U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

Networking

October 2023

cyberforcecompetition@anl.gov

Intro to Networking

Overview

A **computer network** is computers that are connected to communicate data electronically. Computer networks follow protocols, which define how data packets are communicated between devices.

Routers allow data to be communicated across different networks, and switches manage network communication. Every device has a unique address, which ensures data reaches the correct recipient. The internet is a network of computer networks that connects devices across the world.

Types of Computer Networks

There are different types of networks that vary based on their uses.

A **local area network (LAN)** connects computers across a single location. They are typically privately owned. **Ethernet** is a type of wired LAN that allows for a centralized wired connection between devices through ethernet cables. **Wi-Fi** is another type of LAN that allows for wireless local network connection through a shared Ethernet wired relay.

A **wide area network (WAN)** connects computers across different locations or worldwide, like the internet. It connects multiple local networks and allows devices in one LAN network to communicate with others in other LAN networks through routers.

A **virtual provide network (VPN)** is a secure, encrypted channel connecting two endpoints. **Cloud networking** allows developers to connect many devices across a large area using cloud-based wireless networking systems.

Network Infrastructure

Different devices are used to build a computer network. They rely on unique identifiers like MAC addresses or IP addresses to determine where to deliver data on the network.

Nodes are physical devices within networks like computers, printers, switches, and more. They can create, receive, or send data.

Routers link different networks together. They sort and forward data packets to the correct network, and they determine the data's destination by using IP addresses. They are located at **gateways**, which acts as the intersection point between two or more networks.

Both hubs and switches are connection points between devices in a network. A **hub** copies and sends data packets quickly to every device connected to it. **Switches** also forward data packets to network devices within the same network, but it first determines which device it's intended for by using MAC addresses before sending it to those devices.

ⓘ Types of Network Architecture

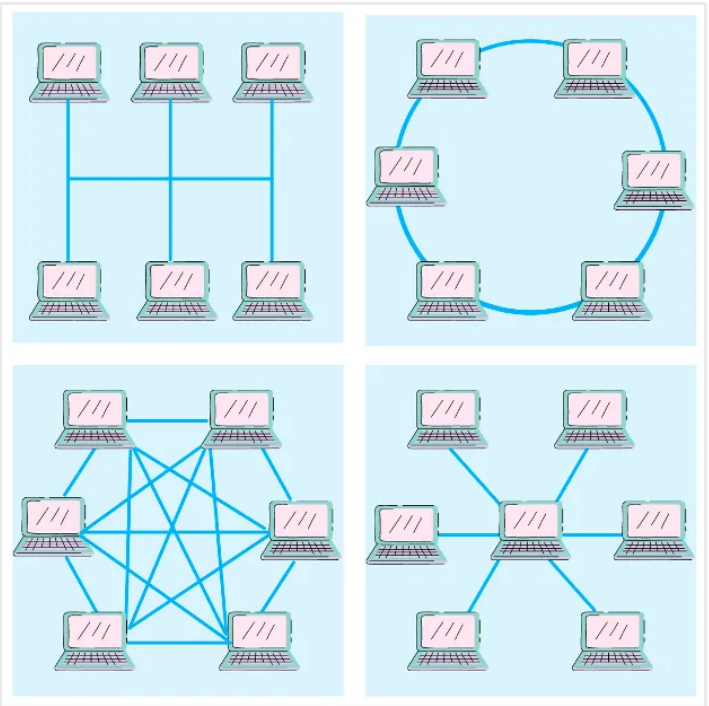
- **Client-Server Architecture** - nodes can be servers or clients; the server manages the client node's behavior
- **Peer-to-Peer Architecture** - each device is free for working as either client or server

Network Topology

Network topology describes the physical arrangement of the elements in a network.

A **bus** topology (top left) is where each device is connected to a single cable. Therefore, all the devices need to be geographically close together, as the strength of the signal weakens along the cable. In a **ring** (top right), each device is connected to its neighbor. With a **mesh** topology (bottom left), each device connects to all other devices, making it the more robust but also one with the most overhead.

For a **star** topology (bottom right), each device connects to a centralized switch, which can link them together. This topology is the most robust and scalable, as well as most used.



From Medium

Network Protocols

A network protocol is a set of rules for how data communicates between devices on a network. **Data packets** consist of raw data and a header and allows for data to be sent between devices. The header includes addresses of the sender and recipient.

Each network device has a unique identifier or address that is used to ensure data is sent to the correct destination. Identifiers include **Hostname**, **MAC (Media Access Control) addresses**, and **IP (Internet Protocol) addresses**.

- Hostname - unique device name for each device in the network
- MAC addresses - unique identifiers assigned to every device during manufacturing
- IP addresses (or logical addresses) - unique identifiers defining a device's host network and location; assigned to every device using the IP to communicate

IPv4 vs IPv6

- IPv4 uses a 32-bit address
  - Manual configuration
  - Numerical dot-decimal notation
  - Example: `192.168.10.150`
- IPv6 uses a 128-bit address
  - Supports autoconfiguration
  - Alphanumeric hexadecimal notation
  - Example: `3002:0bd6:0000:0000:0000:ee00:0033:6778`

IPv6 is the solution that addresses the limited number of addresses possible under IPv4, which has theoretical limit of 4.3 billion addresses, because it has a theoretical limit of 7.9x10^28 addresses

Ports are channels that allow data to be routed to a specific application or service within a host. Unique numbers identify the ports. An IP address and port number together specifies a particular service on a host. By running the command `netstate -a` you can see all the ports being used.

Port Types	Range
Well known	0 - 1023
Registered	1024 - 49151
Ephemeral	49152 - 65535

A **socket** is the unique combination of an IP address and port number together.

IPv4 Address Classes and Reserved Ranges

IP addresses are made of two separate components, with the first part of the address identifying the network that it's a part of and the second part specifying a specific host within that network. The location where the network specification ends and the host specification begins depends on how that network is configured.

IPv4 addresses were traditionally divided into five different "classes," named A through E. These were meant to differentiate segments of the available addressable IPv4 space and are defined by the first four bits of each address.

Class	Description
Class A	First bit is `0---` Any address from `0.0.0.0` to `127.255.255.255`
Class B	First bit is `10--` Any address from `128.0.0.0` to `191.255.255.255`
Class C	First bit is `110-` Any address from `192.0.0.0` to `223.255.255.255`
Class D	First bit is `1110` Any address from `224.0.0.0` to `239.255.255.255`
Class E	First bit is `1111` Any address from `240.0.0.0` to `255.255.255.255`

Class D addresses are reserved for multi-casting protocols, which send a packet to a group of hosts in one movement. Class E addresses are reserved for future and experimental use and are largely not used.

Traditionally classes A through C divided the networking and host portions of the address differently to accommodate different sized networks. Class A uses the remainder of the first octet to represent the network and the rest of the address to define hosts. Class B uses the first two octets for network definition and the rest for host definition. Class C uses the first three octets to define the network and the last one for host definition. However, this has largely been replaced.

For instance, let's take the address `192.168.0.15`. From the address, we can see it is class C. If we break it up to see the network and the host, we see that `192.168.0` describes the network, and `15` describes the host.

There are portions of the IPv4 space that is reserved for specific use. For instance the address from `127.0.0.0` to `127.255.255.255` which is used by each host to test networking to itself. Each of the classes A to C has a range within them that is used to designate private network addresses. For A, it is between `10.0.0.0` to `10.255.255.255`, and for B, it is between `172.16.0.0` to `172.31.255.255`. For C, it is between `192.168.0.0` to `192.168.255.255`.

Netmasks and Subnets

Subnetting is the process of dividing a network into smaller network sections. By default, each network has only one subnet containing all of the host addresses defined within. A **netmask** is basically a specification of the amount of address bits used for the network portion. A subnet mask is another netmask used to further divide the network.

CIDR Notation

CIDR, or Classless Inter-Domain Routing, is a system that was developed as an alternative to traditional subnetting. With this you can add a specification in the IP address itself as to the number of significant bits that make up the networking portion.

For instance, we can express that `192.168.0.15` is associated with the netmask `255.255.255.0` by using the CIDR notation of `192.168.0.15/24` showing that the first 24 bits of the IP address given are considered significant for the network routing.

CIDR allows us more control over addressing continuous blocks of IP addresses.

Communication Protocols

Network communication protocols provide standards for creating and maintaining connections between network devices. They function like data delivery rules, affecting the speed of delivery, sequencing, and error recovery.

- **TCP (Transmission Control Protocol)** - chunks data into packets which can be sent across an IP-based network
- **IP (Internet Protocol)** - assigns sender and destination addresses to the header of a data packet
- **UDP (User Data Protocol)** - establishes low-latency and loss-toleration in communications between applications
- **HTTP (Hypertext Transfer Protocol)** - uses TCP/IP to deliver webpage content from a server to a browser
- **FTP (File Transfer Protocol)** - delivers files between computers on a network
- **DNS (Domain Name System)** - translates human-readable domain names into IP addresses that computers can understand

- **ARP (Address Resolution Protocol)** - converts an IP address to its corresponding physical address
- **RARP (Reverse Address Resolution Protocol)** - provides the IP address of the device given a physical address

> **DNS Server**
>
> The command `nslookup` gives you the IP address of the domain you are looking for.

Difference Between TCP and UDP

TCP/IP

- Connects with the receiving device before transmitting data
- Guarantees delivery to the receiving device
- Checks for errors
- Packets arrive in-order
- Guarantees deliverer does not overwhelm receiver with data
- Slower
- Cannot execute broadcasting tasks
- Used for email, HTTP, and HTTPS

UDP

- Faster
- Simple in transmission, limited data management
- Supports broadcasting
- Unreliable
- No retransmission of lost data packets
- Minimal error checking
- Packets may arrive out of order
- Can overload the receiver
- Used for video streaming, online gaming, etc.

Security Protocols

These protocols increase network security and can prevent cyberattacks.

- **SSL (Secure Socket Layer)** - creates an encrypted connection between a computer and a server

- **TLS (Transfer Layer Security)** - a more robust version of SSL
- **HTTPS (Hypertext Transfer Protocol Secure)** - modifies HTTP to use TLS and encrypt the connection between the web browser and a server
- **SSH (Secure Shell)** - provides an encrypted connection between a computer and a server and supports a variety of authentication methods

Internet Protocol Suite

The **Internet Protocol Suite** (or TCP/IP) shows how protocols can be combined to enable end-to-end communication between devices on an IP network. It is the 'Network Layer' of the OSI (Open Systems Interconnection) model. The Internet Protocol Suite consists of four layers.

- **Application Layer** - defines how network devices create and share data with other applications; concerned with using the appropriate protocol for the type of data being sent
  - Uses HTTP, TLS, and DNS
- **Transport Layer** - performs host to host communication
  - Uses TCP or UDP
- **Network Layer** - exchanges data packets across networks
  - Uses IP (v4, v6)
- **Link Layer** - networking methods which the host uses to communicate; physical mechanism for sending digital data
  - Ethernet or Wireless LAN

The OSI Model

The **Open Systems Interconnection (OSI) model** describes seven layers that systems use to communicate over a network. The modern Internet is based on the TCP/IP model, but the OSI model is widely used to help visualize and communicate how networks operate.

The seven layers (from top down) are the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer.

7. Application Layer

The application layer is used by end-user software like web browsers and email clients. The protocols in this layer allow software to send and receive information and present data to users. HTTP, FTP, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS) fall in this layer.

6. Presentation Layer

This layer prepares data for the application layer. It defines how devices should encode, encrypt, and compress data to be received correctly on the other end. It takes data transmitted by the application layer and prepares it to be transmitted over the session layer.

5. Session Layer

The session layer is responsible for creating communication channels (sessions) between devices. It opens sessions, ensuring they stay open while data is transferred, and closes them when the communication ends. It can set checkpoints during a data transfer so that if a session were to be interrupted, devices can resume the transfer from the last checkpoint.

4. Transport Layer

This layer takes data transferred in the session layer and breaks it into segments on the transmitting end. It reassembles the segments on the receiving end, turning it into data that the session layer can use. It carries out flow control, sending data at a rate that matches the receiving device's connection speed. It also carries out error control, ensuring that the data was received correctly.

3. Network Layer

This layer breaks up segments into network packets before reassembling the packets on the receiving end. This layer also routes packets by discovering the best path across the physical network, using network addresses to route packets to a destination node.

2. Data Link Layer

This layer establishes a connection between two physically-connected nodes on a network and then breaks up packets into frames before sending them to the destination. It has two parts: the Logical Link Control (LLC) and the Media Access Control (MAC). LLC identifies network protocols, performs error checking, and synchronizes frames. MAC uses MAC addresses to connect devices and define permissions to transmit and receive data.

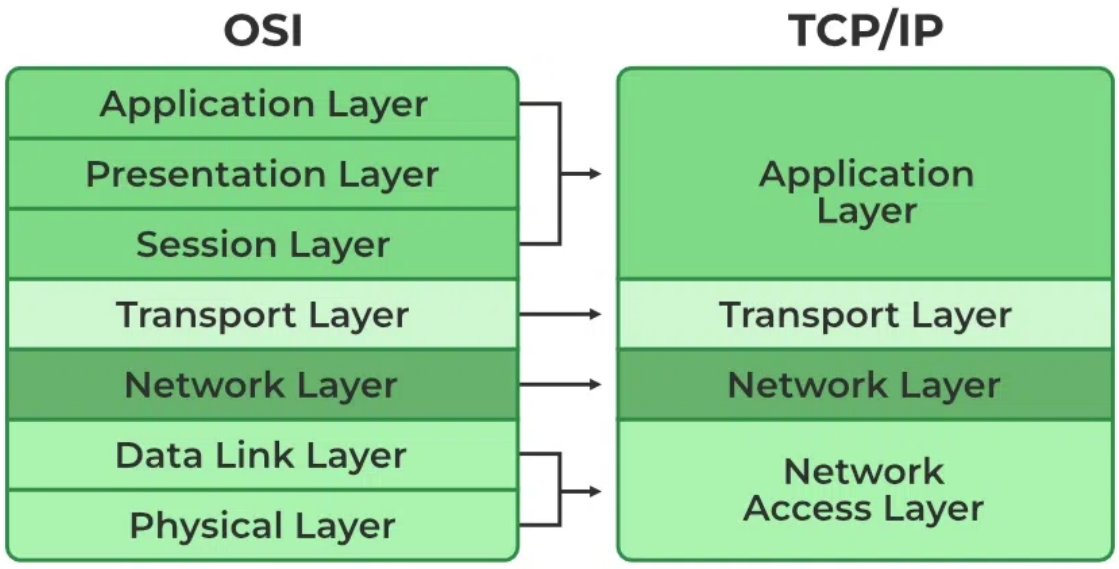
1. Physical Layer

The physical layer is the physical cable or wireless connection between network nodes. It defines the connector (the electrical cable or wireless technology connecting the devices) and transmits the raw data (a series of 0s and 1s) while taking care of bit rate control.

TCP/IP vs OSI

- TCP/IP is simpler and combines several OSI layers into one
  - OSI layers 5, 6, and 7 are combined into the Application Layer in TCP/IP
  - OSI layers 1 and 2 are combined into one Network Access Layer in TCP/IP

- TCP/IP is a functional model based on standard protocols while OSI is a generic, protocol-independent model that describes all forms of network communication
- TCP/IP applications use all the layers while for OSI simple applications do not use all of them as only layers 1, 2, and 3 are mandatory

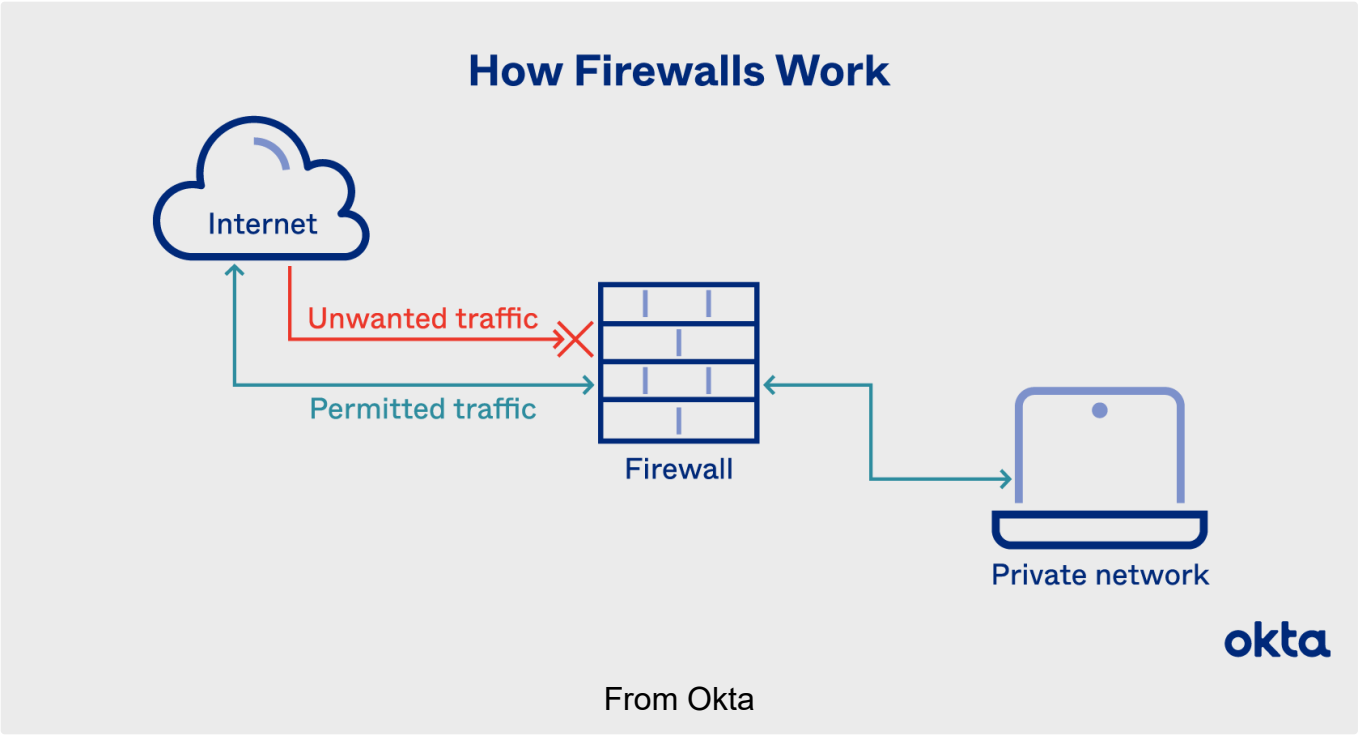


Difference between OSI and TCP/IP (From GeeksforGeeks)

Firewalls

Firewalls are a main tool for network security, acting as a checkpoint where data being passed is reviewed before being accepted or rejected. Network firewalls shouldn't be confused with host based firewalls that are on a single computer. Host based firewalls know about applications and vulnerabilities on a machine or VM whereas network firewalls focus on the traffic going from Internet to a secured LAN and vice versa.

There are different types of security functions used by firewall programs, but most use two or more to provide protection.



From Okta

- **Web Application Firewall** - blocks common types of attacks, like Distributed Denial of Service (DDoS); simple and cheap but susceptible to novel forms of attack unfamiliar to it
- **Packet Filtering** - reviews each data packet that passes through it before accepting or rejecting it based on user-defined rules; effective but difficult to block all possible threats
- **Circuit-level Gateway Implementation** - activates security sweeps when a new TCP/IP or UDP connection links to the system; once the connection and source is deemed secure, data can pass through
- **Proxy Server** - masks the network address of connected devices, directing requests made through an alternative cover device; adds anonymity and filtering with the proxy device acting as a buffer, sending back only specified types of data; slows network performance by adding an additional node to travel through

Sources

1. OSI Model
2. Networking 101: the basics of computer networks and the internet
3. Computer networking 101: Terms, tools, and getting started
4. Basics of computer networking
5. Firewall: Definition, How They Work, and Why You Need One
6. Network Based Firewall vs Host Based Firewall
7. Understanding IP Addresses, Subnets, and CIDR Notation for Networking