

Cybersecurity Professional Program

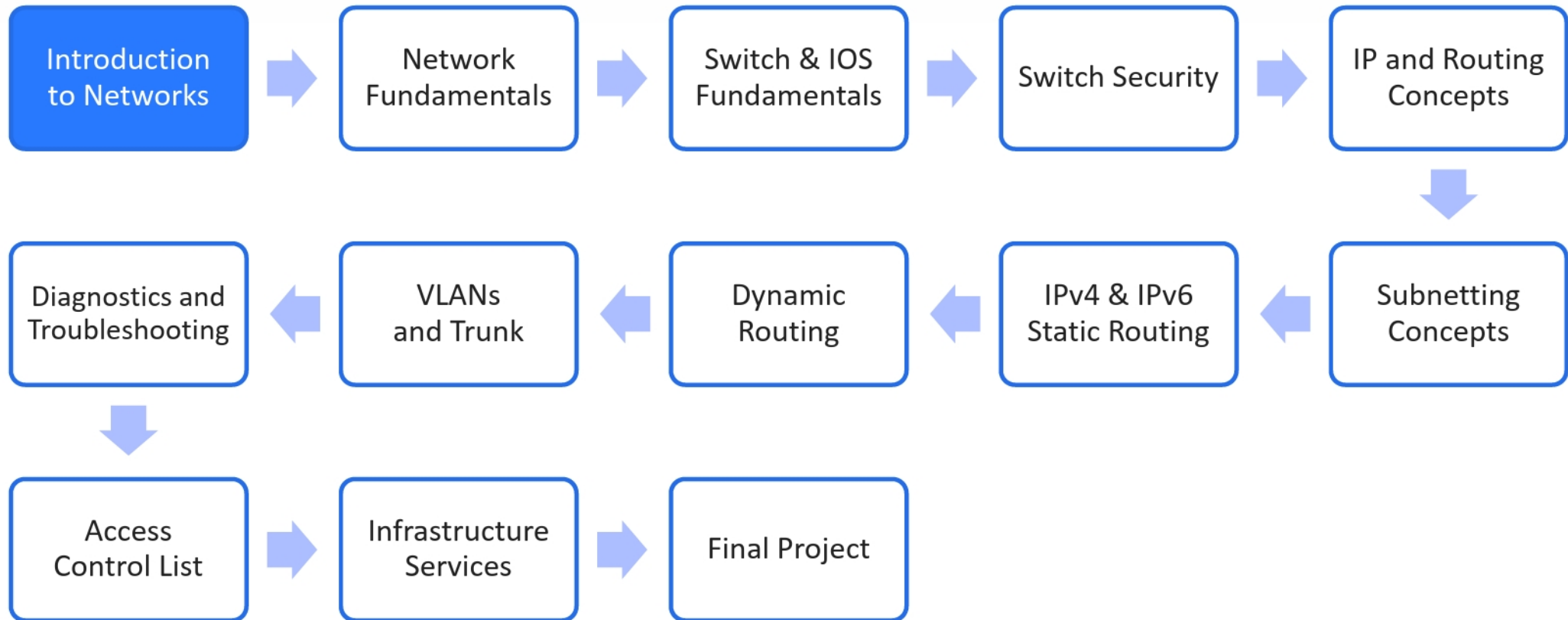
---

# Introduction to Networks

Computer Networking

# Computer Networking Course Path

---



# Overview

---

## Lesson Objective

This lesson is the starting point for networking.

It teaches basic concepts and technologies of network structures, topologies, and devices.



Network Types and Devices

Network Media and Cables

Network Topologies and Architecture

Network Protocols and Commands

Wireless Technology

Introduction to Networks

# **NETWORK TYPES AND DEVICES**



# Why is Networking Necessary?

## Communication



Communication is an essential characteristic of any society.

In today's world, people communicate with other people around the world almost as simply as they talk to a person standing right beside them.

Over the past several decades, global communication has advanced significantly and has greatly improved the human social experience.

Communication over a network (networking) brings people together for either generic or specific purposes.



A network is basically two or more devices that communicate with each other and share information.

# Common Types of Networks

## LAN



A Local Area Network defines a small geographical area in which multiple computers and other devices are connected. LANs can be set up in homes and small businesses, and can be managed individually or centrally.



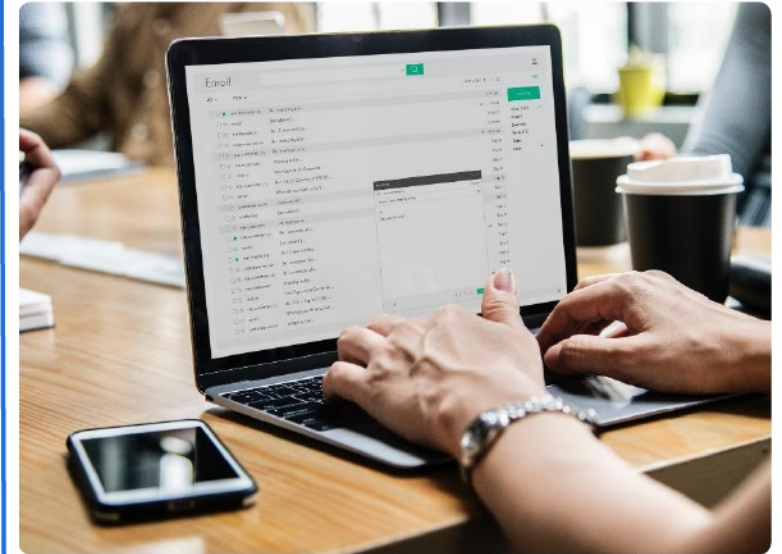
## WAN



A Wide Area Network is spread across an unlimited geographical area and connects between multiple LANs. WANs are usually managed by several service providers.



## Computer



LANs can be designed to use one of two communication methods: Wired or Wireless

# Other Types Of Networks

## MAN



A Metropolitan Area Network is larger than a LAN but smaller than a WAN. In most cases, it is managed by a city municipality and enables connection to broader networks.



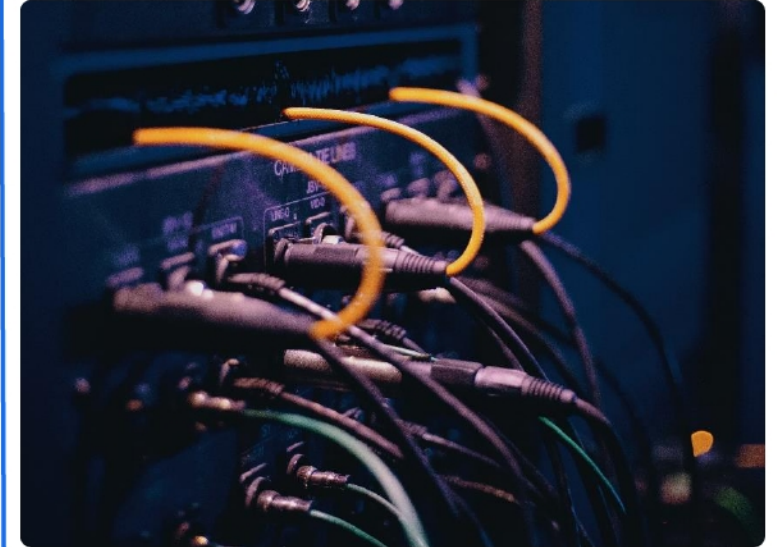
## SAN



A Storage Area Network is a dedicated network that supports file servers and provides efficient transfer of unusually large data sizes at extremely high rates.



## Network Center



SAN is often not regarded as a type of network because it is closer to being infrastructure.

# Network Structure

---

## Network Requirements



Communication among devices can be as simple as connecting a cable between two computers.

On the other hand it can be as complex as a large assembly of multiple networks spread around the world and regulated by a variety of sophisticated devices and protocols.



The history of computer networks began in the 1960s with a network called ARPANET.

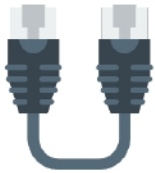
# Network Devices

## End Devices



Devices that connect to a network for communication purposes, such as computers, phones, and others. All end devices have unique addresses that identifies them on the network.

## Media



'Media', based on the word 'medium' (meaning 'in between') is a means of transferring data, such as metallic wire, glass or plastic fiber, wireless radio frequencies, and others.

## Intermediary Devices



Devices that transfer messages over the network and facilitate communication between end devices.

## Network



# End Devices

In today's world, most people communicate with each other through networks.

**End devices** are source or destination devices in a networked system.

Computers, laptops, and phones are **end devices** that allow us to communicate over a network.

End devices must have the ability to connect to a network via an **NIC**, to be able to send and receive information.

## Devices





# Network Interface Card (Media)

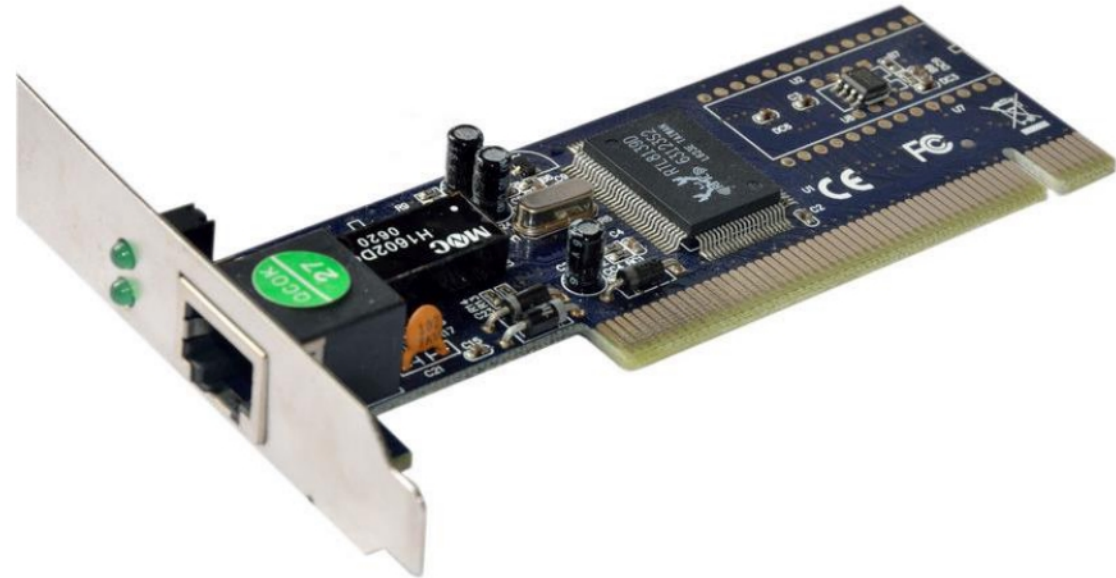
To allow an end device to send and receive information over a network it must have the appropriate hardware.

A Network Interface Card (NIC) allows end devices to interact with other devices over a network.

Other names for NIC include:

- Network Adapter
- LAN Adapter
- Physical Network Interface

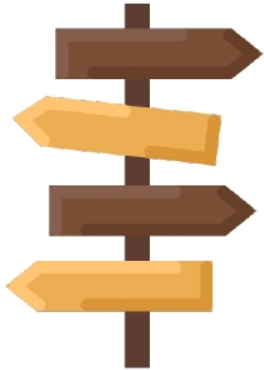
NIC



# Intermediary Devices

---

## Definition



Intermediary devices act as bridges, interconnecting end devices. Smart intermediary devices know how to differentiate between devices, and can send data to specific destinations.



Unlike smart devices, simple intermediary devices send information indiscriminately across a network.

# Switch

For multiple end devices to communicate with each other, a mechanism needs to be set up to handle the transfers.

A **Switch** is a device with physical ports to which end devices can be connected via Ethernet cables, to create a network.

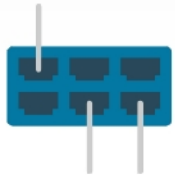
Switches use MAC addresses to pass information from one end device to another.

## Switch



# Switch Types

## Hub



A hub is the legacy implementation of a switch. It broadcasts data to all connected devices, as opposed to sending information to dedicated destinations.

## Layer 2 Switch



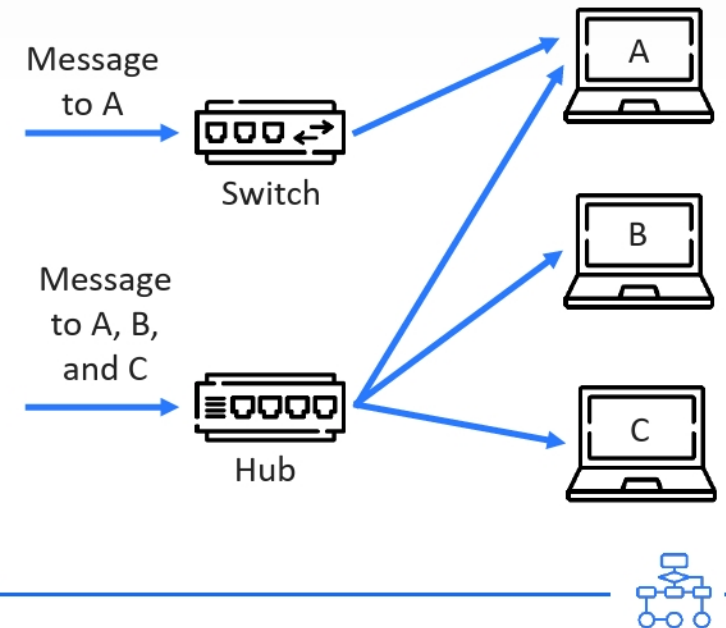
This is the most common and basic switch in use. It uses MAC addresses to forward information to specific destinations within the network.

## Layer 3 Switch



A layer 3 switch performs the same operations as a layer 2 switch, but can also function as a router if it is configured to do so.

## Switch Vs. Hub



# Broadcast & Collision Domains

## Communication



A collision domain is a group of nodes that can 'hear' each other. Ideally, when one node talks, all the others only listen. When two nodes talk at the same time, a collision occurs. To resolve this issue, a hub creates collision domains.

A switch, which operates in Layer 2 of the OSI model, can create separate conversations between nodes, which, in turn, creates separate collision domains.

Although collisions are expected to occur in a half-duplex Ethernet network, if a collision domain becomes too big, traffic problems will arise, due to re-transmissions.



# Broadcast & Collision Domains

---

## Communication



Broadcast is a type of communication whereby the sender sends a single copy of the data to all devices on the same network segment.

Broadcast communication must be used, since protocols such as ARP and DHCP rely on it.

A broadcast domain includes devices that receive broadcast packets originating from senders within the same network segment.

Routers operate in the network layer and separate both collision domains and broadcast domains.





# Duplex Modes

## Half Duplex

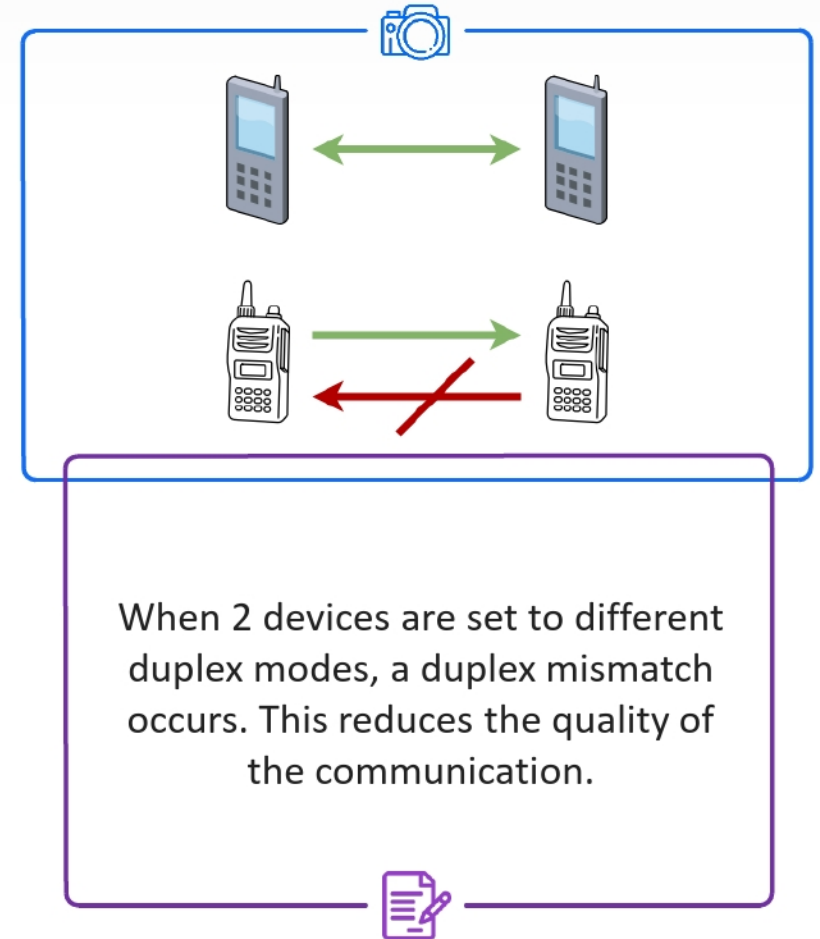


Only one party can send or receive data at a single moment. For example, a walkie-talkie works in half duplex.

## Full Duplex



Both parties can send and receive data at the same time. For example, a phone call is performed in full duplex.



When 2 devices are set to different duplex modes, a duplex mismatch occurs. This reduces the quality of the communication.

# Router

While **switches** allow devices to interact in the same network, **routers** allow them to communicate with different networks.

A **router** connects networks and allows communication between end devices in different networks.

Routers use IP addresses to route information among networks.

## Router



# Other Devices

## Access Point



Access points allow end devices to connect to a network wirelessly and manage information transmission.

A wireless device user can connect to a wired network via a properly configured access point.

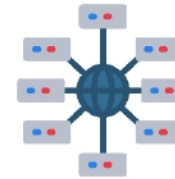
## Firewall



Firewalls are effective security tools against threats that originate from outside a network.

Firewalls implement filters that allow or block the transfer of information in a given direction.

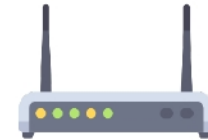
## WLC



A Wireless LAN Controller allows the configuration of multiple APs to be managed from a central device.

This is useful in large organizations where multiple APs are deployed in different sections of a building.

## Home Router



The home router combines the features of all the intermediary devices covered in this lesson so far, in a single device.

It acts as an AP, a switch, and a firewall with the most basic configuration.

Introduction to Networks

# **NETWORK MEDIA AND CABLES**

# Media

---

## What does Media do?



Information cannot be transmitted over a network without a means of transportation.

The term 'media' refers to the physical cables or wireless technologies used to pass the information from one device to another.

Different types of media feature varying speeds and distances of data transfer.



Connections between continents were made possible using “submarine cables” that were stretched across thousands of kilometers through the oceans.

# Ethernet Cable

The most common way to connect to a network is via an **Ethernet cable** with an **RJ-45** connector.

Cables are made of copper and can transmit information in the form of electrical signals.

Signals deteriorate as the distance grows, and due to the influence of RFI & EMI, which limits the cable length.

## CAT5e Cable





# Ethernet Cable Types

Over the years, network speed has increased and cable standards were modified accordingly.

## Cable Categories

| CABLE  | SPECIFICATIONS                                                                                    |
|--------|---------------------------------------------------------------------------------------------------|
| CAT-5  | Maximum length of <b>100m</b> , maximum speed of <b>100 Mb/s</b>                                  |
| CAT-5e | Maximum length of <b>100m</b> , maximum speed of <b>1 Gb/s</b>                                    |
| CAT-6  | Maximum length of <b>100m</b> , maximum speed of <b>1 Gb/s</b> (Note: Supports 10 Gb/s for 55m)   |
| CAT-6a | Maximum length of <b>100m</b> , maximum speed of <b>10 Gb/s</b>                                   |
| CAT-7  | Maximum length of <b>100m</b> , maximum speed of <b>10 Gb/s</b> (Note: Supports 100 Gb/s for 50m) |



# Ethernet STP & UTP

## UTP



Unshielded Twisted-Pair is the most common copper cable in use. It consists of four twisted pairs of colored wires. The act of twisting the wires is done to prevent signal disruption (cross-talk).



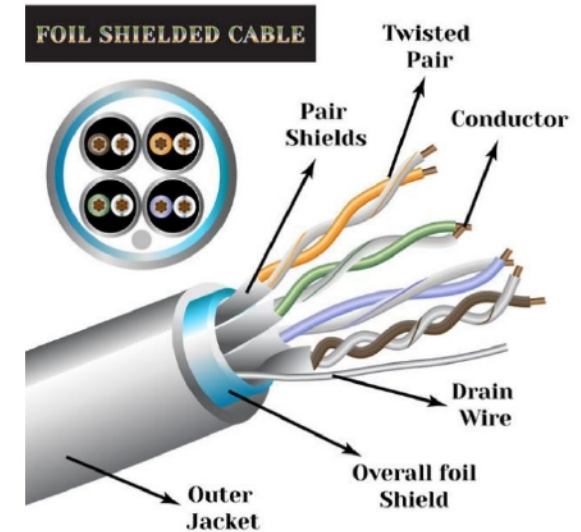
## STP



Shielded Twisted-Pair cables are similar to UTP, but have additional protection against EMI and RFI interferences. Each twisted pair is wrapped in foil.



## Cables



EMI & RFI are electromagnetic and radio frequency interferences that can affect signals.

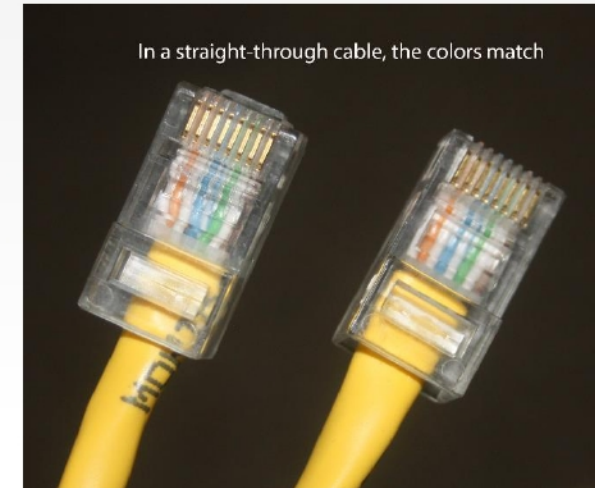
# Ethernet Cable Configurations

## Straight-Through

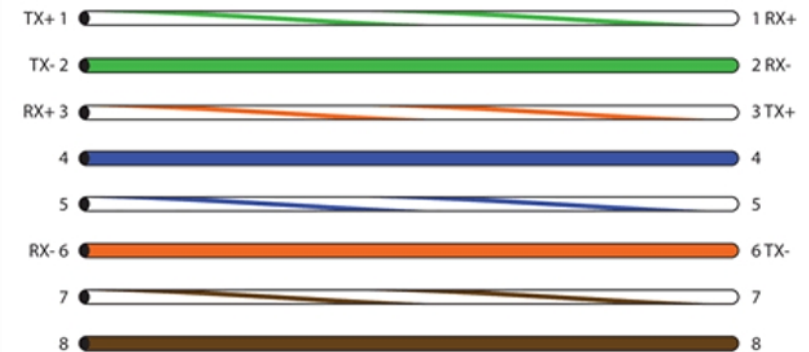


Wires are placed in a straight formation from side A to side B. This form is used for cables that are meant to connect network devices of different types, such as a switch and an endpoint.

- Each cable is connected straight to the matching pin on the other side.



## Straight-Through



Rollover is another type of cable used to connect intermediary devices.

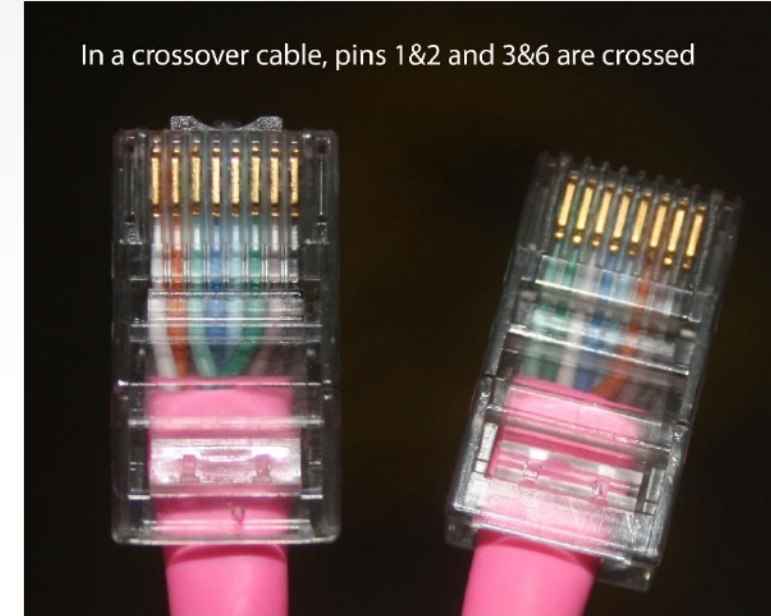
# Ethernet Cable Configurations

## Crossover

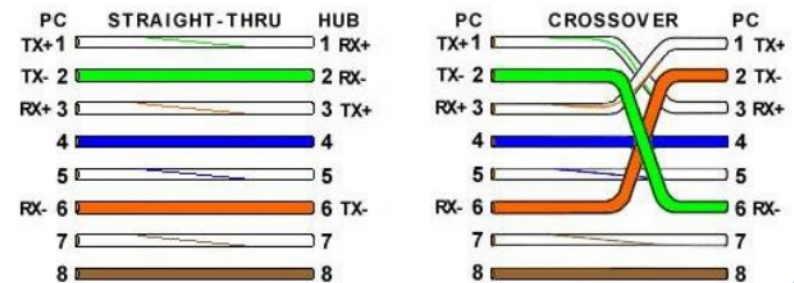


Wires crisscross from side A to side B. This form is used in cables that are meant to connect similar network devices.

- Pins 1 & 2 are crossed
- Pins 3 & 6 are crossed
- T568A to T568B



## Crossover



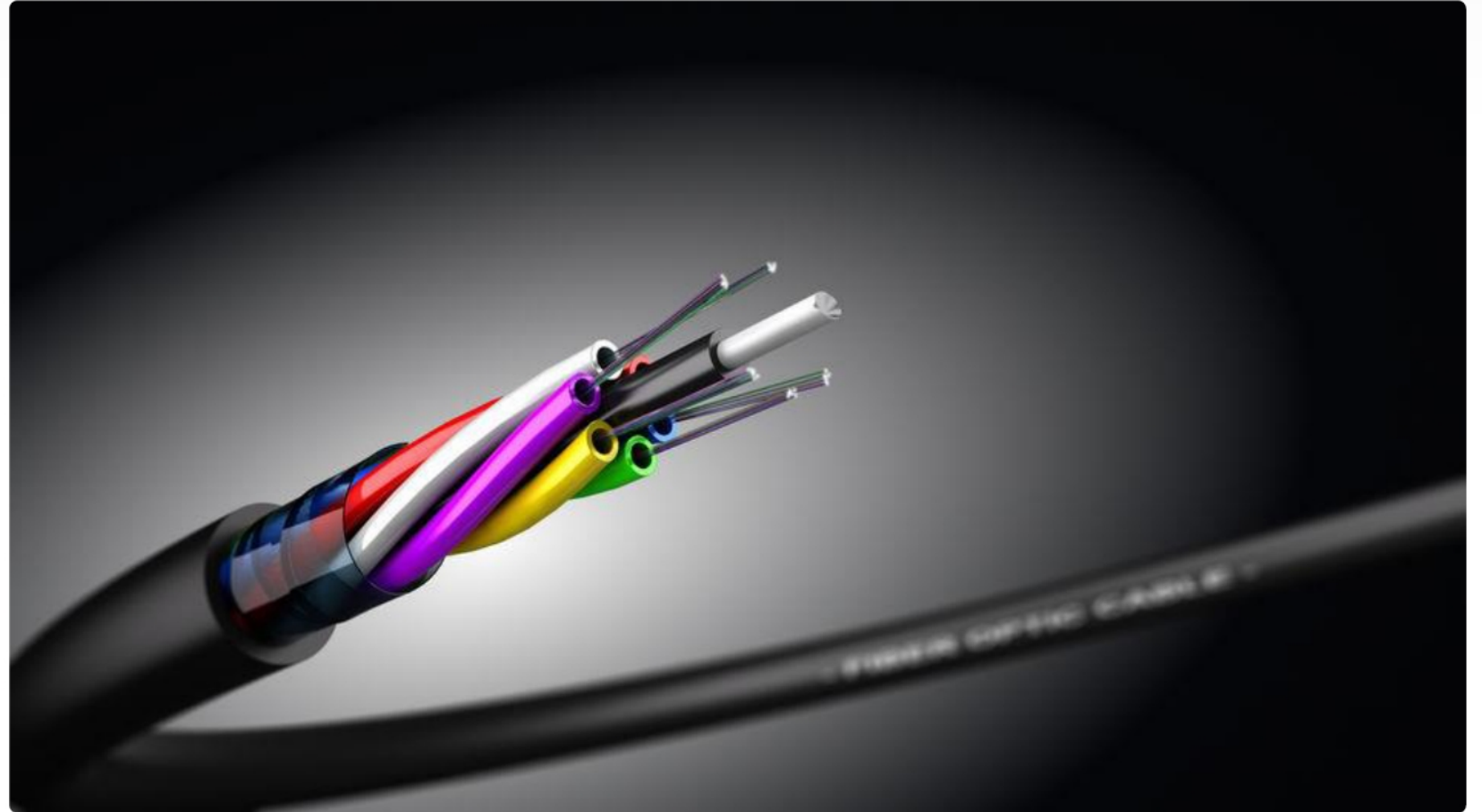
# Fiber Media

Ethernet cables have a length limit of 100m. A different type of cable is used for greater distances.

Optical Fiber Cables transmit information using light, at high speed, over long distances.

These cables are not sensitive to RFI & EMI, but aren't as flexible as Ethernet cables, and are more expensive.

## Fiber Cable



Introduction to Networks

# **NETWORK TOPOLOGIES AND ARCHITECTURE**



# Network Topology

## Definition



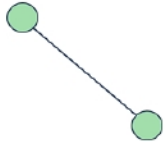
A network topology describes the structure of a network.  
It represents all the connections between all components in a network.  
Several types of topologies can be used to construct networks.



A topology represents the resources of a network, but not locations and distances.

# Network Topologies

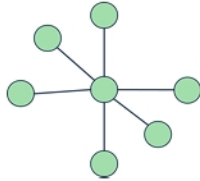
## Point To Point



A connection between two computers, networks or other devices.

If the connection fails, the communication is disrupted.

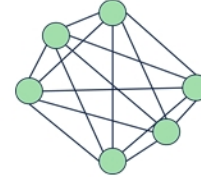
## Star



In a star topology all end devices are connected to a central intermediate device.

This type of topology is easy to set up and maintain. It is also highly scalable.

## Mesh



In a mesh topology each end device can have multiple connections to other end devices.

This configuration is highly resilient, due to its allowance of multiple connections, but it is also expensive and very difficult to maintain.

## Hybrid



A hybrid topology is a combination of other topologies.

Although a hybrid configuration takes advantage of the strong points of other topologies, it also has to deal with the disadvantages of those topologies as well.

# 3-Tier Architecture

---

## Definition



The concept of a 3-Tier Architecture can be applied to any type of network.

The model helps design, implement, and maintain a scalable, reliable, and cost-effective network.

Its simplistic structure makes it very easy to manage.

The combination of these attributes means that it is the best choice for large enterprises, in which thousands of computers need to be interconnected, sometimes over an area that includes several buildings.



Each layer has its own features and functionalities, which reduces network complexity.

# 3-Tier Architecture

A 3-Tier architecture consists of three layers that provide isolation between devices, greater flexibility, more security options, and resilience.

The separated layers are:

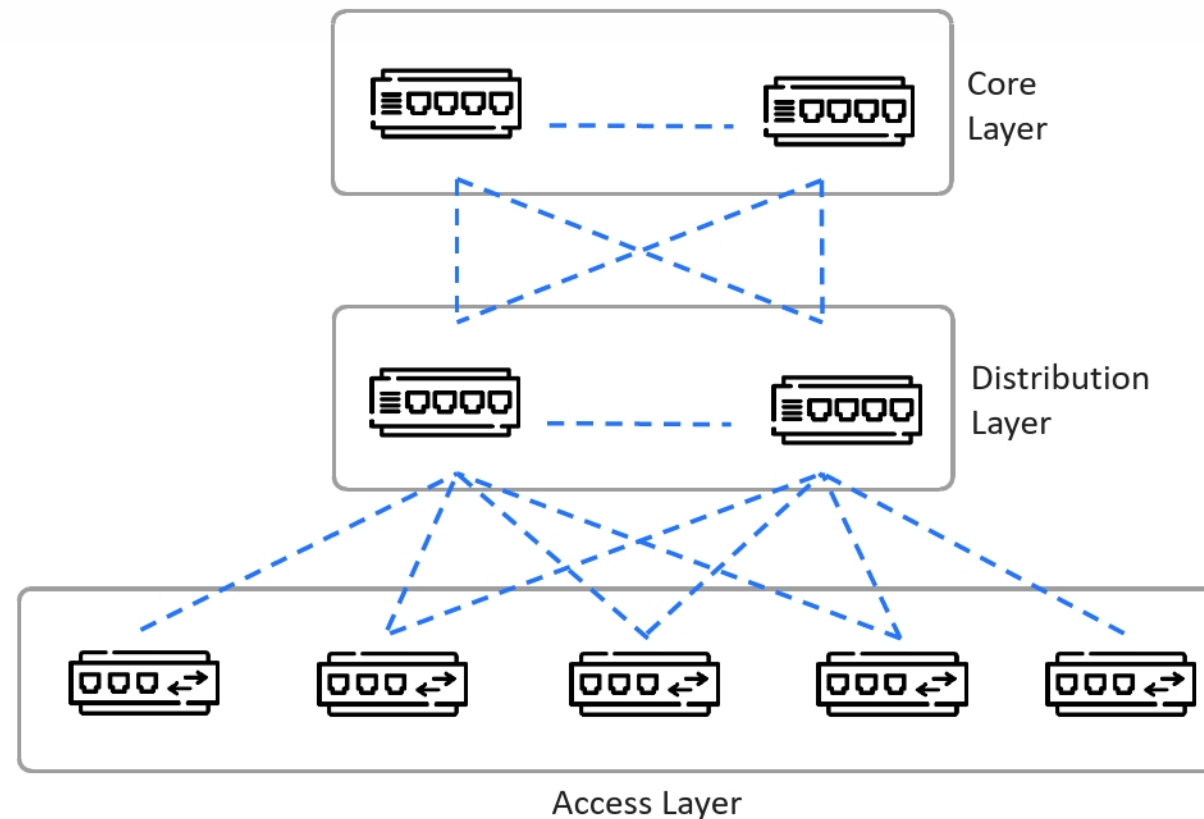
**Core** – routing layer connecting to servers and the Internet.

**Distribution** – separation between core and access layers, and boundary control.

**Access** – communication between end devices.

The layers can be managed independently without affecting other layers.

## 3-Tier Structure



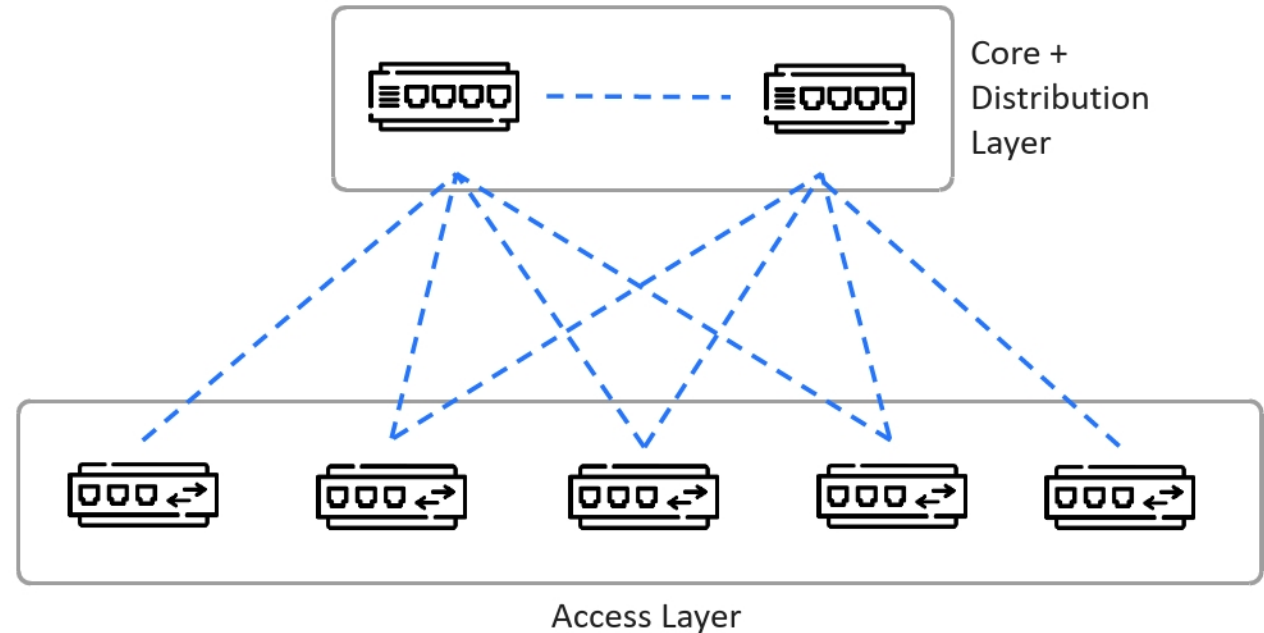
# Collapsed Architecture

This architecture is similar to 3-Tier, but has a different number of layers and a different scalability potential.

In this architecture, the core and distribution layers are collapsed together to form a single layer.

This means it has the advantages of the 3-Tier architecture, but a smaller network scale.

## Collapsed Layer Structure



# Physical & Logical Addresses

## Why do we need a computer address?



When the first networks were created for local computers to communicate with each other and share data, design engineers realized they needed to know how computers would talk to each other and who they could talk to.

The idea was for each computer to have a unique name or identification, and the concept of a MAC address was born.

A MAC address is the unique identity of a computer within a network, while IP addresses are used to identify machines operating in different networks.



Each network card in a device has both a MAC address and an IP address at any given moment.



# Physical Address

## Media Access Control



A MAC address is a unique hardware identifier attached to each network card. The address is static and should not be changed. It consists of six hexadecimal nodes ranging from 00 to FF.

A MAC address includes two parts:

- The first three nodes represent the manufacturer's identifier
- The last three nodes represent a serial identifier



A MAC address will usually be written like 00:0d:83:b1:c0:8e, or sometimes 000d.83b1.c08e

# Internet Protocol

An IP is used to uniquely identify computers on the network and create network partitions.

## IPv4



IPv4 addresses are the most commonly used today. They consist of four octets of numbers between 0-255, which can generate approximately four billion different addresses.

Some addresses, such as X.X.X.255, are special, while others, such as 192.168.X.X, are dedicated to specific uses.



## IPv6



Due to advances in technology, IPv4's four billion addresses were threatened with depletion, and IPv6 was developed with six hexadecimal octets that can generate approximately  $340 \times 10^{36}$  addresses.

IPv6 addresses have not yet been fully integrated in modern use cases.



# Network Classes

Subnet masks define which addresses in an octet can be used in an IP address, while remaining on the same network.

Devices (computers or network) must be in the same network and subnet to communicate without routing

The first IP address of each subnet is the network address and cannot be used for hosts or devices

The last IP address of each subnet is the broadcast address and cannot be used

## Class by Mask

**C**

|              | The network |       |       | The hosts |
|--------------|-------------|-------|-------|-----------|
|              | ←           |       |       | →         |
| IP address:  | 192         | . 168 | . 0   | . 0       |
| Subnet mask: | 255         | . 255 | . 255 | . 0       |

**B**

|              | The network |       | The hosts |  |
|--------------|-------------|-------|-----------|--|
|              | ←           |       | →         |  |
| IP address:  | 172         | . 16  | . 0 . 0   |  |
| Subnet mask: | 255         | . 255 | . 0 . 0   |  |

**A**

|              | The network | The hosts |     |     |  |
|--------------|-------------|-----------|-----|-----|--|
|              | ←           | →         |     |     |  |
| IP address:  | 10          | . 0       | . 0 | . 0 |  |
| Subnet mask: | 255         | . 0       | . 0 | . 0 |  |



Introduction to Networks

# **NETWORK PROTOCOLS AND COMMANDS**

# Communication Protocols

---

## Protocols



To properly communicate with each other, different devices require protocols.

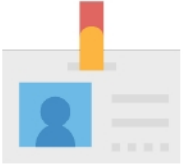
Protocols are predefined sets of rules describing how something should work or behave.

Protocols help maintain order among different technologies.



Protocols can be considered as 'languages' of data transfer. To communicate properly, two or more devices must first agree to use the same 'language'.

# Network Protocols

| IP                                                                                                                                                                                                 | DNS                                                                                                                                                                                        | DHCP                                                                                                                                                                                                        | HTTP                                                                                                                                                                                                  | HTTPS                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>The Internet Protocol is used to establish communication over the network, without delivery verification.</p> |  <p>Domain Name Service is a protocol used to translate domain names to IP addresses, and vice versa.</p> |  <p>The Dynamic Host Configuration Protocol is used to allocate IP addresses to new computers that join the network.</p> |  <p>The Hypertext Transfer Protocol is used to transfer text-based data, such as web pages, over the Internet.</p> |  <p>HTTPS is a secure implementation of HTTP. It encrypts the transferred data to prevent it from being intercepted.</p> |

# Network Commands

---

## The Importance of Commands



Commands are used in network configuration, maintenance, troubleshooting, and more.

It is essential for any network to frequently run commands that check the state of the network and monitor it.

Although some systems enable network configuration via a GUI, the configuration is still often done via the CLI.



An example of a powerful use of network commands is for error detection.



# PING

## Command

Ping x.x.x.x



Ping is the most common command in administrative networking activity.

It is used to check connectivity between computers over the network.

It also provides information such as connection speed and reliability.

## CMD

```
C:\Windows\system32> ping 8.8.8.8
```

```
Pinging 8.8.8.8 with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=224ms TTL=54
```

```
Reply from 8.8.8.8: bytes=32 time=681ms TTL=54
```

```
Reply from 8.8.8.8: bytes=32 time=319ms TTL=54
```

```
Reply from 8.8.8.8: bytes=32 time=103ms TTL=54
```

```
Ping statistics for 8.8.8.8:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 103ms, Maximum = 681ms, Average = 331ms
```



# IPCONFIG

## Command

`ipconfig`



`ipconfig` displays a computer's IP configuration.

It can also request a new IP address, if DHCP is configured.

**`ipconfig /all`** – displays extended information.  
**`ipconfig /release`** – drops an IP address.  
**`ipconfig /renew`** – requests a new IP address.

## CMD

```
C:\Windows\system32> ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fb21::b23e:28e9:c76b:7b35%11  
IPv4 Address. . . . . : 192.168.5.11  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.5.1
```



# NSLOOKUP

## Command

```
nslookup x.x.x.x
```



Computers use IP addresses to communicate with each other, while humans use names that are easier to remember than numbers.

**nslookup** sends a query to get the name of a computer by its IP address.

It can also do the opposite - query an IP address by the domain name.

## Code Example

```
C:\Windows\system32> nslookup www.cyber.com
Server:  pfSense.cl22b.lan
Address: 192.168.0.1
```

Non-authoritative answer:

```
Name:     cyber.com
Address:   199.244.49.102
Aliases:   www.cyber.com
```

```
C:\Windows\system32> nslookup 199.244.49.102
Server:  pfSense.cl22b.lan
Address: 192.168.0.1
```



# TRACERT

## Command

```
tracert x.x.x.x
```



Information in the network passes through multiple stations on the way to its destination.

**Tracert** displays all the stations along the route taken by the information to its destination.

It can work with a domain name or an IP address.

## Code Example

```
C:\Windows\system32> tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    pfSense.cl22b.lan [192.168.0.1]
  1  115 ms    70 ms    59 ms    192.168.1.1
  2  *         *         *        Request timed out.
  3  *         *         *        Request timed out.
  4  241 ms    170 ms    218 ms    172.17.10.182
  5  *         *         *        Request timed out.
  6  *         *         *        Request timed out.
  7  *         *         *        Request timed out.
  8  *         *         *        Request timed out.
  9  *         *         259 ms    core-213-57-0-69.PT.hotnet.net.il [213.57.0.69]
 10 281 ms    245 ms    225 ms    core-213-57-3-150.HFA.hotnet.net.il [213.57.3.150]
 11 201 ms    174 ms    228 ms    108.170.251.129
 12 188 ms    230 ms    326 ms    74.125.37.167
 13 131 ms    83 ms     109 ms    dns.google [8.8.8.8]

Trace complete.
```



# NETSH

## Command

Netsh [ command \ option ]



A fast way to configure network information is to use the **netsh** command.

It allows the configuration of the IP address, DNS, default gateway, and various network functions.

The example on the right shows how to set an IP address and verify settings using **netsh**.

## Code Example

```
C:\Windows\system32> netsh interface ip set address "Ethernet"
static 192.168.10.5 255.255.255.0 192.168.10.1
```

```
C:\Windows\system32> netsh interface ip show config
```

Configuration for interface "Ethernet"

|                                     |              |
|-------------------------------------|--------------|
| DHCP enabled:                       | No           |
| Default Gateway:                    | 192.168.10.1 |
| Gateway Metric:                     | 1            |
| InterfaceMetric:                    | 5            |
| Statically Configured DNS Servers:  | None         |
| Register with which suffix:         | Primary only |
| Statically Configured WINS Servers: | None         |



# Lab NET-01-L1

Local Network Configuration

30–60 Min.



## Mission

Learn and practice CLI network commands in Windows using CMD.

## Steps

- Local Network Configuration
- Test Connectivity
- Domain names & IP

## Environment & Tools

- Windows 7 / 8 / 10
- CMD

## Related Files

- Lab document

Introduction to Networks

# **WIRELESS TECHNOLOGIES**



# Wireless Networks

Wireless networks for computer communication are possible.

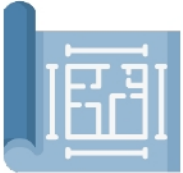
Wireless media features better flexibility than wired media, due to the absence of cables connected to end devices.

Information is transmitted using radio frequencies, which, however, do pose some security challenges.

## Wireless Network Structure



# Wireless Network - Security Issues

| Coverage Area                                                                                                                                                                                                                     | Transmission Interference                                                                                                                                                                                                                                                                                                          | Security                                                                                                                                                                                                                                           | Shared Medium                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>The ideal environment for this technology is open space.</p> <p>Some building materials can limit the range that wireless systems cover.</p> |  <p>Many common devices, such as microwave ovens, and various wireless communication devices, also transmit radio frequencies.</p> <p>These signals may interfere with signals transmitted in the wireless network and affect their quality.</p> |  <p>The absence of physical media exposes the network to the public and allows others to discover it and gain access to it, without authorization to do so.</p> |  <p>The technology operates in half-duplex, which means only one device can send and receive information at a time.</p> <p>When more and more users connect to the network, the available bandwidth for each user will decrease accordingly.</p> |

# Wireless LAN Components

## AP



Access point is the component that allows end devices to connect to a network wirelessly using radio waves. The access point itself will be connected to the network via cable.



## Wireless NIC Adapter



For a device to connect to a wireless network it must have a wireless NIC adapter to send and receive the information.



## NIC Conversion



Wireless NIC adapters can be implemented by an external device, or integrated in the computer.

# Wireless Technologies

## Wi-Fi



Wi-Fi, or wireless fidelity, is a technology based on IEEE 802.11 standards that allows connection to a network wirelessly using radio waves.

Wi-Fi is used for LAN networks in shared spaces.



## Wi-MAX



Wi-MAX is an implementation of wireless network connection over a wide area. It is used for LAN and MAN implementations.



## Bluetooth



Bluetooth is an implementation of WPAN (Wireless Personal Area Network). It is mainly used to pair devices and allows communication at up to 100 meters.



# Wireless Standards

Over the years, network standards were developed and modified to improve speed and bandwidth.

## Wireless Standard History

| STANDARD | MAX SPEED | FREQUENCY         | BACKWARD COMPATIBLE |
|----------|-----------|-------------------|---------------------|
| 802.11a  | 54 Mb/s   | 5 GHz             | NO                  |
| 802.11b  | 11 Mb/s   | 2.4 GHz           | NO                  |
| 802.11g  | 54 Mb/s   | 2.4 GHz           | 802.11b             |
| 802.11n  | 600 Mb/s  | 2.4 GHz & 5 GHz   | 802.11a/b/g         |
| 802.11ac | 1.3 Gb/s  | 5 GHz             | 802.11a/n           |
| 802.11ax | 14 Gb/s*  | 1 GHz - 7.125 GHz | 802.11a/b/g/n/ac    |



# Media Comparison

## Copper

10 Mb/s – 10 Gb/s

Up to 100 meters

Inexpensive

Vulnerable to the effects of EMI & RFI



VS

## Fiber

10 Mb/s – 100 Gb/s

Up to 100 Km

Expensive

Expensive equipment and implementation



VS

## Wi-Fi

54 Mb/s – 14 Gb/s

Depends on the transmitter's strength and receiver's sensitivity

Relatively Inexpensive

The signal can be affected by surrounding structures





An overhead, high-angle shot of three people sitting around a rustic wooden table. The person on the left is a woman with blonde hair, wearing a dark top, pointing with a blue pen at a laptop screen. The person in the center is a man with short blonde hair, wearing a light-colored shirt, looking at the same laptop. The person on the right is a man with dark hair, wearing a blue shirt, looking at a tablet. On the table are two laptops, a tablet, a smartphone, two coffee cups, and a document with charts. The scene is overlaid with a semi-transparent blue filter.

QUESTIONS?





THANK YOU

---