shift + I)

Inspector (HTML & CSS)

Console (JS)

Network (HTTP)

Urls / Method / Request / Response / Header / Body

Storage (Cookies & LocalStorage)