Networking Fundamentals

Quick Notes & Practical Guide, Version 1.0

Guide by

Ziksate

PREFACE

This guide introduces basic networking concepts and practical utilities to help build a strong foundational understanding. While it is not designed as a certification preparation resource, we hope it serves as a helpful starting point for learners new to networking. Minimal prior knowledge is expected, though not mandatory. Some topics are intentionally covered at a basic level.

Commands (including syntax) and utilities presented here generally work across most versions of Microsoft Windows. If you prefer to practice on other operating systems, please consult their respective documentation for equivalent commands, utilities, and syntax.

Screenshots are trimmed and edited for clarity. Actual results may vary depending on time, system configuration, and other factors. Product images, illustrations, and screenshots are provided for reference purposes only.

- Practical exercises are included—please refer to the Appendix.
- Worksheets are provided for comparing products; readers are encouraged to collect and analyze different products to understand features better.
- A quiz with answer keys is included to enhance the learning experience.

DISCLAIMER

The information in this guide is for general informational purposes only. While we strive to keep the content accurate and up-to-date, no warranties are made regarding its completeness, reliability, or suitability for any particular purpose. Use of the information is at your own risk.

The author has made every effort to ensure the accuracy of the information within this book was correct at time of publication. The author does not assume and hereby disclaims any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from accident, negligence, or any other cause.

UPDATES, CORRECTIONS & IMPROVEMENTS

Please visit www.ziksate.com for tutorials, updates, corrections & improvements.

FEEDBACK

Please provide your valuable feedback by visiting www.ziksate.com.

SUPPORT US

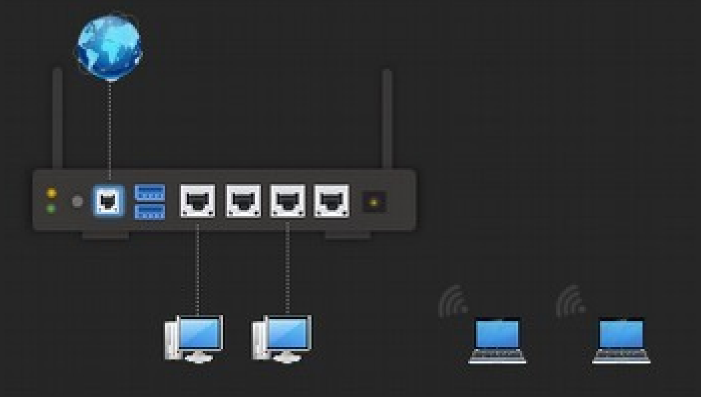
We believe great knowledge should be accessible to everyone. That’s why we are offering this ebook with no fixed price. You choose what it’s worth to you. Please click here to contribute.

OUR SINCERE REQUEST

Please do NOT re-upload this file elsewhere for others to download; if you want to share this guide, please provide a link to www.ziksate.com. Thank You!

RECOMMENDED SETUP

- SOHO/Wi-Fi Router
- 2 to 4 computers
- Active Internet Connection



Recommended Setup: One Router connected to Internet, 2 desktops (Wired) and 2 Laptops (Wireless)

Assumed setup in this guide are based on popular SOHO Router settings:

A. Router’s IP: 192.168.1.1
B. DHCP Range: 192.168.1.2 - 192.168.1.254
  a) Desktop 1 assigned 192.168.1.2
  b) Desktop 2 assigned 192.168.1.3
  c) Laptop 1 assigned 192.168.1.4
  d) Laptop 2 assigned 192.168.1.5
C. WAN Connectivity: DSL or Cable Modem
D. Wi-Fi: IEEE 802.11 a/b/g/n/ac

Important: Most SOHO Routers have the private IP range 192.168.x.x set by default; it is recommended to either login or, refer product manual to find out the correct IP range & settings.

Instructions

- Try with different IPv4 range/addresses once the exercises are clearly understood.
- Use different domains for testing, do NOT abuse domains, servers, hosts and/or networks in anyway.
- Set to “Private Network” (Microsoft Windows) instead of “Public Network”.
- Allow commands, utilities & services in Firewall settings (as required).
- Using | more at the end of certain commands displays one screen at a time; /?, help displays help.

Color Codes

🟨 Indicates commands to be used as it is.
🟦 Indicates values to be replaced.
◼ Indicates syntax is optional.

Commands & Utilities

For basic learning experience, commonly used command line utilities are included:

- HOSTNAME
- GETMAC
- IPCONFIG
- PING
- TRACERT
- NET
- NETSTAT
- ARP
- NSLOOKUP
- NBTSTAT

In addition, WMI & Powershell and few other utilities are introduced at very minimal level which may be explored on your own later.

Reference(s):

https://tools.ietf.org/html/rfc1574
https://en.wikipedia.org/wiki/Windows_Management_Instrumentation
https://en.wikipedia.org/wiki/PowerShell

Table of Contents

Introduction

Networking by definition, “Sharing of resources”. Networking refers to collection of devices (desktop, laptop, printer, smartphone, etc.) connected for the purpose of sharing and accessing resources. Networks are widely implemented in homes, offices, public places, etc.

Home Networks are usually simple and have fewer computers connected through devices that require almost minimal technical expertise to manage; on contrast, Enterprise Networks usually have devices that require specific product/technical expertise and may have hundreds to thousands of computers.

Resources that can be shared:

- Files
- Internet Connectivity
- Printers
- Storage Devices
- Scanners
- Optical Drive

Note: Some devices cannot be shared due to specific technical limitations.

Why share?

- Reduce costs (for example, a single printer can be shared across multiple computers).
- Security (restrict who can access shared resources).

Terminology

- Server Devices, provide resources.
- Client Devices, access resources.

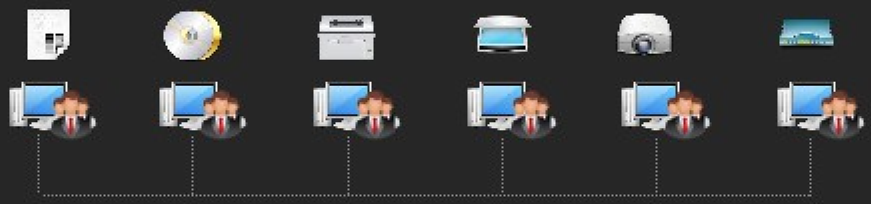
Standards

Networking specifications are well-documented through RFCs (Request for comments), which can be referred for in-depth understanding. There are thousands of RFCs available in plain text format, you may find links to handful of them in this guide.

Core Concepts

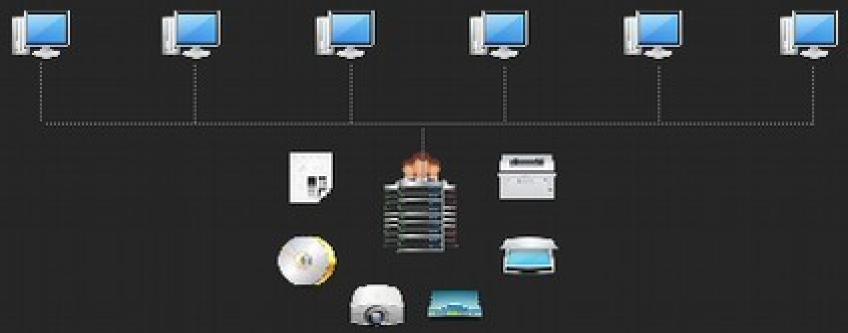
A. Conceptual types of networks

a) Peer-to-Peer: In this type of network, all computers can share resources directly with each other. Security is managed individually on each computer. Peer-to-peer networks are commonly used in home and small office environments and are typically suitable for around 10 to 30 computers (though this is not a strict limit).



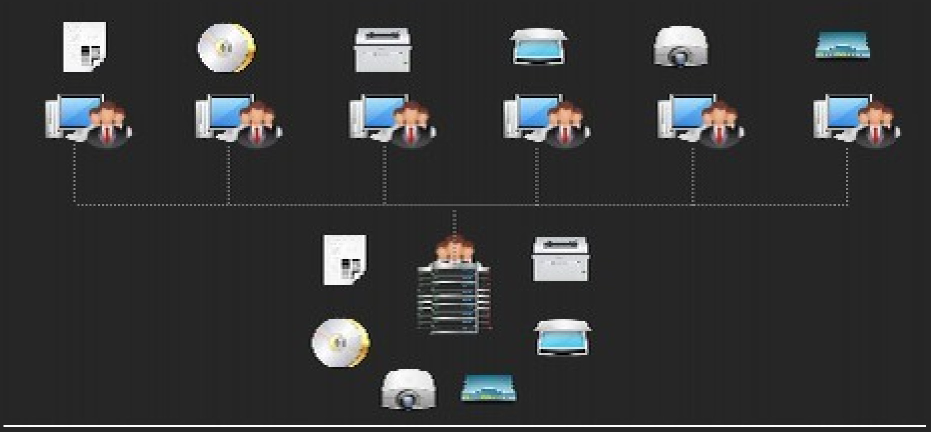
P2P: Each computer can share their resources, local security

b) Client/Server: In the Client/Server model, a single computer (called the server) provides resources or services to multiple client computers. A server can offer a single service or multiple services, depending on the administrator's configuration. Security is typically centralized, making it easier to manage and enforce across the network.



C/S: Resources shared from one main computer

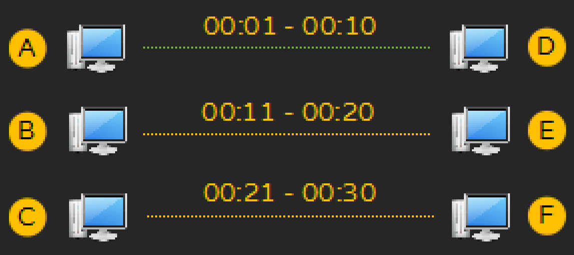
c) Hybrid: A hybrid network combines elements of both Peer-to-Peer and Client/Server models. It is a mixed (heterogeneous) setup, allowing flexibility in how resources are shared and managed. The exact configuration depends on the administrator's preferences and the needs of the network.



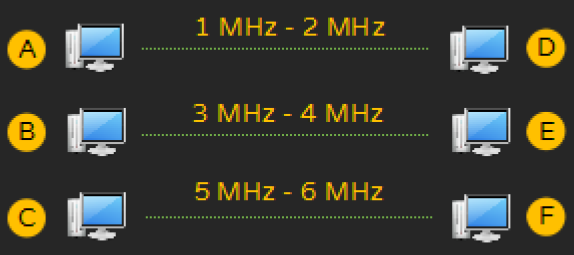
Hybrid: Mix of both P2P & Client/Server model

B. Signaling Methods

- Defines how communication happens using electric, optical or radio signals.
- Types
  - Baseband
    - Digital Signals
    - Use entire bandwidth
    - Uses TDM (Time-division Multiplexing), send multiple signals at different time intervals
    - Very high transfer rates
    - Example: Ethernet
  - Broadband
    - Analog Signals
    - Use part of the bandwidth
    - Uses FDM (Frequency-division Multiplexing), send multiple signals at different frequencies
    - Speed usually less when compared to Baseband, depends on technology
    - Example: DSL



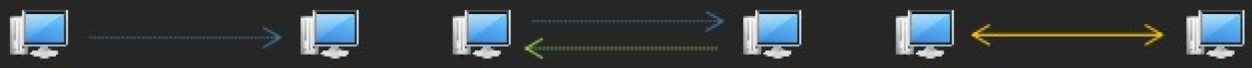
TDM, time sharing - one at a time



FDM, same time at different frequencies

C. Channel Operation

- Defines mode of communication between devices on a network.
- Types
  - Simplex: One way communication (Similar to a Radio).
  - Half-Duplex: Two ways, but only one way at a time (Similar to a walkie-talkie).
  - Full-Duplex: Both ways at the same time (Similar to a telephone).



Simplex *Half-Duplex* *Full-Duplex*

D. Data Transmission methods

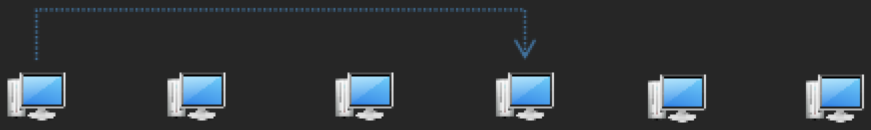
- Defines how data is transferred over a network.
- Types
  - Circuit Switching: Dedicated physical path (circuit) is established before transferring data; no other device can use the path until termination. Example: Dial-Up Networking.
  - Packet Switching: Data is divided as packets and sent through different paths, enabling multiple devices to communicate at the same time. Example: IP (Internet Protocol) Networks.

E. Channel Access

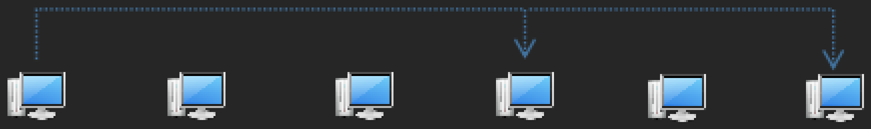
- Defines how devices should use shared medium for communication.
- Types
  - CSMA/CD (Carrier Sense Multiple Access/Collision Detect): Only one device can transmit at a time and other devices should "listen" before transmissions to avoid collisions. When two devices communicate at the same time, a collision occurs. If collision is detected, devices should retry transmissions after random interval.
  - CSMA/CA (Carrier sense multiple access with collision avoidance): Similar to CSMA/CD, designed for wireless networks. Devices sense if a channel is "idle" before transmissions.

F. Addressing Methods

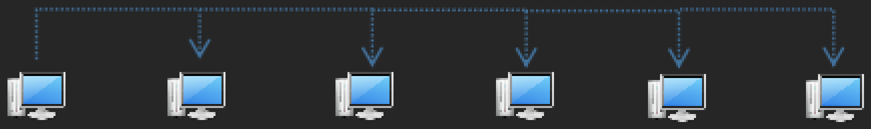
- Defines how signals should be addressed
- Types: Unicast, Multicast & Broadcast



Unicast: One device to a specific device on a network.



Multicast: One device to selective devices on a network.



Broadcast: One device to all other devices in a network.

G. Network Classification

- PAN (Personal Area Network): Refers to network connections within limited range, like Smartphone & computer typically connected using Wi-Fi, Bluetooth, etc.
- LAN (Local Area Network): Refers to networks within a limited geographic area such as within a building, home or an office.
- MAN (Metropolitan Area Network): Refers to networks within a city (but less than WAN).
- WAN (Wide Area Network): Refers to networks covering a large geography like different locations or countries.

H. Network Definitions

- Intranet: Refers to private networks operated by an organization.
- Extranet: Refers to private networks operated by an organization & and it's vendors/partners.
- Internet: Refers to interconnected computers across the globe.

Reference(s):

https://www.ietf.org/rfc/rfc1208.txt

I. Collision & Broadcast Domains

- Collision domain refers to a network segment where packets may collide with each other on a shared medium. Collision happens often on shared network medium such as the Ethernet (applies to Hub or Co-axial but not when using network switches).
- Broadcast domain refers to a area of network where a frame is forwarded to all devices.
- When two devices send packets at the same time, a collision may occur requiring re-transmission; in such cases, devices should attempt to resend packet again, after a random interval.
- Devices
  - Hub: Single Collision & Broadcast Domain (Possibility of collision is very high since all computers belong to a single collision & broadcast domain).
  - Switch: Single Broadcast Domain and each port is a collision domain (hence very effective in reducing & managing collisions).
  - Router: Different Collision & Broadcast domains.

Hub	Switch	Router
Layer 1	Layer 2	Layer 3
All Devices share one medium hence collision occurs.	Isolate collision domain but forward broadcasts.	Do not forward broadcasts

J. Types of Servers

- File Servers: Used for documents, images, etc.
- Print Servers: Allows users to access printers.
- Web Servers: Used for serving web pages.
- FTP Servers: Allows content such as documents, media files, etc. to be downloaded or uploaded.
- Mail Servers: Used for sending & receiving emails.
- Database Servers: Provides centralized access to databases.
- Game Servers: Allows users to play multiplayer games.
- Media Servers: Streams Audio & Video content.
- Domain Controllers: Used for centralized authentication.

Note: Any computer can act as a server or a client, depending on administrator's preference. For example a desktop operating system can function as a web server, if a web server software like Apache or IIS (Internet Information Services) is installed. However, using a desktop operating system as a server may have technical limitations as compared to a server operating system.

Software	Type	Platform / Operating System
Apache	Web Server	Microsoft Windows, Linux
Internet Information Services	Web & FTP Server	Microsoft Windows
FileZilla Server	FTP Server	Microsoft Windows, Linux
MySQL	Database Server	Microsoft Windows, Linux
Microsoft SQL Server	Database Server	Microsoft Windows
Microsoft Exchange	Email Server	Microsoft Windows
Zimbra	Email Server	Linux

Server Software

Server Hardware

More powerful than a typical desktop computer or a laptop. Hardware requirements for a server are determined based on (Not limited to):

- Server Operating System requirements.
- Type of service(s) being provided (web / email / storage, etc.) and associated software.
- Resource required for handling 100's to 1000's of client requests.

Options

- A single server can provide multiple services, usually requiring moderate to high-performance hardware.
- Multiple servers can be used to provide a single service, ideal for environments with heavy load demands.
- Multiple services can also be distributed across multiple servers for better performance and reliability.

Costs

- Server hardware costs vary depending on the components and required software licenses.
- Key considerations include CPU type, storage technology (HDD, SSD, NVMe), total storage capacity, RAM, network interfaces, and more—based on the server's intended role.
- It is recommended to seek **professional advice** to determine exact hardware requirements.
- Servers can be purchased, leased, or rented, depending on budget and preference.

Tower Model

Rack Model

Mini Model

Server operating systems

Server operating systems are designed to support higher number of CPU’s, large amounts of RAM and so on. For example, Microsoft Windows 10 (desktop operating system) can support only 2 physical processors but Microsoft Windows Server edition is designed to support 64 physical processors. Such limitations entirely depends on the edition/version of an operating system as defined by the vendor, which can be found in technical documentation.

Popular server operating systems include:

- Microsoft Windows Server Series
- Several Unix & Linux Editions
- Mac OS Server

Quiz 01

1. Networking is best defined as:

A. Sharing of Resources B. Connectivity between desktop computers
C. Connectivity between mobile computers D. The Internet

2. Resources that can be shared in a network:

A. CD-ROM Drive B. Hard Disk Drive C. Internet Connectivity D. All of the above

3. Maximum number of computers in a network:

A. 10 B. 20 C. 100 D. Unlimited

4. _____ defines network connectivity within a limited area such as a home or a small office network.

A. LAN B. MAN C. WAN D. PAN

5. _____ defines network connectivity between networks within a city.

A. LAN B. MAN C. WAN D. PAN

6. _____ defines network connectivity between networks across the globe.

A. LAN B. MAN C. WAN D. PAN

7. Acronym - LAN.

A. Limited Area Network B. Legacy Area Network
C. Local Area Network D. Local Assisted Network

8. Acronym - WAN.

A. World Area Network B. Wide Access Network
C. Wide Area Network D. Wide Assisted Network

9. Acronym - MAN.

A. Mini Area Network B. Metropolitan Area Network
C. Macro Area Network D. Metropolitan Assisted Network

10. Acronym - PAN.

A. Professional Area Network B. Personal Area Network
C. Pinned Area Network D. Pinned Assisted Network

11. _____ refers to a computer that provide resources.

A. Client B. Server C. Mobile D. Smart Net

12. _____ refers to computers that access resources.

A. Client B. Server C. Mobile D. Smart Net

13. _____ model utilizes centralized security.

A. Personal Network B. Peer-to-Peer C. Client-Server D. Mobile Area Network

14. _____ are referred to as service requestors.

A. Servers B. Clients C. Peer-to-Peer D. Client-Server

15. _____ are referred to as service providers.

A. Servers B. Clients C. Peer-to-Peer D. Client-Server

16. _____ refers to network of networks.

A. Intranet B. Internet C. LAN D. WAN

17. _____ refers to private networks used by organizations, not accessible by public.

A. Intranet B. Internet C. Peer-to-Peer D. Client-Server

18. In _____ data is sent as digital signals by using entire bandwidth of a media.

A. Broadband B. Baseband C. Digiband D. Analogband

19. In _____ data is sent as analog signals by using portion of a bandwidth.

A. Broadband B. Baseband C. Digiband D. Analogband

20. Examples of Broadband:

A. DSL B. Cable Internet C. Ethernet D. Both A & B

21. Example of Baseband:

A. Ethernet B. DSL C. Cable Internet D. Both B & C

22. Acronym - TDM.

A. Telecommunication Division Multiplier B. Time Division Multiplexing
C. Tele Division Multiplexing D. Transfer Division Multiplexing

23. Acronym - FDM.

A. Fast Division Multiplexing B. Fine Division Multiplier
C. Far Division Multiplexing D. Frequency Division Multiplexing

24. _____ refers to one-way communication.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

25. _____ refers to two-way communication but one direction at a time.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

26. _____ refers to simultaneous two-way communication.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

27. Acronym - CSMA/CD.

A. Collision Sense Multiple Access/Carrier Detect
B. Collision System Multiple Access/Carrier Detect
C. Carrier Sense Multiple Access/Collision Detect
D. Collision Sense Multiple Access/Carrier Divide

28. One-to-One communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

29. One-to-Many communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

30. One-to-All communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

31. Examples of Circuit switching networks:

A. PSTN B. ISDN C. GSM D. All of the above

32. Examples of Packet Switching Networks:

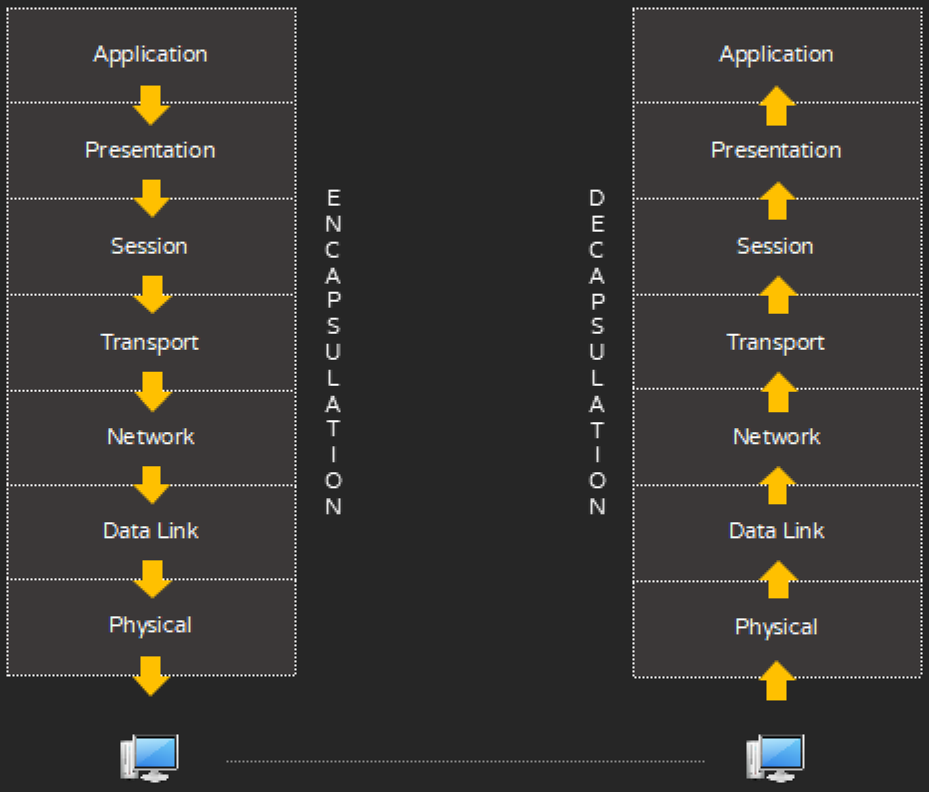
A. IP B. X.25 C. Frame relay D. All of the above

OSI Model

- Open Systems Interconnection, how computers should communicate.
- Introduced by by the International Standards Organization (ISO) in 1978.
- Conceptual model for networking, divided into 7 organized layers.
- Lays out standards for Interoperability between manufacturers.

Tip: OSI Model helps in understanding networking concepts layer-by-layer and can also be used as a foundation for step-by-step troubleshooting.

OSI Layers



Conceptual Flow in OSI Layer

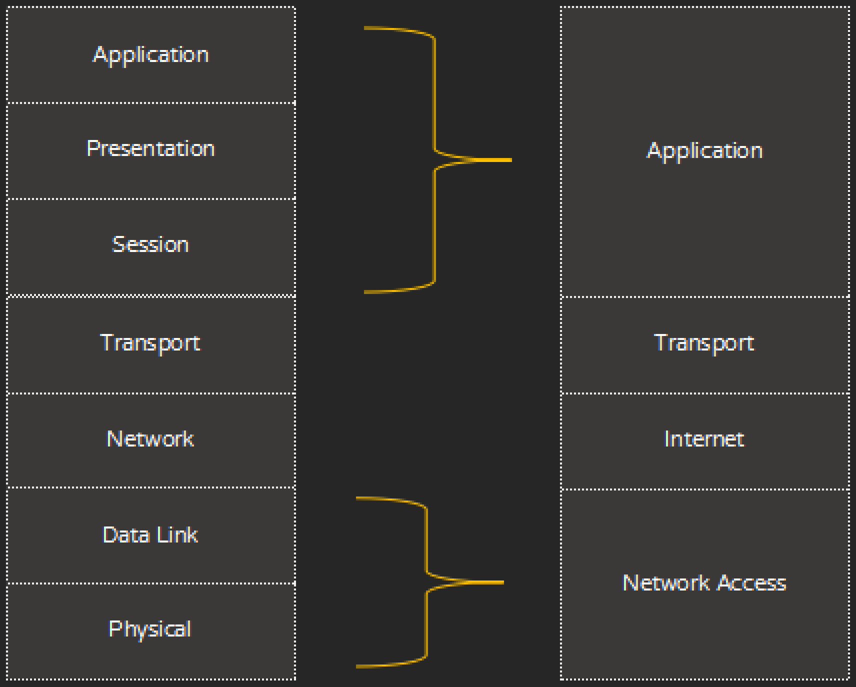
Layer	Name	Example
7	Application	End-user access (HTTP, FTP, SMTP)
6	Presentation	Data format, encryption, compression
5	Session	Session management, API calls
4	Transport	Delivery (TCP/UDP)
3	Network	Routing and IP addressing (IP, ICMP)
2	Data Link	MAC addressing, error detection
1	Physical	Cables, signals, hardware

PDU (Protocol Data Unit) is added at each layer in a process called “Encapsulation.” For example, when browsing the Internet—HTTP headers are added first, then the data is passed on to the Transport Layer where TCP headers are added, then to the Network Layer where IP headers are added, and so on. Similarly, decapsulation happens at the destination.

- Physical
  - Layer 1
  - Establishes and terminates connections.
  - Transmitting raw bits over a physical link.
  - Functional specifications for electrical, optical, radio waves, etc. defined in this layer.
  - Protocols in this layer: 1000BASE-SX, DSL, ISDN.
  - Unit of Measurement: Kbps, Mbps or Gbps.
- Data-link
  - Layer 2
  - Manages delivery of frames between nodes within a LAN segment.
  - Devices at this layer: Network Interface Cards, Bridges and Switches.
  - Protocols in this layer: Ethernet, PPP, SLIP, Token Ring.
  - Unit of Measurement: Frames (Data Packet).
  - Sub-divided into:
    - Logical Link Control (LLC): Provides support to link Multiple protocols.
    - Media Access Control (MAC): Provides physical addressing Scheme.
    - LLC + MAC = Data Link Layer.
- Network
  - Layer 3.
  - Packet forwarding and routing.
  - Protocols at this layer: IPv4, IPv6, IPX, RIP, OSPF.
  - Unit of Measurement: Packets or Datagram.
- Transport
  - Layer 4.
  - Connection oriented communication.
  - Sequencing & reliable delivery of packets.
  - Flow Control & Multiplexing.
  - Protocols at this layer: TCP, UDP.
  - Unit of Measurement: Segments.
- Session
  - Layer 5.
  - Manage sessions between end-to-end application processes.
  - Establish, Maintain & Terminate connections between applications.
  - Protocols at this layer: NetBIOS, PAP, PPTP, L2TP.
- Presentation
  - Layer 6.
  - Data formats and delivery of information.
  - Encoding/decoding, encryption/decryption, compression/decompression of data.
  - Protocols at this layer: ASCII, JPG, MIME, SSL, TLS.
- Application
  - Layer 7.
  - Provides Interface and protocols required by users.
  - Process-to-Process communication between hosts on a network.
  - Protocols at this layer: HTTP, FTP, SMTP, POP3, DNS, DHCP.

TCP / IP Model

- Simplified 4 Layer Conceptual Model



OSI vs TCP/IP Model

Internet protocol suite (Mapped to TCP/IP Model)

Layer	Protocols
Application	HTTP, FTP, SMTP, POP3, LDAP, SSL, TLS…
Transport	TCP, UDP, SCTP…
Internet	IP, ICMP, IPSec…
Link	ARP, PPP, Wi-FI, DSL, FDDI…

Quiz 02

1. Acronym - ISO.

A. Internal Standards Organization B. International Standards Organization
C. Internet Standards Organization D. Intranet Standards Organization

2. Acronym - OSI.

A. Open Systems Internet B. Open Systems Intranet
C. Open Service Interconnect D. Open Systems Interconnection

3. _____ is the first layer of the OSI Model.

A. Transport B. Network C. Data-link D. Physical

4. _____ is the second layer of the OSI Model.

A. Presentation B. Session C. Transport D. Data-link

5. _____ is the third layer of the OSI Model.

A. Presentation B. Session C. Transport D. Network

6. _____ is the top-most layer of the OSI Model.

A. Application B. Presentation C. Session D. Transport

7. Sub-layers of data-link layer are:

A. Session B. MAC C. LLC D. Application

8. _____ layer defines the electrical and physical specification.

A. Transport B. Data-link C. Physical D. Both A & B

9. _____ layer handles physical addressing.

A. Physical B. Data-link C. Application D. Presentation

10. _____ layer handles logical addressing and routing.

A. Presentation B. Network C. Session D. Transport

11. _____ layer handles end-to-end communications between devices on a network.

A. Data-link B. Application C. Presentation D. Session

12. _____ layer deals with standards for data formats; encryption & compression.

A. Physical B. Data-link C. Presentation D. Application

13. Examples of layer 1 protocols:

A. DSL B. RS-232 C. 100BASE-TX D. All of the above

14. Examples of layer 2 protocols:

A. Ethernet B. PPP C. Token Ring D. All of the above

15. Examples of layer 3 protocols:

A. IP B. IPX C. ICMP D. All of the above

16. Examples of layer 4 protocols:

A. TCP B. UDP C. SCTP D. All of the above

17. Examples of layer 5 protocols:

A. PAP B. PPTP C. L2TP D. All of the above

18. Examples of layer 6 protocols:

A. ASCII B. MIDI C. SSL D. All of the above

19. Examples of layer 7 protocols:

A. HTTP B. POP3 C. DSL D. All of the above

20. Unit of measurement at Layer 1.

A. bits B. frames C. packets D. segments

21. Unit of measurement at Layer 2.

A. bits B. frames C. packets D. segments

22. Unit of measurement at Layer 3.

A. bits B. frames C. packets D. segments

23. Unit of measurement at Layer 4.

A. bits B. frames C. packets D. segments

24. ___ model has 4 layers.

A. OSI Model B. TCP/IP Model C. MIME Model D. Presentation Model

Connectivity Options

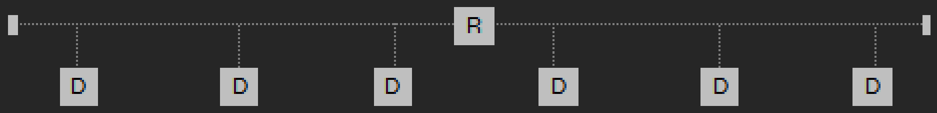
There are a variety of options to form a network, depending on cost, convenience & expertise. For example, you can use Wi-Fi or Bluetooth for transferring files (small to medium sized) between a smartphone and a laptop. You can use Wi-Fi or UTP cable between two laptops for transferring medium to large sized files (way faster) and so on.

Connectivity Type	Speed	Ease of Setup	Cost
Serial Port	Very Low	Medium	Very Low
Parallel Port	Very Low	Medium	Very Low
Infrared	Very Low	Medium	Very Low
Bluetooth	Low	Easy	Very Low
Crossover or Straight-through Cable	Very High	Easy	Low
Wi-Fi	High	Easy	Low
Powerline	High	Medium	Medium
Hub	Medium	Easy	Very Low
Network Switch	Very High	Depends	Depends
SOHO Router	Medium	Easy	Low
USB	Medium	Medium	Medium
IEEE 1394	Medium	Medium	Medium

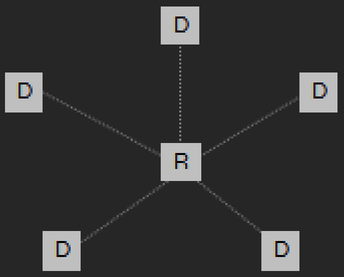
Connectivity Types, a rough guideline

Network Topology

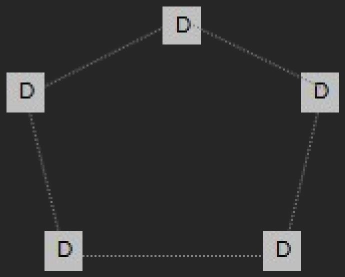
- Representation of devices in a network (theoretical/conceptual design of a network).
- Types
  - Bus
  - Ring
  - Star
  - Mesh



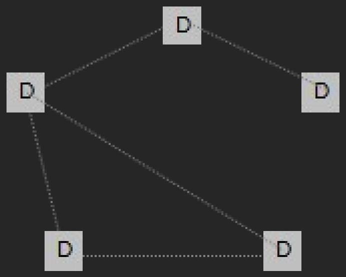
Bus Topology



Star Topology



Ring Topology



Mesh Topology

Bus Topology

- Computers (a.k.a. nodes) connected to a single backbone. All computers/devices tap into one coaxial cable using T-connectors and BNC connectors and Terminators are used at both ends, to prevent signal reflection and network interference. Repeaters (and hubs) are used to extend networks.
- High chance of collisions due to shared bandwidth.
- Single break anywhere causes entire network to be down.
- Types: 10BASE2 (Thinnet, RG-58 Coaxial, 185 Meters) & 10BASE5 (Thicknet, RG-8 Coaxial, 500 Meters)

Star Topology

- Computers connected to a centralized device, like a hub or network switch.
- Adding or removing devices is simple and does not disrupt the entire network.
- If one cable fail, only that particular computer is affected – not entire network.
- If the hub or network switch goes down, entire network gets affected.
- You can increase number of connections by cascading hub or switch (connecting one hub or switch to another).

Ring Topology

- Ring topology is a network configuration where each device is connected to exactly two other devices, forming a circular data path. Data flows around the loop in one direction (or both, in a dual ring) using a method called token passing.
- Similar to Star, but involves a closed loop (Physically Star, Logically Ring).

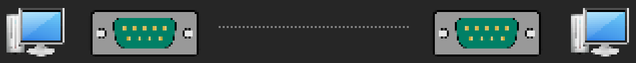
- Computers are connected through Token Ring Card & MSAU (Multistation Access Units)
- Devices are connected in a ring-like fashion. Each device receives data from one neighbor and forwards it to the next. A small data packet called a token circulates around the ring. Only the device that holds the token is allowed to transmit data. Prevents collisions and ensures organized communication.
- Token Passing Protocol - Developed by IBM, typically operated at 4 or 16 Mbps.

Mesh Topology

- Mesh topology is a network structure where each node can be connected to multiple other nodes, allowing data to travel through many possible paths. It is known for its robustness, fault tolerance, and dynamic routing.
- Connected non-hierarchically & Dynamically to achieve connectivity.
- Nodes take care of choosing route.
- The network can self-heal by rerouting traffic if a link or node fails.

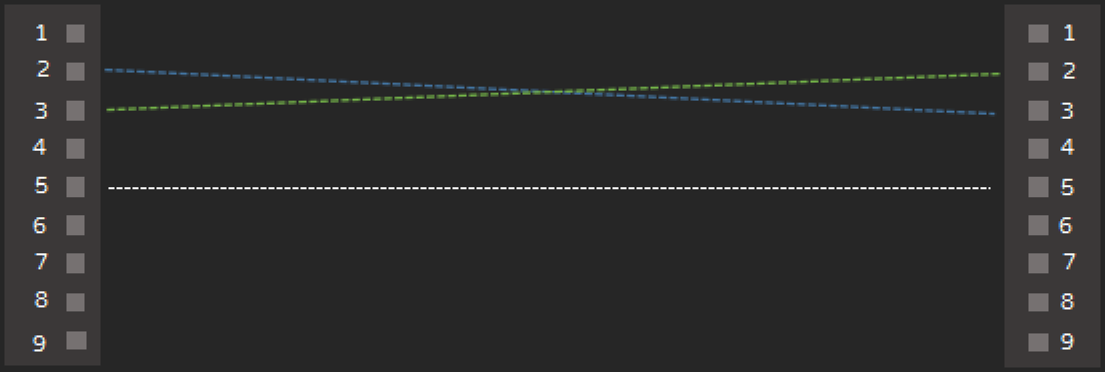
Real-world: Most networks use network switch these days, utilizing Twisted pair & Fiber optic cables.

Serial Port (Legacy)



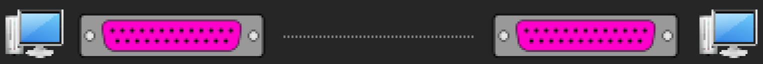
Serial Port Connectivity

- Found on very old computers.
- Transfer one bit a time, sequentially.
- Follows Recommended Standard 232 (a.k.a. RS-232).
- Used usually for connecting to Dial-Up Modems & Serial Printers.
- Typical Speeds - 9600, 19200, 38400, 57600 and 115200 bit/s.
- Replaced by USB & FireWire, Industrial & handful commercial usage exist.



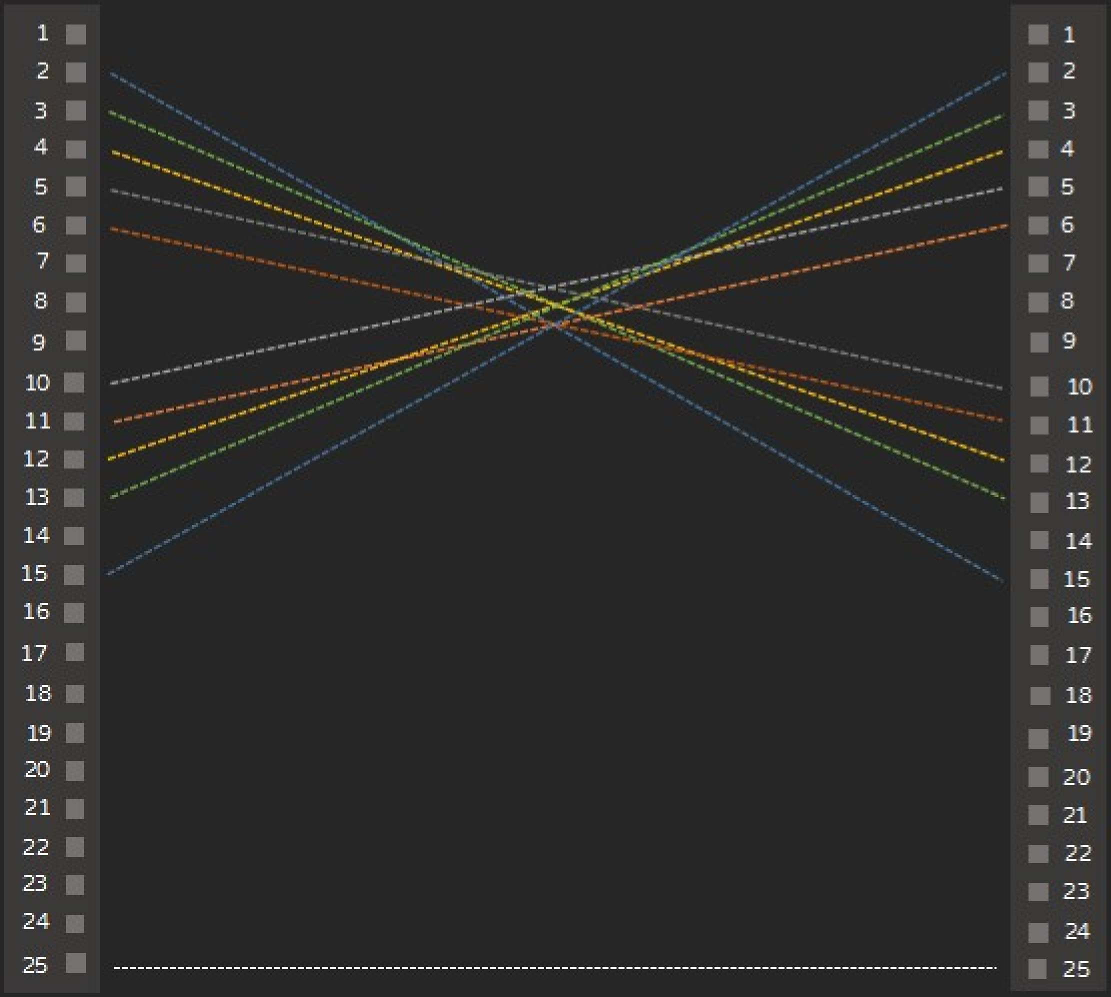
Serial Port Pin-Out

Parallel Port (Legacy)



Parallel Port Connectivity

- Found on very old computers.
- Transfer 8 bits at a time, in parallel.
- Follows IEEE 1284 Standard.
- Speed Range: 150 kbit/s - 2.5 MB/s.
- Popular for connecting Printers, Scanners, Zip Drives, etc.
- Replaced by USB & FireWire, Industrial & commercial usage exist.



Parallel Port Pin-Out

Infrared

Infrared Connectivity

- Low Speed Wireless.
- Follows IrDA (Infrared Data Association) standards.
- Common in older laptops, PDAs, printers, and mobile phones (pre-Bluetooth era).
- Works only in a direct line of sight & 10 feet approx.
- Obsolete — largely replaced by Bluetooth, NFC, and Wi-Fi.

Technology	Speed	
IrDA-Control	72 kbit/s	9 kB/s
IrDA-SIR	115.2 kbit/s	14 kB/s
IrDA-FIR	4 Mbit/s	500 kB/s
IrDA-VFIR	16 Mbit/s	2 MB/s
IrDA-UFIR	96 Mbit/s	12 MB/s
IrDA-Giga-IR	1024 Mbit/s	128 MB/s

Bluetooth

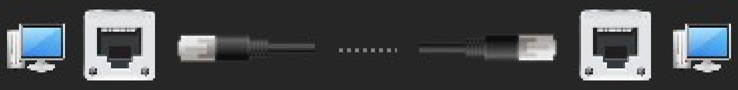
Bluetooth Connectivity

- Low to medium speed Wireless Technology.
- Simple “Pairing” mechanism to connect to each other.
- Standards managed by the Bluetooth Special Interest Group (SIG).
- Designed for shorter distances & low-bandwidth applications.
- Widely implemented in Mobile Phones, Laptops, etc.
- Suitable for transferring small to medium sized files.

Class	Range
1	100 Meters / 300 Feet
2	10 Meters / 33 Feet
3	1 Meter / 3.3 Feet

Technology	Speed	
Bluetooth 1.1	1 Mbit/s	125 kB/s
Bluetooth 2.0+EDR	3 Mbit/s	375 kB/s
Bluetooth 3.0	25 Mbit/s	3.125 MB/s
Bluetooth 4.0	25 Mbit/s	3.125 MB/s
Bluetooth 5.0	50 Mbit/s	6.25 MB/s

Twisted Pair Cable



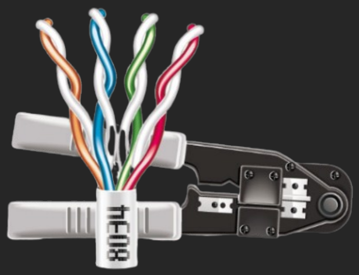
Connectivity using a patch cable, through Ethernet ports

- Used in telephone & computer networks.
- “Twisted” at predefined intervals to reduce EMI (Electro Magnetic Interference) & Crosstalk.
- Types
  - UTP: Normal 2 or 4 pair wires.
  - STP: UTP with a special extra foil shield layer to protect against EMI. Preferred in environments with higher interference.

Unshielded Twisted Pair

Shielded Twisted Pair

RJ-45 Connector



Crimping Tool

Cable Tester

- Registered Jack, RJ-45 is the de facto standard connector for Ethernet networks.
- RJ-11 is the de facto standard for telephone networks.
- Crimping Tool used for terminating cables into jacks (process referred to as “Crimping”).
- Cable Testers used for checking connectivity at both ends.

Cables are categorized according to standards:

Category	Bandwidth	Speed	Application
CAT 1	1 MHz	10	Used in telephone networks
CAT 2	4 MHz	4 Mbps	Used in Token Ring Networks
CAT 3	16 MHz	10 Mbps	Used in Ethernet Networks
CAT 4	20 MHz	16 Mbps	Used in Token Ring Networks
CAT 5	100 MHz	100 Mbps	Used in Ethernet Networks
CAT 5e	100 MHz	1000 Mbps	
CAT 6	Up to 250 MHz	1000 Mbps	

Standards

Name	Standard	Speed (Mbps)	Pairs	Max distance (m)	Cable
10BASE-T	802.3i	10	2	100	Cat 3
100BASE-TX	802.3u	100	2	100	Cat 5
1000BASE-T	802.3ab	1000	4	100	Cat 5e
1000BASE-TX	TIA/EIA-854	1000	4	100	Cat 6
2.5GBASE-T	802.3bz	2500	4	100	Cat 5e
5GBASE-T	802.3bz	5000	4	100	Cat 6
10GBASE-T	802.3an	10000	4	100	Cat 6A
25GBASE-T	802.3bq	25000	4	30	Cat 8
40GBASE-T	802.3bq	40000	4	30	Cat 8

For example, 1000BASE-T:

- 1000 indicates speed in Mbps.
- “BASE” indicates baseband.
- “T” - Twisted Pair.

Note:

- 10 Mbps is referred to as Ethernet.
- 100 Mbps is referred to as Fast Ethernet.
- 1000 Mbps is referred to as Gigabit Ethernet.

Ethernet

Ethernet refers to collection of technologies (following IEEE 802.3 standards) used in LAN. Ethernet uses co-axial, UTP & Fiber-optic links for connections.

Reference: https://en.wikipedia.org/wiki/Ethernet

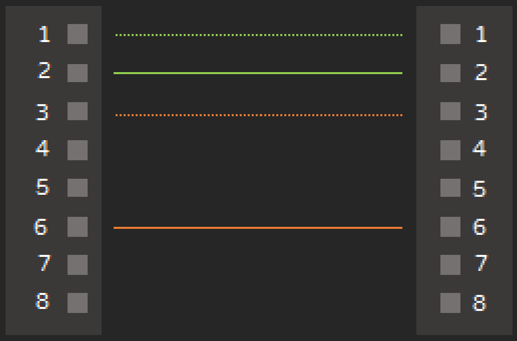
NIC, Hubs & Network Switches have MDI/MDIX, a type of interface for connecting twisted pair cables. Cables are wired either following straight-through (Medium Dependent Interface) or, cross-over (Medium Dependent Interface Cross-over) configuration (irrespective of cable standard T568A or T568B).

Pin #	T568A	T568B
1	White / Green Stripes	White / Orange Stripes
2	Solid Green	Solid Orange
3	White / Orange Stripes	White / Green Stripes
4	Solid Blue	Solid Blue
5	White / Blue Stripes	White / Blue Stripes
6	Solid Orange	Solid Green
7	White / Brown Stripes	White / Brown Stripes
8	Solid Brown	Solid Brown

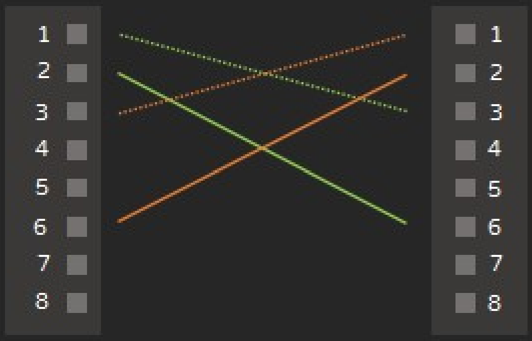
Cable Standard: Color coded for easy understanding.

In Straight-through cables, pin assignments match at both ends (i.e. Pin 1 wired to Pin 1, Pin 2 wired to Pin 2, etc.). Straight-Through cables are most common and used widely. In other words, transmitting & receiving pairs match at both ends. Straight-through cables are used for connecting dissimilar devices; for example, connecting a hub/network switch (MDI-X Interface) to a computer (MDI Interface).

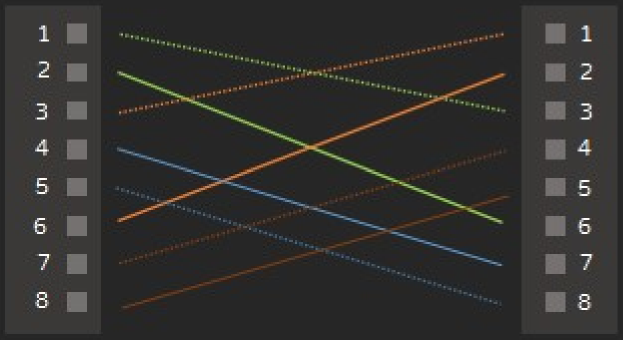
In Cross-over cables, pin assignments are swapped (transmitting & receiving pairs are swapped). Cross-over cables are used when connecting similar devices; for example, connecting one computer (MDI Interface) to another computer (MDI Interface).



2 Pair Straight Through (1-1, 2-2, 3-3, 6-6)



2 Pair Cross Over (1-3, 2-6, 3-1, 6-2)



4 Pair Cross Over Cable (1-3, 2-6, 3-1, 6-2, 5-8, 7-4, 4-7, 8-5)

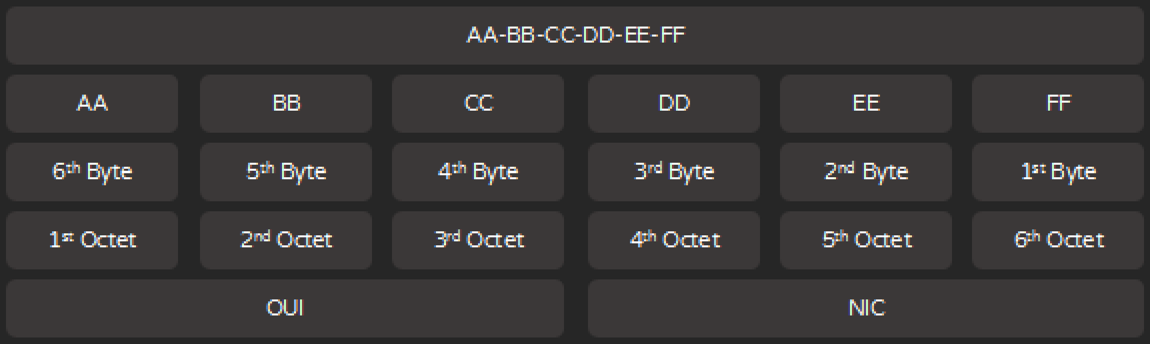
Network Interface Card (NIC)

Direct Connectivity using NIC

- Device that enables computers to connect to a network.
- Layer 1 & 2 (Physical & Data Link).
- Has hard-coded Unique MAC Address.

Media Access Control (MAC) Address

- Also known as “Physical Address”.
- Each NIC has one MAC address, usually not changeable.
- Used for addressing purposes (identifying a node) on a physical network.
- Uses 48-bit (2^{48}) addressing scheme as governed by IEEE.
- 281,474,976,710,656 Possible Physical Addresses.
- 24-bit part reserved for Organization (OUI) & 24-bit part for the hardware (NIC).
- Denoted in hexadecimal format, separated by hyphens (Example: AA-BB-CC-DD-EE-FF).

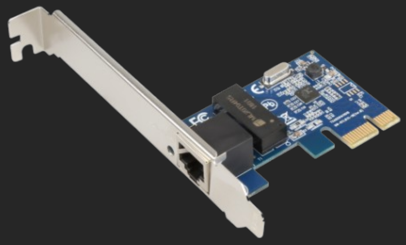


AA-BB-CC-DD-EE-FF					
AA	BB	CC	DD	EE	FF
6th Byte	5th Byte	4th Byte	3rd Byte	2nd Byte	1st Byte
1st Octet	2nd Octet	3rd Octet	4th Octet	5th Octet	6th Octet
OUI			NIC		

MAC Address Structure

Typical features of NIC:

- BOOT ROM: An additional special chip (usually integrated with the NIC) that allows a computer to boot from the network—loading an operating system from a remote computer.
- Power Management: Enables the NIC to conserve and manage power usage, typically controlled by the operating system.
- Auto-Negotiation: Automatically determines optimal NIC settings such as speed and duplex mode when connected to another computer or network device.
- Wake-On-LAN (WOL): Allows a computer to be powered on from a low-power state remotely over the network.
- Link Aggregation: Combines multiple NICs to increase network throughput. For example, combining two 100 Mbps NICs can provide up to 200 Mbps total bandwidth.
- Auto MDI/MDI-X: A modern feature that detects and automatically configures the appropriate cable type (straight-through or crossover), eliminating the need for manual selection.



Single Port NIC

Dual Port NIC

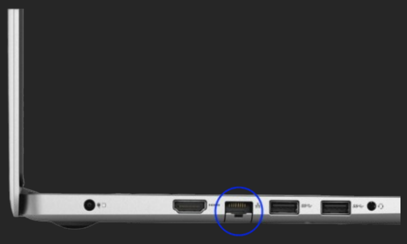
Quad Port NIC

USB to Ethernet Adapter

PCMCIA Ethernet Adapter

USB Type C to Ethernet Adapter

Motherboard with 4 NIC



Ethernet Port on Laptop

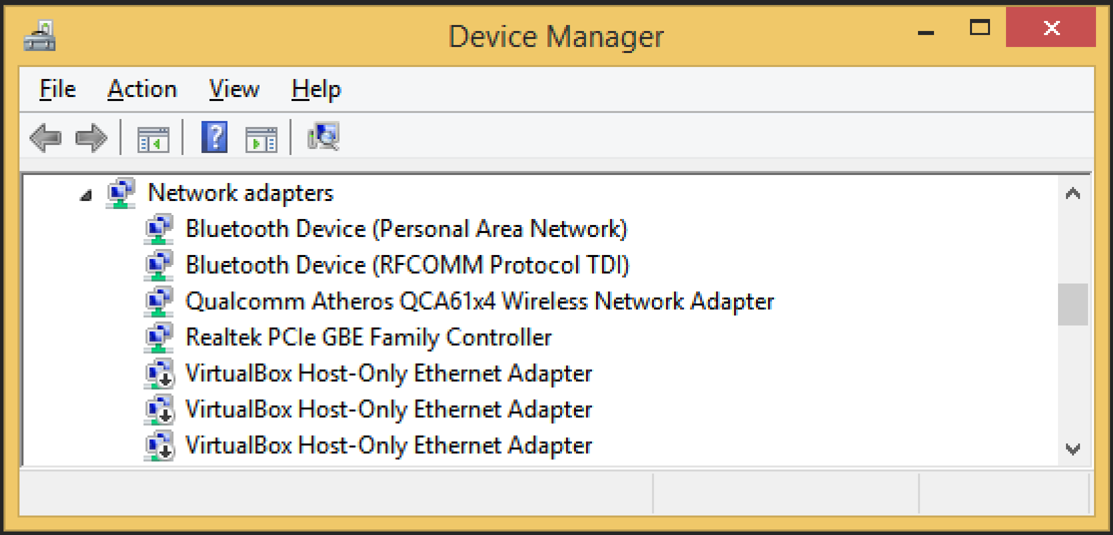
- NIC’s are integrated on most desktop computers & laptops. NIC settings are controlled through BIOS settings and/or Operating systems.
- For desktop computers: PCI, PCIe or USB types.
- For laptops: USB, Type C Ethernet Converter, CardBus or ExpressCard types.

Note: PCI interface is almost obsolete, replaced by PCIe on recent computers; it is recommended to check the technical specification of a computer before purchasing any type of NIC.

Wired Adapters Worksheet			
Vendor			
Model			
Interface			
PCI			
PCIe			
USB			
PCMCIA			
CardBus			
32 / 64 bit			
# of RJ-45 Ports			
# of Fiber Optic Ports			
Features			
WOL Support (Yes / No)			
Boot ROM (Yes / No)			
Power Management (Yes / No)			
Fail Over Support (Yes / No)			
Supported OS (Device Drivers)			
Microsoft Windows			
Linux			
MAC OS			
Standard Compliance			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
IEEE 802.3z			
IEEE 802.3ae			

Reference: https://en.wikipedia.org/wiki/IEEE_802.3

- View list of installed Network Adapters
  - START > RUN > DEVMGMT.MSC
  - Expand Network Adapters



Network adapters
- Bluetooth Device (Personal Area Network)
- Bluetooth Device (RFCOMM Protocol TDI)
- Qualcomm Atheros QCA61x4 Wireless Network Adapter
- Realtek PCIe GBE Family Controller
- VirtualBox Host-Only Ethernet Adapter
- VirtualBox Host-Only Ethernet Adapter
- VirtualBox Host-Only Ethernet Adapter

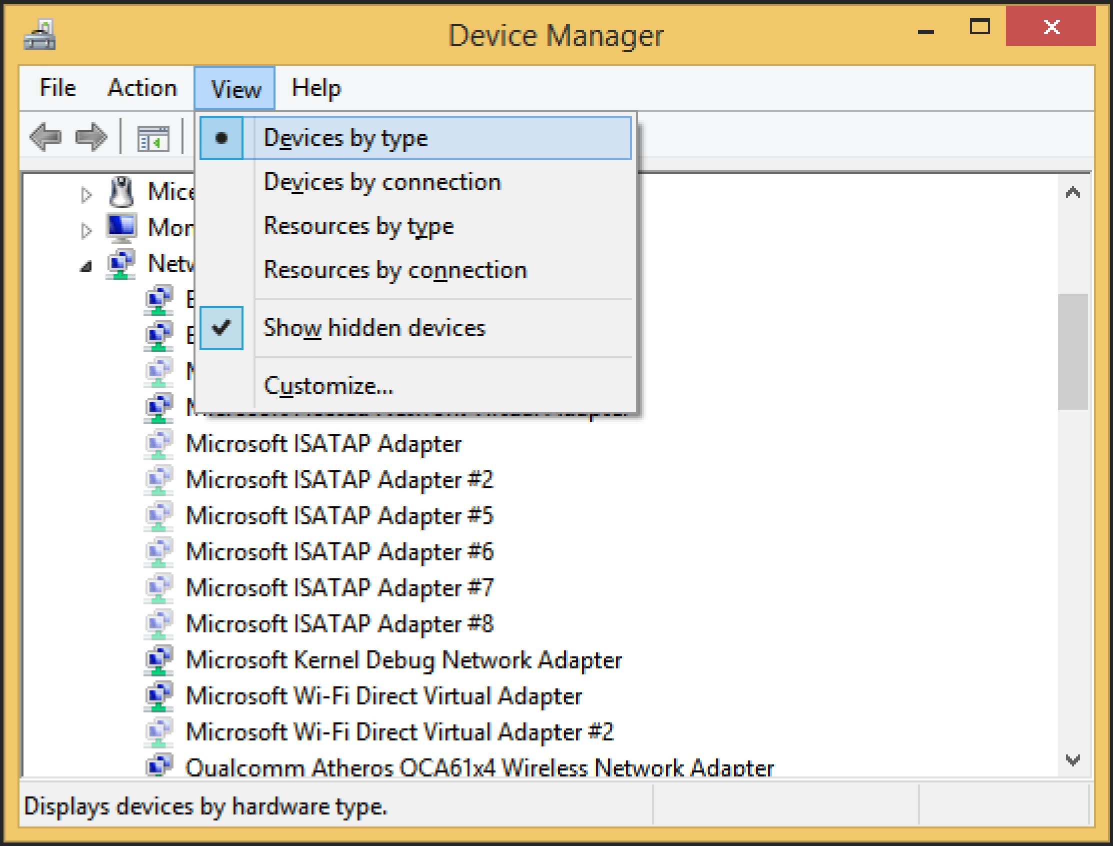
View all Network Adapters using Device manager

Example based on above image:

- Realtek PCIe GBE Family Controller - 1000 Mbps Wired NIC.
- Qualcomm Atheros QCA61x4 Wireless Network Adapter - Wireless NIC.

Note: You may find “Bluetooth Network Adapters", “Virtual adapters”, etc. installed for specific purposes by the operating system to support additional hardware or by a 3rd party software; such adapters may be researched further to understand their purpose. Do NOT compare “Virtual” with “Physical” adapters.

- View all Network Adapters (including Virtual, Hidden, etc.)
  - Select View > Show hidden devices



Mice
Mon
Netw
Microsoft ISATAP Adapter
Microsoft ISATAP Adapter #2
Microsoft ISATAP Adapter #5
Microsoft ISATAP Adapter #6
Microsoft ISATAP Adapter #7
Microsoft ISATAP Adapter #8
Microsoft Kernel Debug Network Adapter
Microsoft Wi-Fi Direct Virtual Adapter
Microsoft Wi-Fi Direct Virtual Adapter #2
Qualcomm Atheros QCA61x4 Wireless Network Adapter

Displays devices by hardware type.

Output listing all network adapters

For example:

- Microsoft 6to4 Adapter: Encapsulate IPV6 packets into IPv4 packet.
- Microsoft ISATAP Adapter: Inter Site Automatic Tunneling Address Protocol, used for IPV6.
- WAN Miniport (PPPOE): Used for establishing connectivity using PPPOE over Ethernet.

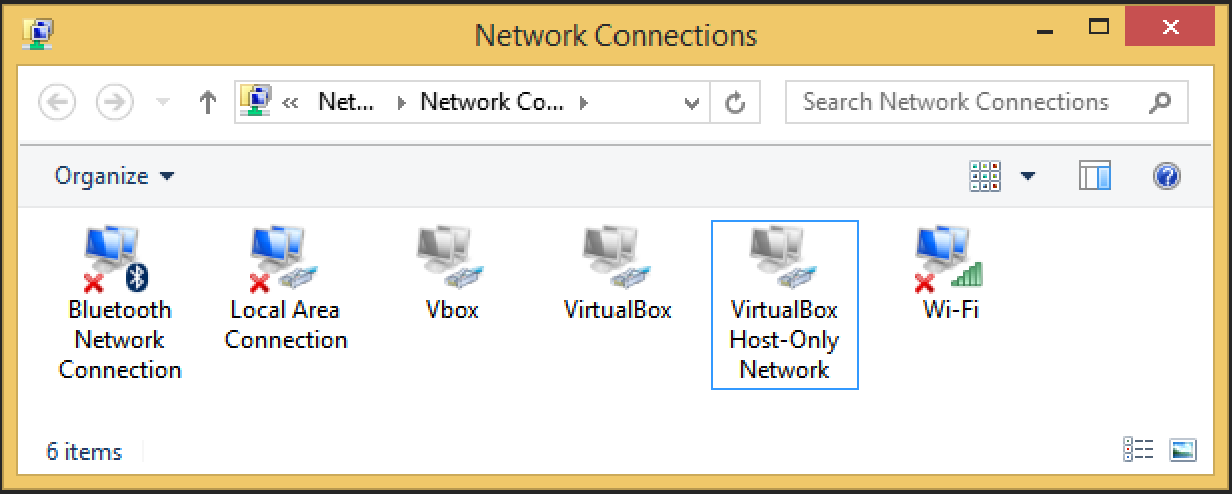
Note: Above topics may be explored once there is sufficient understanding of basic networking, hence not covered in-depth.

Network Connections (Microsoft Windows)

Network connections with names such as “Local Area Connection,” “Local Area Connection 2,” or “Bluetooth Network Connection” are automatically created by Microsoft Windows during installation. These names are intended for human reference. Whenever a new network adapter is installed, Windows automatically binds basic protocols and services to the connection, making the adapter usable without requiring much technical expertise.

Connection names are purely for identification and have no technical impact. For example, “Local Area Connection 2” can be renamed to “Ethernet” or “Wi-Fi” for easier identification.

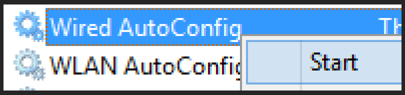
- View list of network connections
  - START > RUN > NCPA.CPL


Network Connections
« Net... › Network Co... ›
Search Network Connections
Organize ▾
Bluetooth Network Connection
Local Area Connection
Vbox
VirtualBox
VirtualBox Host-Only Network
Wi-Fi
6 items

List of Network Connections

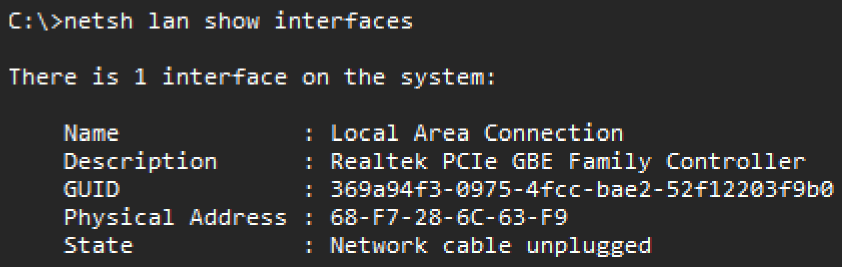
NETSH is a command line utility to manage network configuration.

- View list of Wired Adapters:
  - START > RUN > SERVICES.MSC
  - Select Wired AutoConfig , Right-click and Select “Start”



Note: Wired Autoconfig Service needs to be started for the following command to work.

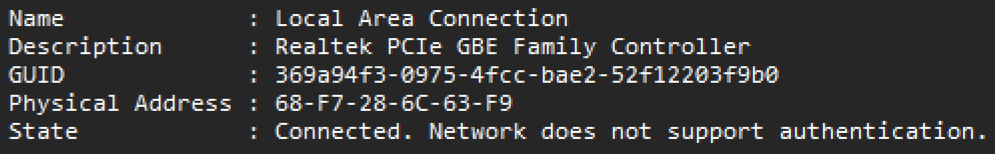
- CMD > netsh lan show interfaces



```
C:\>netsh lan show interfaces

There is 1 interface on the system:

    Name             : Local Area Connection
    Description      : Realtek PCIe GBE Family Controller
    GUID             : 369a94f3-0975-4fcc-bae2-52f12203f9b0
    Physical Address : 68-F7-28-6C-63-F9
    State            : Network cable unplugged
```

Output listing only Wired NIC (Disconnected) along with Connection Name, Model & MAC

- CMD > netsh lan show interfaces

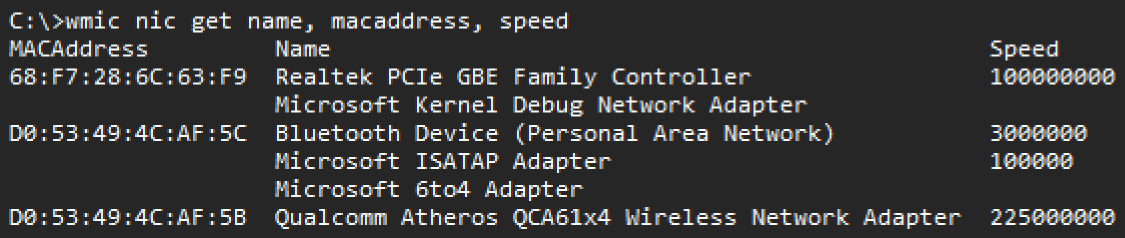


```
Name             : Local Area Connection
Description      : Realtek PCIe GBE Family Controller
GUID             : 369a94f3-0975-4fcc-bae2-52f12203f9b0
Physical Address : 68-F7-28-6C-63-F9
State            : Connected. Network does not support authentication.
```

Output listing only Wired NIC (If Connected)

WMIC (Windows Management Instrumentation Command-line) is a command line interface to WMI; WMI is used to manage several aspects of Microsoft Windows Operating systems through it’s interface and scripting languages.

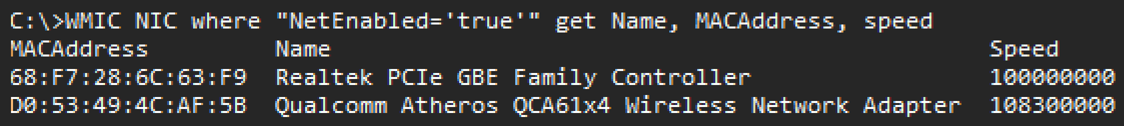
- View list of NIC using WMIC:
    - CMD > wmic nic get name, macaddress, speed



```
C:\>wmic nic get name, macaddress, speed
MACAddress         Name                                            Speed
68:F7:28:6C:63:F9  Realtek PCIe GBE Family Controller              100000000
                   Microsoft Kernel Debug Network Adapter
D0:53:49:4C:AF:5C  Bluetooth Device (Personal Area Network)        3000000
                   Microsoft ISATAP Adapter                        100000
                   Microsoft 6to4 Adapter
D0:53:49:4C:AF:5B  Qualcomm Atheros QCA61x4 Wireless Network Adapter  225000000
```

Output listing all adapters (including inactive connections, Virtual & hidden adapters)

- View Active (Connected) NIC:
    - CMD > wmic nic where "NetEnabled='true'" get Name, MACAddress, speed

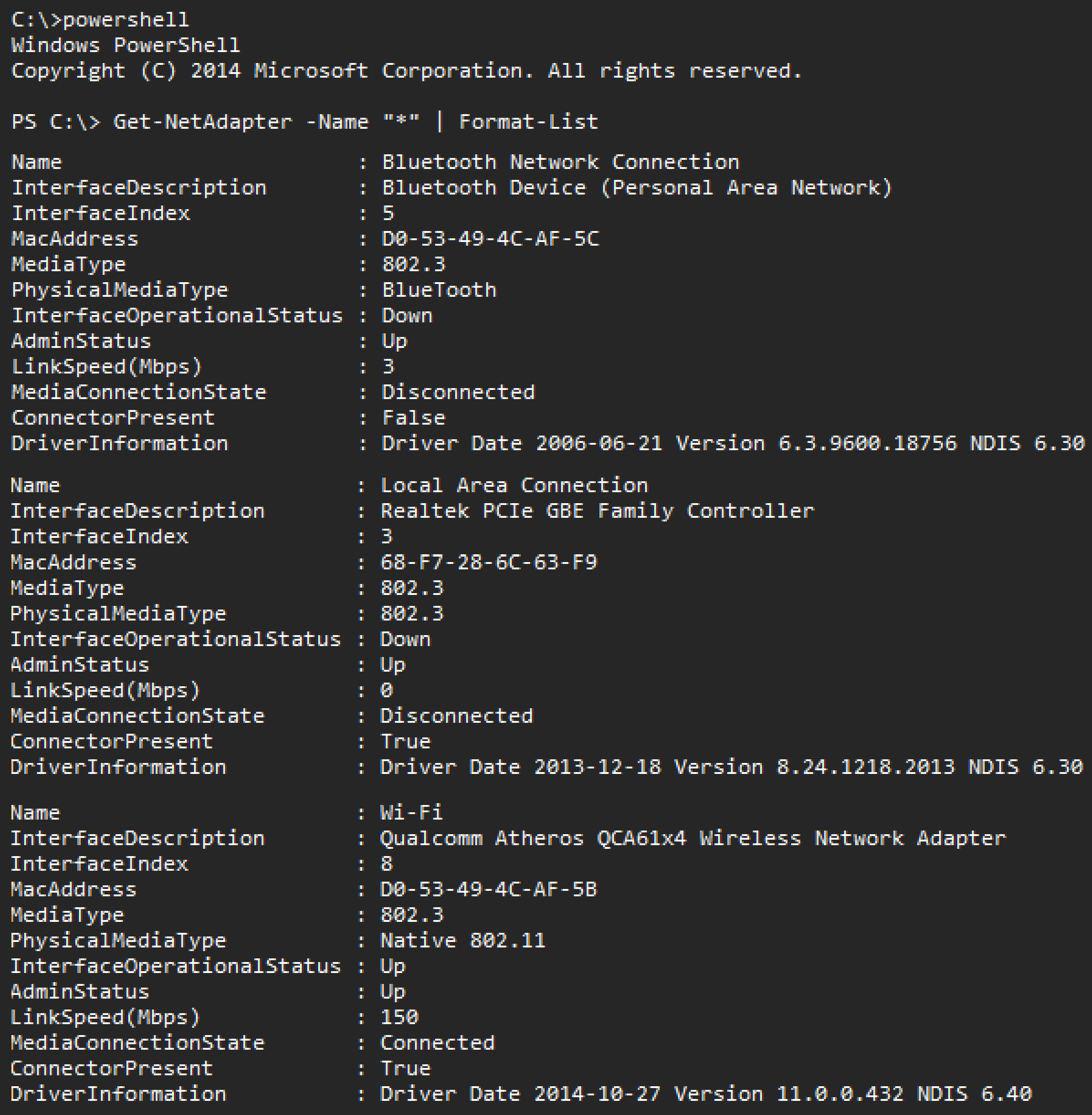


```
C:\>WMIC NIC where "NetEnabled='true'" get Name, MACAddress, speed
MACAddress         Name                                               Speed
68:F7:28:6C:63:F9  Realtek PCIe GBE Family Controller                 100000000
D0:53:49:4C:AF:5B  Qualcomm Atheros QCA61x4 Wireless Network Adapter  108300000
```

Output listing active adapters: Name, MAC & Speed

Powershell is a configuration management framework, which can be used for multiple purposes.

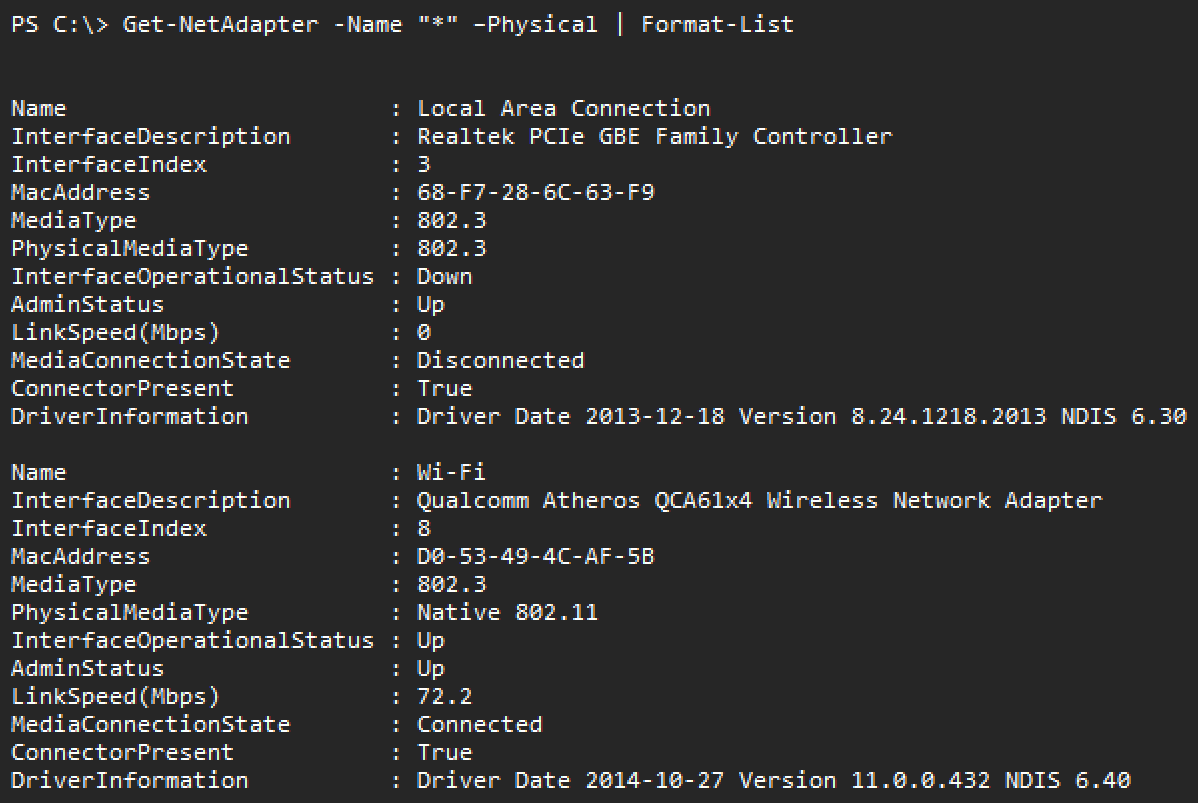
- CMD > Powershell > Get-NetAdapter -Name “*” | Format-List



```
C:\>powershell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\> Get-NetAdapter -Name "*" | Format-List

Name                        : Bluetooth Network Connection
InterfaceDescription        : Bluetooth Device (Personal Area Network)
InterfaceIndex              : 5
MacAddress                  : D0-53-49-4C-AF-5C
MediaType                   : 802.3
PhysicalMediaType           : BlueTooth
InterfaceOperationalStatus : Down
AdminStatus                 : Up
LinkSpeed(Mbps)             : 3
MediaConnectionState        : Disconnected
ConnectorPresent            : False
DriverInformation           : Driver Date 2006-06-21 Version 6.3.9600.18756 NDIS 6.30

Name                        : Local Area Connection
InterfaceDescription        : Realtek PCIe GBE Family Controller
InterfaceIndex              : 3
MacAddress                  : 68-F7-28-6C-63-F9
MediaType                   : 802.3
PhysicalMediaType           : 802.3
InterfaceOperationalStatus : Down
AdminStatus                 : Up
LinkSpeed(Mbps)             : 0
MediaConnectionState        : Disconnected
ConnectorPresent            : True
DriverInformation           : Driver Date 2013-12-18 Version 8.24.1218.2013 NDIS 6.30

Name                        : Wi-Fi
InterfaceDescription        : Qualcomm Atheros QCA61x4 Wireless Network Adapter
InterfaceIndex              : 8
MacAddress                  : D0-53-49-4C-AF-5B
MediaType                   : 802.3
PhysicalMediaType           : Native 802.11
InterfaceOperationalStatus : Up
AdminStatus                 : Up
LinkSpeed(Mbps)             : 150
MediaConnectionState        : Connected
ConnectorPresent            : True
DriverInformation           : Driver Date 2014-10-27 Version 11.0.0.432 NDIS 6.40
```

Output listing all adapters, list view

- View Physical Adapters:
  - CMD > Powershell > Get-NetAdapter -Name “*” –Physical | Format-List

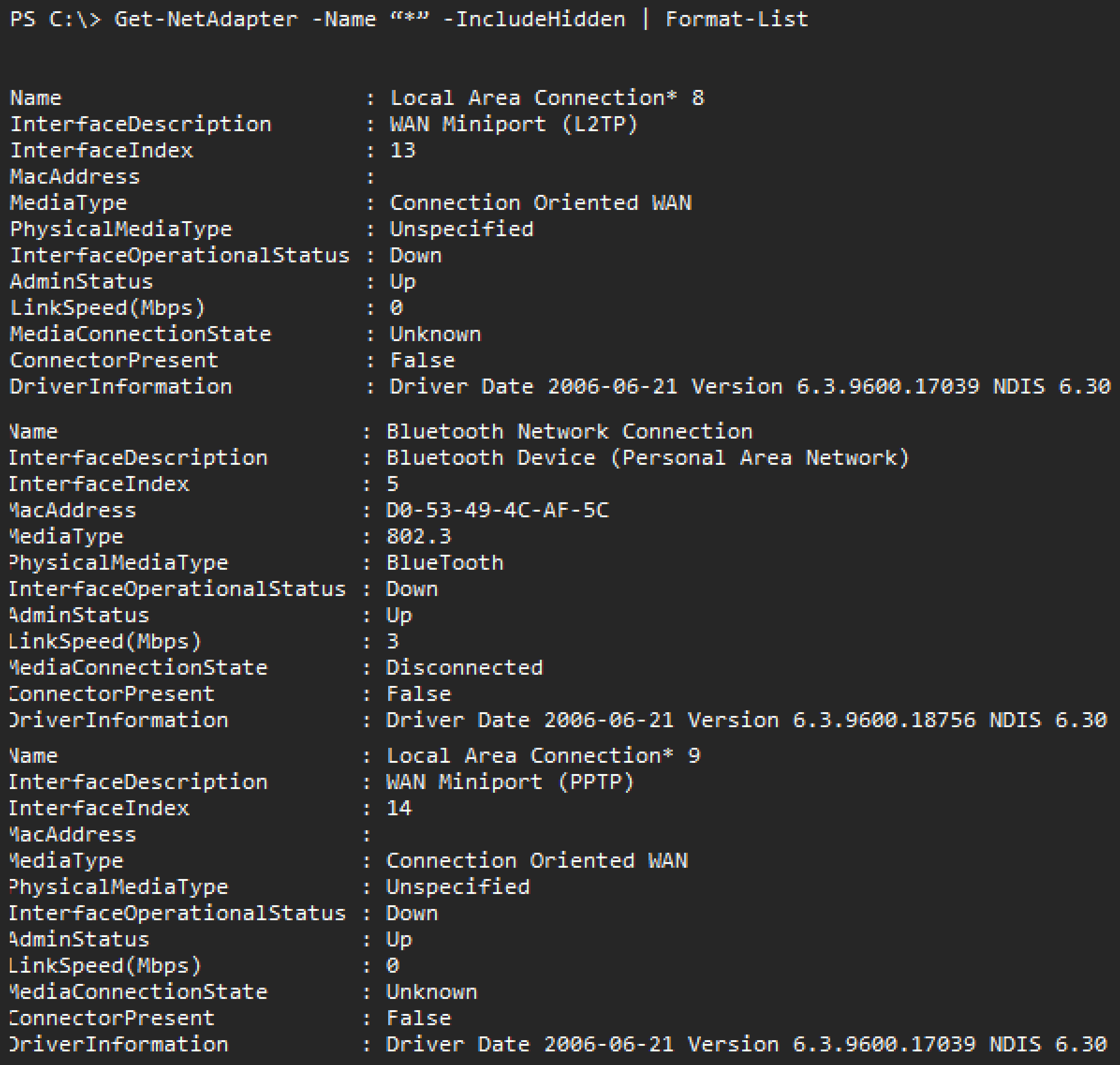


```
PS C:\> Get-NetAdapter -Name "*" -Physical | Format-List


Name                       : Local Area Connection
InterfaceDescription       : Realtek PCIe GBE Family Controller
InterfaceIndex             : 3
MacAddress                 : 68-F7-28-6C-63-F9
MediaType                  : 802.3
PhysicalMediaType          : 802.3
InterfaceOperationalStatus : Down
AdminStatus                : Up
LinkSpeed(Mbps)            : 0
MediaConnectionState       : Disconnected
ConnectorPresent           : True
DriverInformation          : Driver Date 2013-12-18 Version 8.24.1218.2013 NDIS 6.30

Name                       : Wi-Fi
InterfaceDescription       : Qualcomm Atheros QCA61x4 Wireless Network Adapter
InterfaceIndex             : 8
MacAddress                 : D0-53-49-4C-AF-5B
MediaType                  : 802.3
PhysicalMediaType          : Native 802.11
InterfaceOperationalStatus : Up
AdminStatus                : Up
LinkSpeed(Mbps)            : 72.2
MediaConnectionState       : Connected
ConnectorPresent           : True
DriverInformation          : Driver Date 2014-10-27 Version 11.0.0.432 NDIS 6.40
```

Output listing NIC, Supported IEEE Standards, Link Status, MAC Address & Speed if connected

Note: “| Format-List” option may be used for a list style view and is optional.

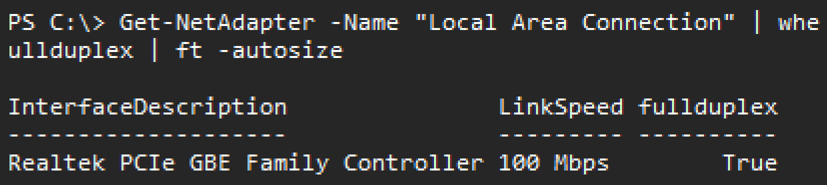
- View all Adapters (including hidden):
  - CMD > Powershell > Get-NetAdapter -Name “*” -IncludeHidden | Format-List



```
PS C:\> Get-NetAdapter -Name “*” -IncludeHidden | Format-List


Name                          : Local Area Connection* 8
InterfaceDescription          : WAN Miniport (L2TP)
InterfaceIndex                : 13
MacAddress                    :
MediaType                     : Connection Oriented WAN
PhysicalMediaType             : Unspecified
InterfaceOperationalStatus    : Down
AdminStatus                   : Up
LinkSpeed(Mbps)               : 0
MediaConnectionState          : Unknown
ConnectorPresent              : False
DriverInformation             : Driver Date 2006-06-21 Version 6.3.9600.17039 NDIS 6.30

Name                          : Bluetooth Network Connection
InterfaceDescription          : Bluetooth Device (Personal Area Network)
InterfaceIndex                : 5
MacAddress                    : D0-53-49-4C-AF-5C
MediaType                     : 802.3
PhysicalMediaType             : BlueTooth
InterfaceOperationalStatus    : Down
AdminStatus                   : Up
LinkSpeed(Mbps)               : 3
MediaConnectionState          : Disconnected
ConnectorPresent              : False
DriverInformation             : Driver Date 2006-06-21 Version 6.3.9600.18756 NDIS 6.30

Name                          : Local Area Connection* 9
InterfaceDescription          : WAN Miniport (PPTP)
InterfaceIndex                : 14
MacAddress                    :
MediaType                     : Connection Oriented WAN
PhysicalMediaType             : Unspecified
InterfaceOperationalStatus    : Down
AdminStatus                   : Up
LinkSpeed(Mbps)               : 0
MediaConnectionState          : Unknown
ConnectorPresent              : False
DriverInformation             : Driver Date 2006-06-21 Version 6.3.9600.17039 NDIS 6.30
```

Output listing all NIC, Link Status, MAC Address & Speed

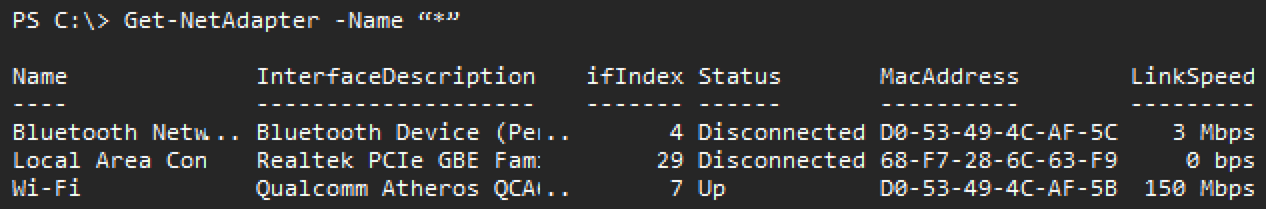
- View details for a specific adapter using Powershell:
  - CMD > Powershell
  - Powershell > Get-NetAdapter -Name “CONNECTIONNAME” | where Status -eq "Up" | select InterfaceDescription, LinkSpeed, fullduplex | ft -autosize



```
PS C:\> Get-NetAdapter -Name "Local Area Connection" | whe
ullduplex | ft -autosize

InterfaceDescription               LinkSpeed fullduplex
--------------------               --------- ----------
Realtek PCIe GBE Family Controller 100 Mbps        True
```

Output listing Name, current speed & select duplex mode for a specific wired connection

- View All adapters using Powershell:
  - CMD > Powershell > Get-NetAdapter -Name “*”

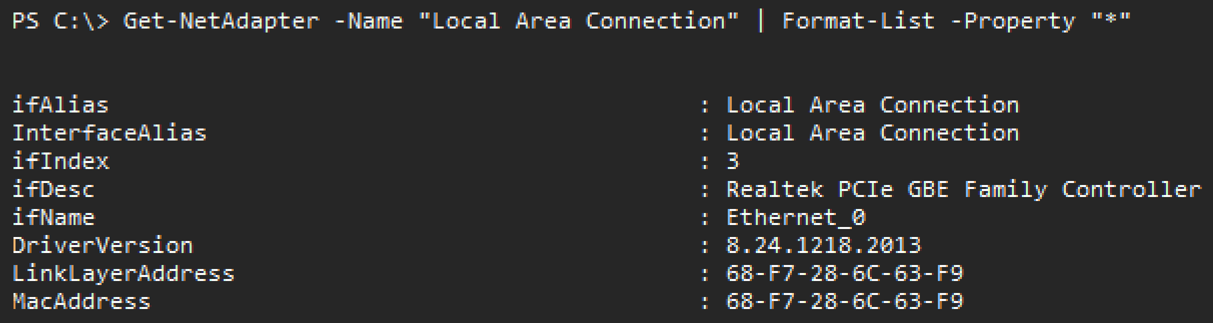


```
PS C:\> Get-NetAdapter -Name “*”

Name                 InterfaceDescription    ifIndex Status       MacAddress         LinkSpeed
----                 --------------------    ------- ------       ----------         ---------
Bluetooth Netw..     Bluetooth Device (Pe..        4 Disconnected D0-53-49-4C-AF-5C     3 Mbps
Local Area Con       Realtek PCIe GBE Fam:        29 Disconnected 68-F7-28-6C-63-F9      0 bps
Wi-Fi                Qualcomm Atheros QCA..        7 Up           D0-53-49-4C-AF-5B   150 Mbps
```

Output listing all adapters (Disconnected & Disabled if any), Link Status, MAC Address & Speed

Note: ifIndex refers to Interface Index, an internal reference ID maintained by the Operating System.

- View details of a particular NIC using Powershell:
  - CMD >
    - Powershell > Get-NetAdapter -Name "CONNECTIONNAME" | Format-List -Property "*"

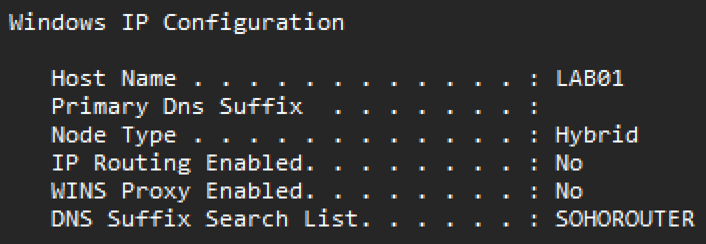


```
PS C:\> Get-NetAdapter -Name "Local Area Connection" | Format-List -Property "*"


ifAlias                                          : Local Area Connection
InterfaceAlias                                   : Local Area Connection
ifIndex                                          : 3
ifDesc                                           : Realtek PCIe GBE Family Controller
ifName                                           : Ethernet_0
DriverVersion                                    : 8.24.1218.2013
LinkLayerAddress                                 : 68-F7-28-6C-63-F9
MacAddress                                       : 68-F7-28-6C-63-F9
```

Output listing details of an NIC

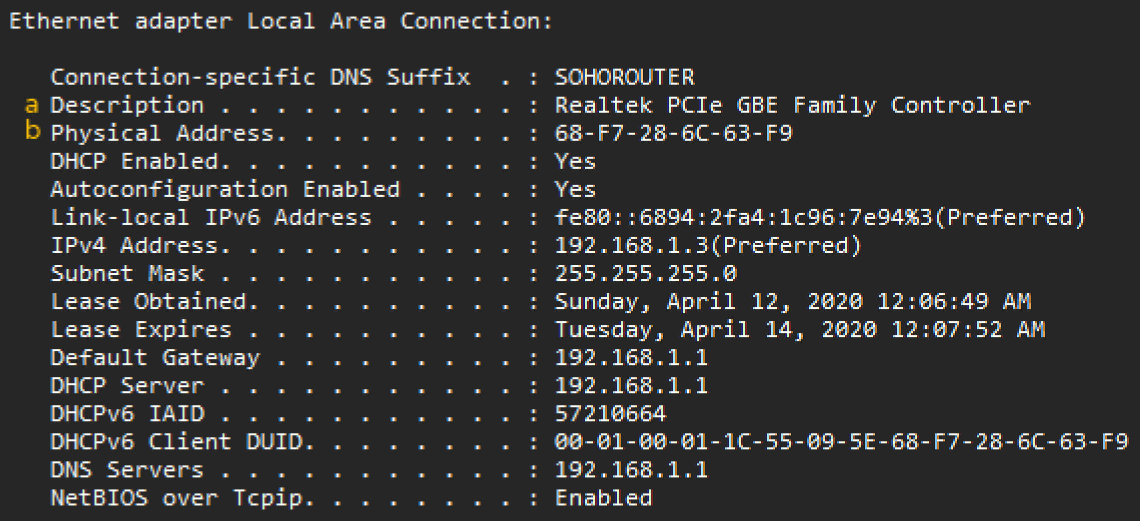
IPCONFIG (Internet Protocol Configuration) is a command line utility to manage IP configuration, that can also be used for viewing list of network cards.

- View list of network adapters on a computer:
  - CMD > ipconfig /all



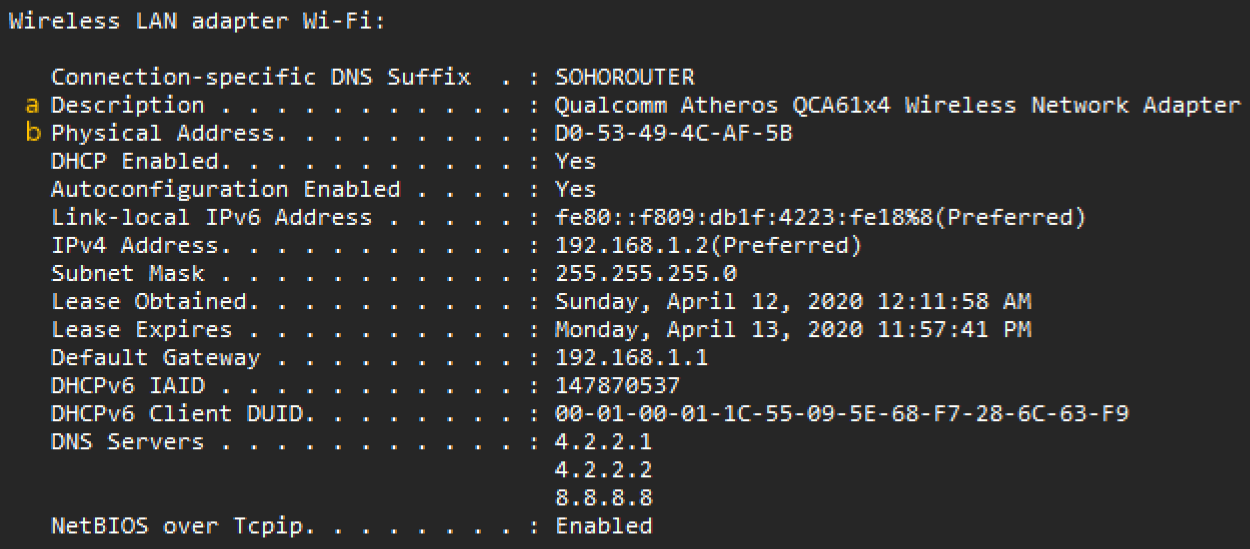
```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAB01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : SOHOROUTER
```

Output listing Host Name (Computer Name)



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
 a Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
 b Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 12:06:49 AM
   Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 12:07:52 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Wired Adapter: a) Manufacturer, Model & Adapter type & b) MAC Address in hexadecimal format



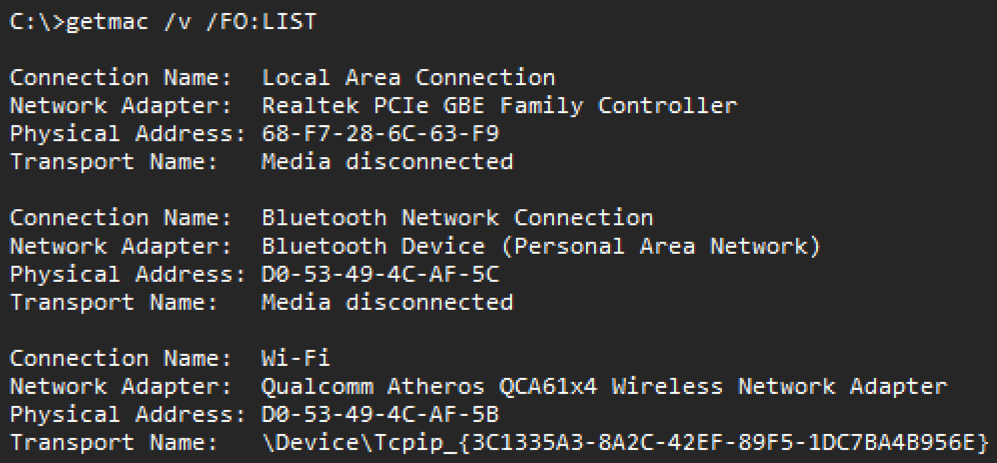
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : SOHOROUTER
 a Description . . . . . . . . . . . : Qualcomm Atheros QCA61x4 Wireless Network Adapter
 b Physical Address. . . . . . . . . : D0-53-49-4C-AF-5B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f809:db1f:4223:fe18%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 12:11:58 AM
   Lease Expires . . . . . . . . . . : Monday, April 13, 2020 11:57:41 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 147870537
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 4.2.2.1
                                       4.2.2.2
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Wireless Adapter: a) Manufacturer, Model & Adapter type & b) MAC Address

Tip: Use "ipconfig /all | more" to view line by line.

GETMAC is a command line utility to view MAC addresses.

- View Connection Name & MAC Address:
  - CMD > getmac /v /FO:LIST

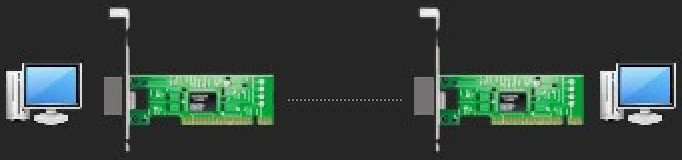


```
C:\>getmac /v /FO:LIST

Connection Name:  Local Area Connection
Network Adapter:  Realtek PCIe GBE Family Controller
Physical Address: 68-F7-28-6C-63-F9
Transport Name:   Media disconnected

Connection Name:  Bluetooth Network Connection
Network Adapter:  Bluetooth Device (Personal Area Network)
Physical Address: D0-53-49-4C-AF-5C
Transport Name:   Media disconnected

Connection Name:  Wi-Fi
Network Adapter:  Qualcomm Atheros QCA61x4 Wireless Network Adapter
Physical Address: D0-53-49-4C-AF-5B
Transport Name:   \Device\Tcpip_{3C1335A3-8A2C-42EF-89F5-1DC7BA4B956E}
```

Output listing Connection Name, Network Adapter & MAC Address

- MAC Address Vendor Search
  - Get MAC address of a computer using IPCONFIG or other command
  - Search MAC address via sites like https://www.macvendorlookup.com

Fiber Optic Card & Cable



Connectivity using Fiber Optic NIC & Fiber Cable

- Uses optical technology for communication instead of electric signals.
- No EMI, Near-end Crosstalk (NEXT), or Far-end Crosstalk (FEXT).
- Suitable for long distances and/or places that has heavy EMI.
- Optic cables are made of high-quality glass or fiber, covered by durable plastic or PVC.
- Require high precision for termination at both ends.
- Optical Network cards & optical cables are expensive compared to normal NIC / twisted pair cables.
- Optical Fiber Types:
  - Single-Mode Fiber (SMF) for long distances.
  - Multi-Mode Fiber (MMF) for shorter distances.

Single Mode Fiber Optic Cable

Multi Mode Fiber Optic Cable

Fiber Optic Connector

Fiber Optic Network Card

Fiber Optic Cable Tester

Fiber Cable with Connectors

Standards

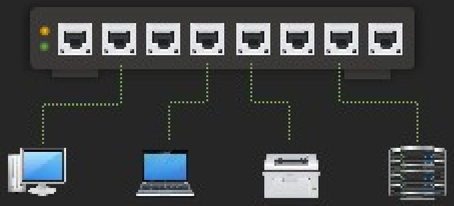
Transmission Standards	100 Mb Ethernet	1000 Mb Ethernet	10 Gb Ethernet	40 Gb Ethernet	100 Gb Ethernet
OM1 (62.5/125)	2000 meters (FX)	275 meters (SX)	33 meters (SR)	Not supported	Not supported
OM2 (50/125)	2000 meters (FX)	550 meters (SX)	82 meters (SR)	Not supported	Not supported
OM3 (50/125)	2000 meters (FX)	550 meters (SX)	300 meters (SR)	100 meters	100 meters
OM4 (50/125)	2000 meters (FX)	1000 meters (SX)	550 meters (SR)	150 meters	150 meters

Standard	Specification	Speed	Media
10BASEFL	IEEE 802.3	10 Mbps	Fiber Optic
100BASE-FX	IEEE 802.3u	100 Mbps	Fiber Optic
1000BASESX	IEEE 802.3z	1 Gbps	Fiber Optic
1000BASELX	IEEE 802.3z	1 Gbps	Fiber Optic
10GBASE-SR	IEEE 802.3ae	10 Gbps	Fiber Optic
10GBASE-SW	IEEE 802.3ae	10 Gbps	Fiber Optic
10GBASE-LX4	IEEE 802.3ae	10 Gbps	Fiber Optic
10GBASE-LR	IEEE 802.3ae	10 Gbps	Fiber Optic
10GBASE-LW	IEEE 802.3ae	10 Gbps	Fiber Optic
10GBASE-ER	IEEE 802.3ae	10 Gbps	Fiber Optic

Terms

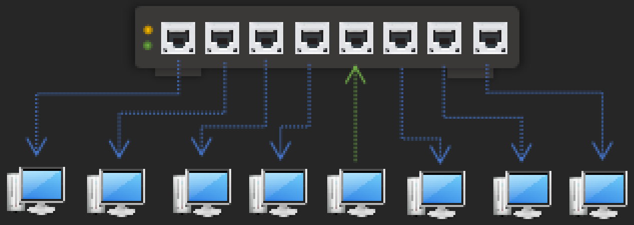
- EMI (Electromagnetic Interference) disrupts signals and may cause errors or complete communication to fail. Impacts quality & reliability of signals.
- NEXT is a type of cross-talk that happens near the source (sender) and FEXT at the end of the source (receiver).

Hub (legacy)



An 8 Port Hub, can connect up to 8 devices

- Operates at Layer 1 (Physical).
- Is a simple Multi-port repeater, broadcasts to all ports.
- Usually available as 4, 5 or 8 port options.
- Limited to half-duplex communication.
- Networks extended by using repeaters, following 5-4-3 rule.
- Transfer speeds 10 to 100 Mbps.
- Not suitable for large number of computers.
- Replaced by Network Switch.



Layer 1: A hub forwards to all other ports, hence not suitable beyond small networks

5-4-3 Rule

An Ethernet segment can be extended using 4 repeaters (which means maximum of 5 segments) and 3 of 5 segments can have devices. This rule applies only to networks that use repeaters (historical days when 10 Mbps / hubs were used).

Repeater

- Operates at Layer 1.
- Used for extending networks.
- Works by amplifying and re-transmitting signals.

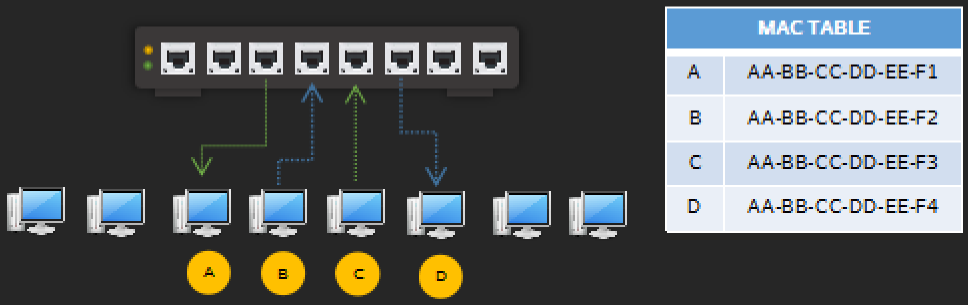
Network Bridge

- Operates at Layer 2.
- Uses MAC table for forwarding frames.

Switch (a.k.a Network Switch)

A 24 Port Network Switch, with Uplink/Downlink Ports

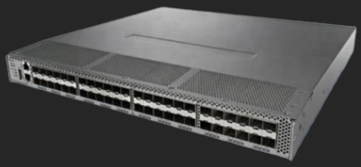
- Is a Multi-port Bridge.
- Operates at Layer 2 (Data Link).
- Suitable for small, medium and/or large networks.
- Builds MAC table based on devices connected to it, analyzes frames and forwards to matching MAC address thereby minimizing collisions.
- Uses Store and forward, cut through, Fragment free or Adaptive switching methods.
- Full-duplex communication.
- Usually has 4, 8, 16, 24, 32 or 48 ports, designed to support transfer speeds 10 to 10000 Mbps.
- Networks are extended by cascading multiple network switches and/or by using Uplink/Downlink Ports if available (depending on the model).
- ARP (Address Resolution Protocol), used for resolving IP to MAC Address.
- Types
  - Unmanaged Switch: Designed to work automatically requiring no technical expertise; suitable for most home & small office networks. Users simply connect computers to Network Switch.
  - Managed Switch: Requires specific technical expertise based on vendor / model. Requires product specific knowledge before it can be used (depends on model).



MAC TABLE	
A	AA-BB-CC-DD-EE-F1
B	AA-BB-CC-DD-EE-F2
C	AA-BB-CC-DD-EE-F3
D	AA-BB-CC-DD-EE-F4

Layer 2: A switch analyzes and forwards data packet to the matching MAC address

Unmanaged Switch

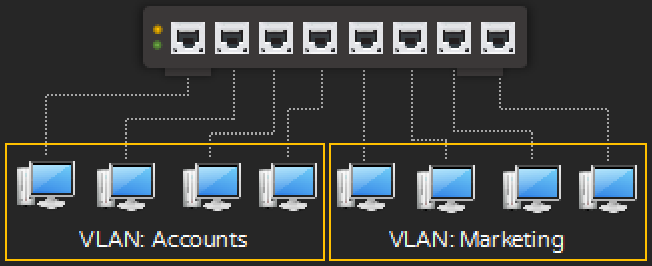


Managed Switch

Fiber Optic Switch

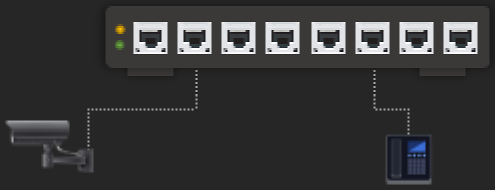
Typical features:

- Has serial port, USB and/or web based facilities for administration.
- Access Control is a security feature that allows only authorized devices to connect—commonly implemented by whitelisting MAC addresses to permit only specific computers.
- Facility to remotely monitor & manage, using the Simple Network Management Protocol.
- Modify duplex, speed & other network parameters.
- VLAN (Virtual LAN) is a feature used Used to partition Layer 2 networks for improved security and reduced collisions. VLANs can isolate different departments or groups—even if all computers are connected to the same physical switch or multiple interconnected switches.



Departments isolated through virtual networks, though connected to same switch

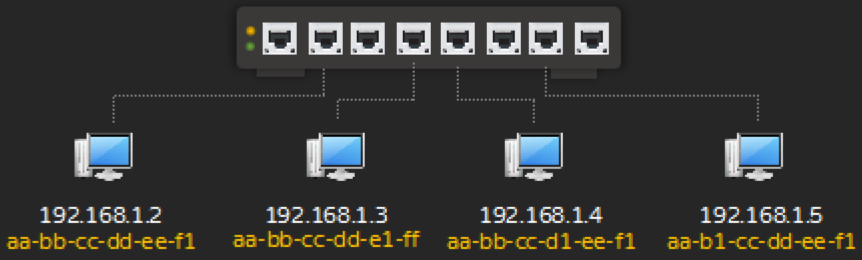
- PoE (Power over Ethernet) is a feature that delivers electrical power through network cables (UTP) to end devices such as network cameras, IP phones, and wireless access points. This eliminates the need for separate power adapters for each device. PoE typically provides around 57 volts and up to 100 watts of power, depending on the device and the PoE standard used.



Network Switch with PoE facility providing data & power to a CCTV Camera & a VoIP Phone

Network Switch Worksheet			
Vendor			
Model			
Desktop / Rack Mount			
Managed / Unmanaged			
No. of Ports (UTP/STP)			
No. of Ports (Optical)			
No. of Ports (PoE)			
Console Port (Yes / No)			
Web Interface (Yes / No)			
VLAN (Yes / No)			
Standard Compliance			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
IEEE 802.3z			
IEEE 802.1q			
IEEE 802.1p			
IEEE 802.3ad			
IEEE 802.3az			
IEEE 802.3w			
IEEE 802.1x			

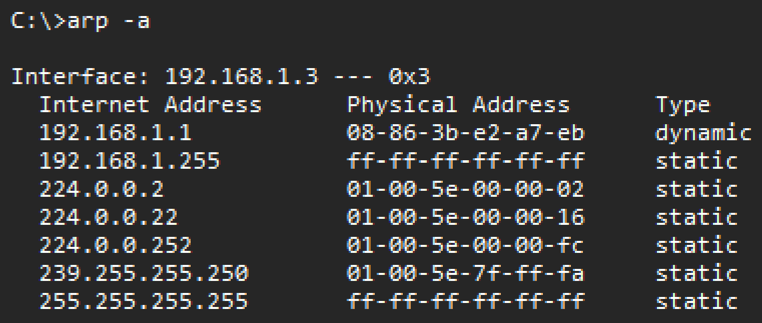
IP addresses are resolved to MAC addresses, for computers to communicate within a network. Resolved MAC addresses are stored in respective computer's ARP cache and used for future communication.



Computers connected to a network switch

ARP is a command line utility to view and manage ARP cache.

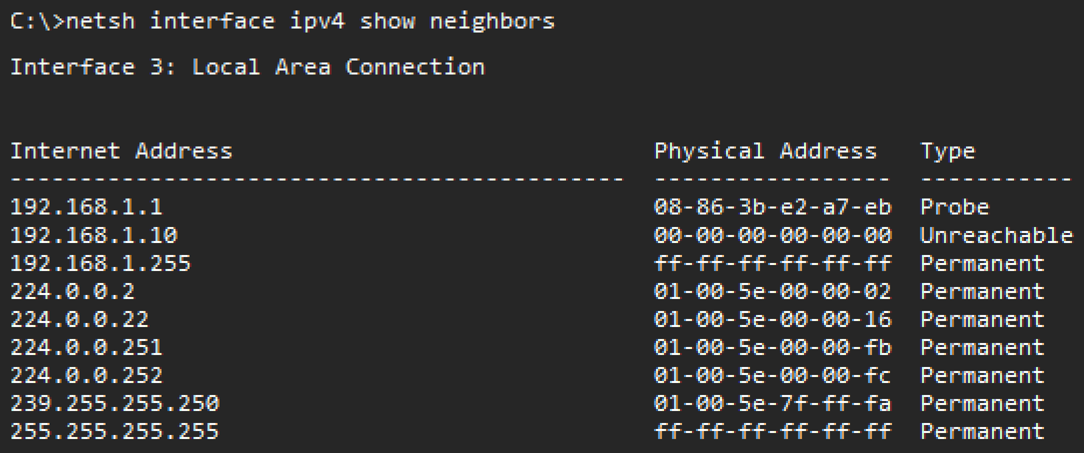
- View ARP Cache (Resolved MAC Addresses):
  - CMD > arp -a



```
C:\>arp -a

Interface: 192.168.1.3 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           08-86-3b-e2-a7-eb     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Output listing ARP cache, listing IP to MAC Address mapping

- View ARP Cache:
  - CMD > netsh interface ipv4 show neighbors



```
C:\>netsh interface ipv4 show neighbors

Interface 3: Local Area Connection


Internet Address                              Physical Address   Type
--------------------------------------------  -----------------  -----------
192.168.1.1                                   08-86-3b-e2-a7-eb  Probe
192.168.1.10                                  00-00-00-00-00-00  Unreachable
192.168.1.255                                 ff-ff-ff-ff-ff-ff  Permanent
224.0.0.2                                     01-00-5e-00-00-02  Permanent
224.0.0.22                                    01-00-5e-00-00-16  Permanent
224.0.0.251                                   01-00-5e-00-00-fb  Permanent
224.0.0.252                                   01-00-5e-00-00-fc  Permanent
239.255.255.250                               01-00-5e-7f-ff-fa  Permanent
255.255.255.255                               ff-ff-ff-ff-ff-ff  Permanent
```

Output listing ARP Cache

Note: If the destination host is present on a remote network, MAC address of the gateway will be listed.

- Clear ARP Cache:
  - CMD > netsh -d

Quiz 03

1. IEEE standard related to Ethernet _________________.

A. IEEE 802.11 B. IEEE 803.21 C. IEEE 802.3 D. IEEE 802.6

2. IEEE standard related to Bluetooth:

A. IEEE 802.3 B. IEEE 802.12 C. IEEE 802.14 D. IEEE 802.15

3. Which network topology allows computers to be connected to a centralized device?

A. Bus B. Star C. AD-HOC D. Mesh

4. Components used in Bus topology:

A. T-Connector B. BNC Connector C. Co-Axial Cable D. All of the above

5. Components used in Star topology:

A. RJ-45 B. Twisted-pair cable C. Switch D. All of the above

6. _____ is used for amplifying and re-transmitting weak signals.

A. Access Point B. Bridge C. Repeater D. All of the above

7. Advantage of a network switch over a hub:

A. Filters Frames B. Operates at Layer 2 C. Reduces Collision D. All of the above

8. In 10base2 '10' refers to:

A. 10 Meters B. 10 Mbps C. 10 Mbps D. Both B & C

9. In 10base2 'base' refers to:

A. Broadband B. Baseband C. Narrowband D. Wideband

10. In 10base2 '2' refers to:

A. 200 Meters B. 200 Mbps C. 2 Mbps D. 200 Feet

11. 10Base2 is also known as:

A. Broadband B. Thinnet C. Thicknet D. Baseband

12. 10Base5 is also known as:

A. Broadband B. Thinnet C. Thicknet D. Baseband

13. Acronym - UTP.

A. Ultimate Twisted Pair B. Unwinded Twisted Pair
C. Unshielded Twisted Pair D. Unlimited Twisted Pair

14. Speed of Ethernet:

A. 10 Mbps B. 100 Mbps C. 1000 Mbps D. 10000 Mbps

15. Speed of Fast Ethernet:

A. 10 Mbps B. 100 Mbps C. 1000 Mbps D. 10000 Mbps

16. In 100baseT 'T' refers to:

A. Twisted-Pair B. Telecommunication C. Thin-Pair D. Tele-Pair

17. Category of UTP that support speeds greater than 100 Mbps:

A. Cat 1 B. Cat 2 C. Cat 3 D. Cat 5

18. Category of UTP that support speeds greater than 1000 Mbps:

A. Cat 3 B. Cat 5e C. Cat 6 D. Both B & C

19. Category of UTP used in Telephone lines:

A. Cat 1 B. Cat 2 C. Cat 3 D. Cat T

20. Maximum distance supported by UTP _____.

A. 100 Feet B. 1000 Feet C. 100 Meters D. 10 Meters

21. IEEE 802.3 Specification corresponds to _____ standard.

A. 10BASE2 B. 100BASE-TX C. 1000BASE-T D. 1000BASESX

22. Type of cable that uses light as the media for transmitting signals:

A. Co-Axial B. UTP C. STP D. Fiber-optic

23. Type of cable that is not susceptible to EMI:

A. Co-Axial B. UTP C. STP D. Fiber-optic

24. Type of material used for protecting cables against fire:

A. PVC B. Plenum C. STP D. UTP

25. Type of cable preferred for connecting dissimilar devices:

A. Single-mode fiber B. Straight through C. Cross over D. PVC Coated

26. Type of cable preferred for connecting similar devices:

A. Single-mode fiber B. Straight through C. Cross over D. PVC Coated

27. Type of NIC for use in desktop computers.

A. PCI B. PCIe C. USB D. All of the above

28. Type of NIC for use in laptop computers.

A. PCI B. CardBus C. ExpressCard D. ISA

29. _____ is a unique hardware address assigned to an NIC.

A. MAC B. IP C. IPX D. TCP

30. MAC addresses are _____ addresses.

A. 16-bit B. 32-bit C. 48-bit D. 64-bit

31. Example of a valid MAC address:

A. 00-B0-D0-1D-F5-5B
B. 192.168.2.5
C. 00-B0-D000-B0-D000-B0-D000-B0-D0
D. server05

32. Connectors for Ethernet card _____.

A. RJ-11 B. RJ-58 C. RJ-45 D. RJ-E

33. Connectors for telephones _____.

A. RJ-11 B. RJ-58 C. RJ-45 D. RJ-E

34. _____ is a special chip that allows loading of an operating system over a network.

A. WOL B. Boot ROM C. MAC ROM D. RIS

35. Procedure through which devices choose common transmission parameters such as speed; duplex mode and flow control:

A. Auto-negotiation B. Auto-duplex C. Auto-connection D. Auto-speed

36. Layer 1 device _____.

A. Hub B. Bridge C. Switch D. Router

37. Layer 2 devices _____.

A. Hub B. Bridge C. Switch D. Router

38. Layer 3 devices _____.

A. Hub B. Bridge C. Switch D. Router

39. _____ is a multi-port repeater.

A. Hub B. Bridge C. Switch D. Router

40. _____ is a multi-port bridge.

A. Hub B. Switch C. Router D. Access Point

41. MAC Addresses are also known as _____.

A. Logical Address B. Routing Address C. Network Address D. Physical Address

42. Type of switch that do not require administrative configuration:

A. Managed B. Unmanaged C. Typical D. Custom

43. Acronym - VLAN.

A. Visual LAN B. Virtual LAN C. Vertical LAN D. Viral LAN

44. Device that helps reduce broadcast domains:

A. Hub B. Switch C. Router D. Access Point

45. _____ reduces collisions and improves security.

A. WLAN B. Wi-Fi C. VLAN D. CSMA/CD

46. System that supplies electricity through Ethernet cables:

A. VLAN B. PoE C. WOL D. CSMA/CA

47. Methods used in switching:

A. Store and forward B. Cut through C. Fragment free D. All of the above

48. Device used for creating patch cables:

A. Patch Tool B. Crimping Tool C. Cable Tester D. Loopback Adapter

49. 2-pair Straight-through pin / cable configuration:

A. 1-2; 2-1; 3-6; 6-3 B. 1-3; 3-1; 2-6; 6-2
C. 1-1; 2-2; 3-3; 6-6 D. 1-6; 6-1; 2-3; 3-2

50. 2-pair Cross-over pin / cable configuration:

A. 1-2; 2-1; 3-6; 6-3 B. 1-3; 3-1; 2-6; 6-2
C. 1-1; 2-2; 3-3; 6-6 D. 1-6; 6-1; 2-3; 3-2

51. Command-line utility for viewing MAC address:

A. IPCONFIG B. GETMAC C. VIEWMAC D. HOSTNAME

52. MAC addresses are usually displayed in _____ format.

A. ASCII B. Hexadecimal C. Numeric D. Encrypted

53. Utility for viewing or modifying settings of network interface cards:

A. GETMAC B. Device Manager C. Disk Manager D. Network Manager

54. Correct syntax for viewing MAC address with manufacturer / model details:

A. GETMAC B. GETMAC /v C. IPCONFIG /m D. IPCONFIG /L

55. _____ resolves IP addresses to MAC addresses.

A. ARP B. DHCP C. DNS D. WINS

56. Command to view ARP Cache

A. GETMAC B. IPCONFIG C. ARP D. PING

57. _____ is used for network management & monitoring.

A. SMTP B. SNMP C. POP3 D. FTP

58. Type of Connectors used for Fiber-Optic NIC.

A. RJ-11 B. RJ-45 C. MT-RJ D. BNC

59. Acronym - NEXT (Context: Signaling):

A. Null End Crosstalk B. Null Ethernet Crosstalk
C. Near End Crosstalk D. All of the above

60. Acronym - FEXT (Context: Signaling):

A. Field End Crosstalk B. Far End Crosstalk
C. Federation End Cross Talk D. Far Ethernet Crosstalk

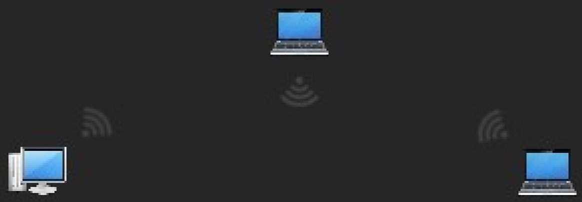
Wi-Fi

Connectivity using Wi-Fi

- Wi-Fi is a trademark of the Wi-Fi Alliance.
- Refers to a collection of wireless technologies based on IEEE 802 standards.
- Operates similarly to a radio, using specific radio frequencies for connectivity.
- Performs best in open environments; physical barriers can reduce speed and range.
- Recommended in situations where wired connections are not feasible or when convenience is a priority.
- Also referred to as a “P2P Network” or “Wi-Fi Direct” in direct device-to-device communication scenarios.
- Uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) as the access method.
- Typical network coverage is up to 100 meters under ideal conditions.
- Common security options include WEP and WPA.

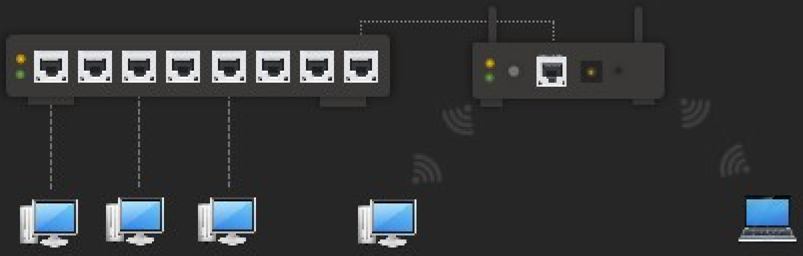
Modes Of Operation

- ADHOC Mode: Computers are connected to each other directly, without need for a base station.



ADHOC Mode, Theory maximum 256 nodes.

- Infrastructure Mode: Wireless clients connect to each other through a base station (usually a wireless access point). It also allows wireless networks to connect to wired networks via the base station, enabling broader network integration and centralized management.



Infrastructure Mode, Theory maximum 2048 nodes.

Note: Maximum number of connections entirely depends on internal hardware & supported technology/standards.

Standards

Generation	IEEE Standard	Speed Range	Radio Frequency
Wi-Fi 1	802.11b	1 to 11 Mbit/s	2.4 GHz
Wi-Fi 2	802.11a	1.5 to 54 Mbit/s	5 GHz
Wi-Fi 3	802.11g	3–54 Mbit/s	2.4 GHz
Wi-Fi 4	802.11n	72–600 Mbit/s	2.4/5 GHz
Wi-Fi 5	802.11ac	433–6933 Mbit/s	5 GHz
Wi-Fi 6	802.11ax	600–9608 Mbit/s	2.4/5 GHz/1–6 GHz ISM

Note: IEEE 802.11n devices may use 2.4 and/or 5 GHz frequency range depending on the model; it is recommended to check technical specification of the product for frequency details.

SSID

- SSID (Service Set Identifier) refers to the network name of a wireless network.
- SSID is commonly known as the Network Name.
- SSIDs are broadcast (advertised) so that wireless clients can discover available networks.
- Maximum 32 Characters, Case Sensitive & Special Charterers are allowed.
- A wireless client can connect to only one SSID at a time.
  - BSSID: Basic SSID is the MAC address of an AP.
  - ESSID: Extended SSID refers to the same SSID used across multiple APs, enabling seamless roaming in larger wireless networks.

Note: In Ad hoc mode, the SSID is referred to as IBSS (Independent Basic Service Set).

Wireless Channels

- Wireless connectivity is established using **regulated channels/frequencies**.
- The 2.4 GHz band is widely used not only by Wi-Fi but also by other devices such as radio remote controls, microwave ovens, cordless phones, and baby monitors, which can cause signal interference.
- 5 GHz band is less congested, as fewer consumer devices operate in this frequency range compared to 2.4 GHz.
- Wi-Fi standards define both overlapping and non-overlapping channels, which can affect network performance and interference.

Standard	Frequency	Bandwidth	Speeds (Mbps)	Max. Stream(s)
IEEE 802.11b	2.4 GHz	20 MHz	1, 2, 5.5 & 11	1
IEEE 802.11a	5 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48 & 54	1
IEEE 802.11g	2.4 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48 & 54	1
IEEE 802.11n	2.4 / 5 GHz	20 MHz	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65 & 72.2	4
		40 MHz	15, 30, 45, 60, 90, 120, 135 & 150	4
IEEE 802.11ac	5 GHz	20 MHz	Up to 87.6	8
		40 MHz	Up to 200	8
		60 MHz	Up to 433.3	8
		80 MHz	Up to 866.7	8

Reference(s):

https://en.wikipedia.org/wiki/List_of_WLAN_channels
https://en.wikipedia.org/wiki/IEEE_802.11

https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation
https://en.wikipedia.org/wiki/IEEE_802.11ac

Wireless Security

In wireless networks, signals are transmitted over the air and are prone to eavesdropping. To secure these networks, encryption standards such as WEP and the more secure WPA/WPA2 are commonly used.

Note: An "Open Network" is a wireless network with no security measures—anyone can connect to it without a password.

- WEP
  - Wired Equivalent Privacy, 1st encryption algorithm for Wireless networks.
  - Supports 64-bit, 128-bit, or 256-bit encryption.
  - Outdated (yet still used in some scenarios).
- WPA
  - Wi-Fi Protected Access.
  - Uses Temporal Key Integrity Protocol.
  - Assigns a unique 128-bit key for each packet, offering improved security.
- WPA2
  - Much stronger than WEP or WPA.
  - Uses CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).
  - Highly recommended for all modern wireless networks.

Note: Always use WPA2 if available, as it provides the best security among current wireless standards.

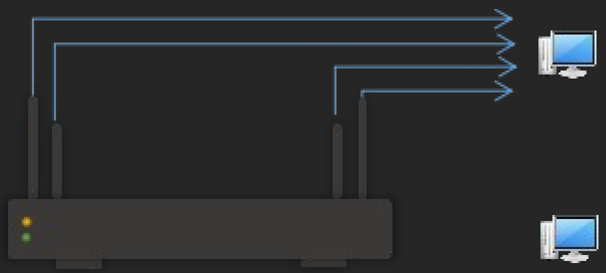
WPS - “Wi-Fi Protected Setup”

- A convenience feature found on many SOHO (Small Office/Home Office) routers and access points.
- Allows users to connect to a network using a PIN or push button, instead of entering a password.
- Not as secure as WPA/WPA2 and is not recommended for networks where security is a priority.

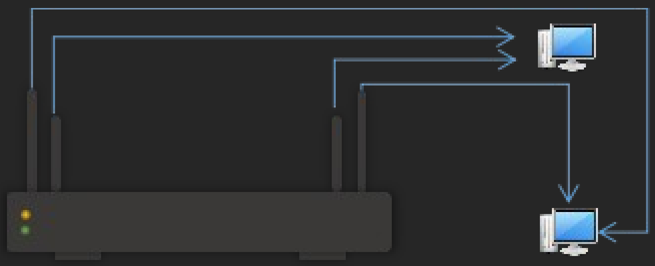
MIMO

MIMO enables the simultaneous use of multiple radio links to achieve higher speeds. This feature was introduced in IEEE 802.11n. Devices or computers that support MIMO typically have two or more antennas to take advantage of this capability.

- SU-MIMO
    - Stands for Single-User Multiple Input Multiple Output.
    - Only one device is served at a time using multiple spatial streams.
    - Common in Wi-Fi 4 (802.11n) and early Wi-Fi 5 (802.11ac) implementations.
- MU-MIMO
    - Stands for Multi-User Multiple Input Multiple Output.
    - Allows multiple devices to be served simultaneously, improving network efficiency.
    - Introduced in Wi-Fi 5 and enhanced in Wi-Fi 6 to support both uplink and downlink communication.



SU-MIMO, 4 Streams to a single client



MU-MIMO, 2 streams each to 2 clients

Note: Client devices must support MU-MIMO to benefit from it. MU-MIMO USB dongles and network cards are available for devices that don't have built-in support. Many recent laptops and smartphones come with MU-MIMO support out of the box.

IEEE 802.11ac

- Manufacturers often advertise products based on combined throughput.
- For example, AC1900 means a total speed of 1900 Mbps, which is the sum of 600 Mbps on the 2.4 GHz band and 1300 Mbps on the 5 GHz band.

Type	2.4 GHz		5 GHz	
	Mbit/s	[all 40 MHz]	Mbit/s	[all 80 MHz]
AC450	-	-	433	1 stream @ MCS 9
AC600	150	1 stream @ MCS 7	433	1 stream @ MCS 9
AC750	300	2 streams @ MCS 7	433	1 stream @ MCS 9
AC1000	300	2 streams @ MCS 7	650	2 streams @ MCS 7
AC1200	300	2 streams @ MCS 7	867	2 streams @ MCS 9
AC1300	400	2 streams @ 256-QAM	867	2 streams @ MCS 9
AC1300	-	-	1,300	3 streams @ MCS 9
AC1350	450	3 streams @ MCS 7	867	2 streams @ MCS 9
AC1450	450	3 streams @ MCS 7	975	3 streams @ MCS 7
AC1600	300	2 streams @ MCS 7	1,300	3 streams @ MCS 9
AC1700	800	4 streams @ 256-QAM	867	2 streams @ MCS 9
AC1750	450	3 streams @ MCS 7	1,300	3 streams @ MCS 9
AC1900	600	3 streams @ 256-QAM	1,300	3 streams @ MCS 9
AC2100	800	4 streams @ 256-QAM	1,300	3 streams @ MCS 9
AC2200	450	3 streams @ MCS 7	1,733	4 streams @ MCS 9
AC2300	600	4 streams @ MCS 7	1,625	3 streams @ 1024-QAM
AC2400	600	4 streams @ MCS 7	1,733	4 streams @ MCS 9
AC2600	800	4 streams @ 256-QAM	1,733	4 streams @ MCS 9
AC3000	450	3 streams @ MCS 7	1,300 + 1,300	3 streams @ MCS 9 x 2
AC3150	1000	4 streams @ 1024-QAM	2,167	4 streams @ 1024-QAM
AC3200	600	3 streams @ 256-QAM	1,300 + 1,300	3 streams @ MCS 9 x 2
AC5000	600	4 streams @ MCS 7	2,167 + 2,167	4 streams @ 1024-QAM x 2
AC5300	1000	4 streams @ 1024-QAM	2,167 + 2,167	4 streams @ 1024-QAM x 2

Wireless NIC

Computers connected via Wireless NIC

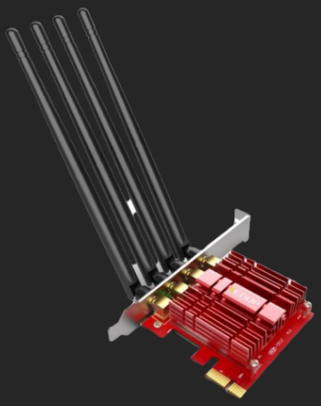
- Use radio signals for communication instead of physical cables.
- Follow IEEE 802.11 standards.
- Operate mainly at OSI Layer 1 (Radio Signals) and Layer 2 (MAC Address and wireless access protocol, CSMA/CA).
- Available in various forms such as PCI, PCIe, USB adapters, or integrated into devices.
- Signal quality can vary based on location, interference, and antenna design.
- Generally provide less consistent speeds compared to wired NICs.
- Most recent laptops, all-in-one PCs, and mobile phones include wireless NICs by default.

WNIC for Desktops

WNIC module for Laptops

USB WNIC

USB WNIC Mini Dongle

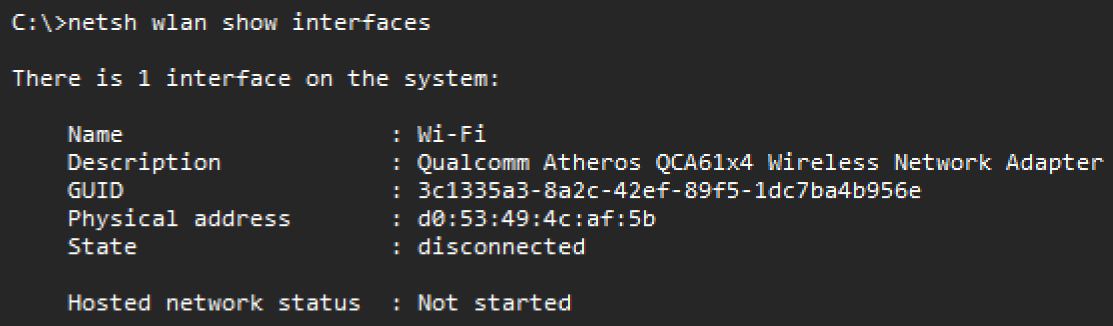


WNIC, 4 Antennas

Note: It is recommended to check the technical specifications of a wireless NIC to confirm the supported standards and other features such as MIMO.

Wireless Adapters Worksheet			
Vendor			
Model			
Interface			
PCI			
PCIe			
USB			
PCMCIA			
CardBus			
32 / 64 bit			
Supported OS (Device Drivers)			
Microsoft Windows			
Linux			
MAC OS			
Standard Compliance			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			
IEEE 802.11n			
IEEE 802.11ac			
IEEE 802.11ax			
Frequency			
2.4 GHz			
5 GHz			
Dual Band			
Triband			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
WPS			
Antennas			
1x1 SISO			
2x2 MIMO			
3x3 MIMO			
4x4 MIMO			
Detachable (Yes/No)			

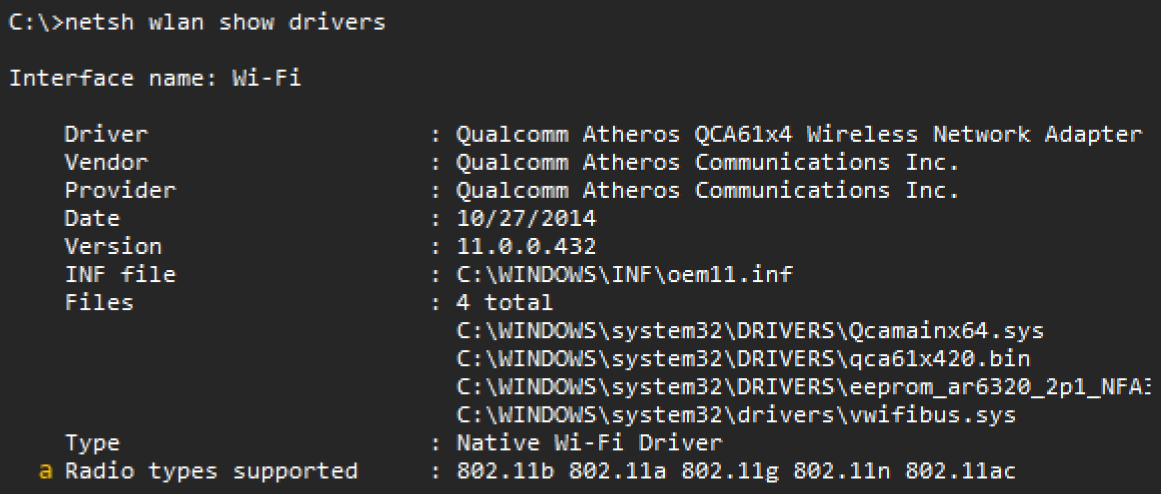
- View list of WNIC:
  - CMD > netsh wlan show interfaces



```
C:\>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : Wi-Fi
    Description            : Qualcomm Atheros QCA61x4 Wireless Network Adapter
    GUID                   : 3c1335a3-8a2c-42ef-89f5-1dc7ba4b956e
    Physical address       : d0:53:49:4c:af:5b
    State                  : disconnected

    Hosted network status  : Not started
```

Output listing only Wireless Adapters (Not associated)

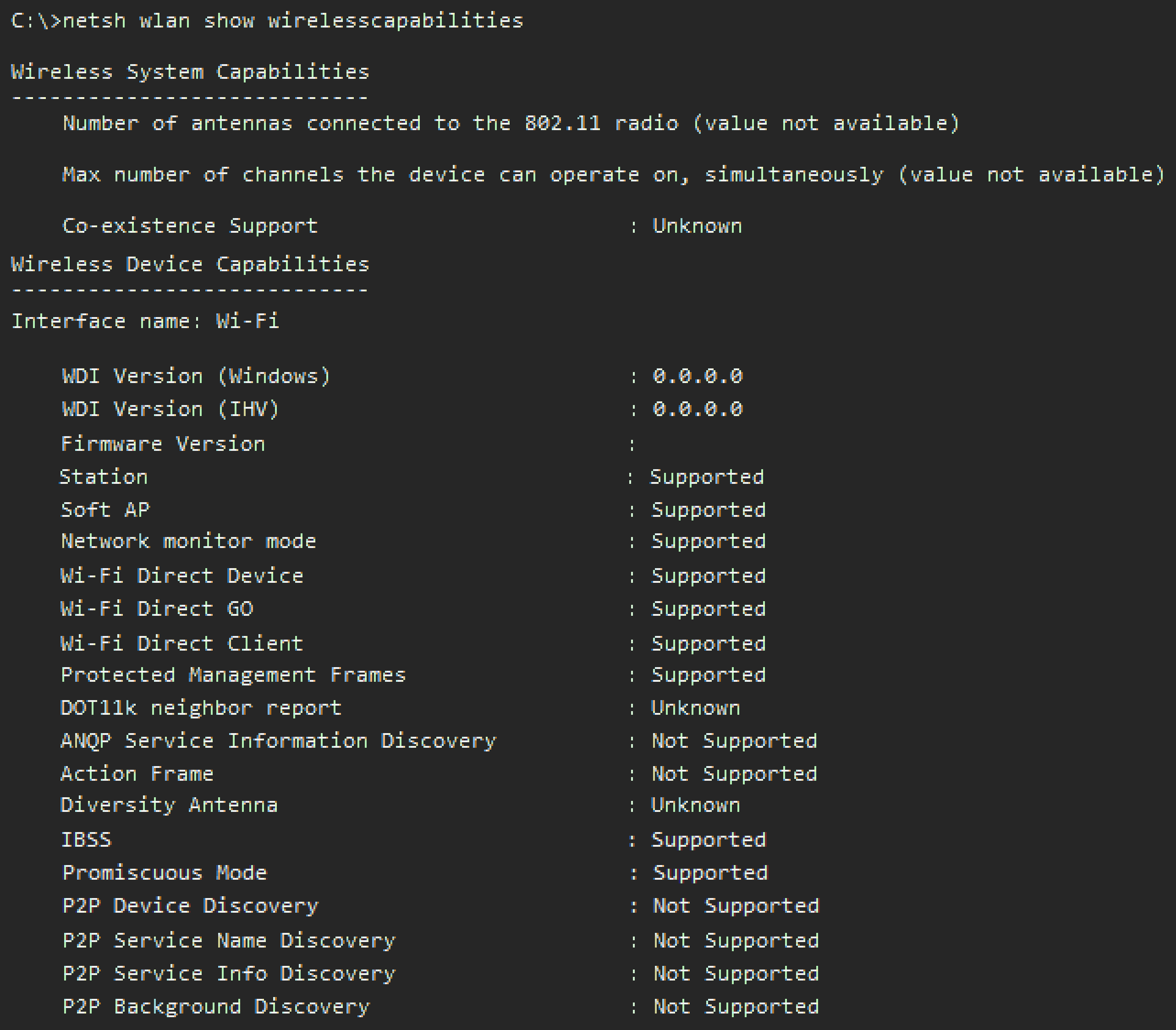
- View IEEE standards supported by WNIC:
  - CMD > netsh wlan show drivers



```
C:\>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                    : Qualcomm Atheros QCA61x4 Wireless Network Adapter
    Vendor                    : Qualcomm Atheros Communications Inc.
    Provider                  : Qualcomm Atheros Communications Inc.
    Date                      : 10/27/2014
    Version                   : 11.0.0.432
    INF file                  : C:\WINDOWS\INF\oem11.inf
    Files                     : 4 total
                                C:\WINDOWS\system32\DRIVERS\Qcamainx64.sys
                                C:\WINDOWS\system32\DRIVERS\qca61x420.bin
                                C:\WINDOWS\system32\DRIVERS\eeprom_ar6320_2p1_NFA
                                C:\WINDOWS\system32\drivers\vwifibus.sys
    Type                      : Native Wi-Fi Driver
  a Radio types supported     : 802.11b 802.11a 802.11g 802.11n 802.11ac
```

Output a) IEEE 802.11 standards supported by the Wireless adapter

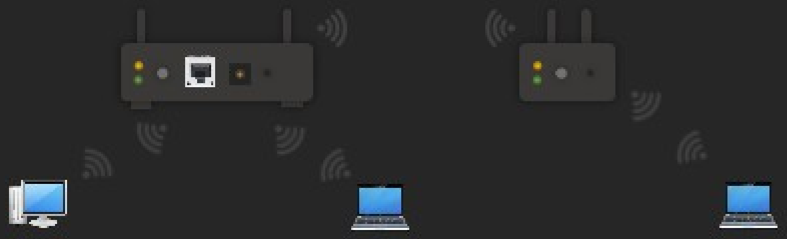
- Show Wireless Adapter’s capabilities (Microsoft Windows 10)
  - CMD > netsh wlan show wirelesscapabilities



```
C:\>netsh wlan show wirelesscapabilities

Wireless System Capabilities
----------------------------
    Number of antennas connected to the 802.11 radio (value not available)

    Max number of channels the device can operate on, simultaneously (value not available)

    Co-existence Support                          : Unknown
Wireless Device Capabilities
----------------------------
Interface name: Wi-Fi

    WDI Version (Windows)                         : 0.0.0.0
    WDI Version (IHV)                             : 0.0.0.0
    Firmware Version                              :
    Station                                       : Supported
    Soft AP                                       : Supported
    Network monitor mode                          : Supported
    Wi-Fi Direct Device                           : Supported
    Wi-Fi Direct GO                               : Supported
    Wi-Fi Direct Client                           : Supported
    Protected Management Frames                   : Supported
    DOT11k neighbor report                        : Unknown
    ANQP Service Information Discovery            : Not Supported
    Action Frame                                  : Not Supported
    Diversity Antenna                             : Unknown
    IBSS                                          : Supported
    Promiscuous Mode                              : Supported
    P2P Device Discovery                          : Not Supported
    P2P Service Name Discovery                    : Not Supported
    P2P Service Info Discovery                    : Not Supported
    P2P Background Discovery                      : Not Supported
```

Output listing features supported by WNIC

Access Point



Wireless AP with 2 clients, 3rd Client connected via Wireless Extender

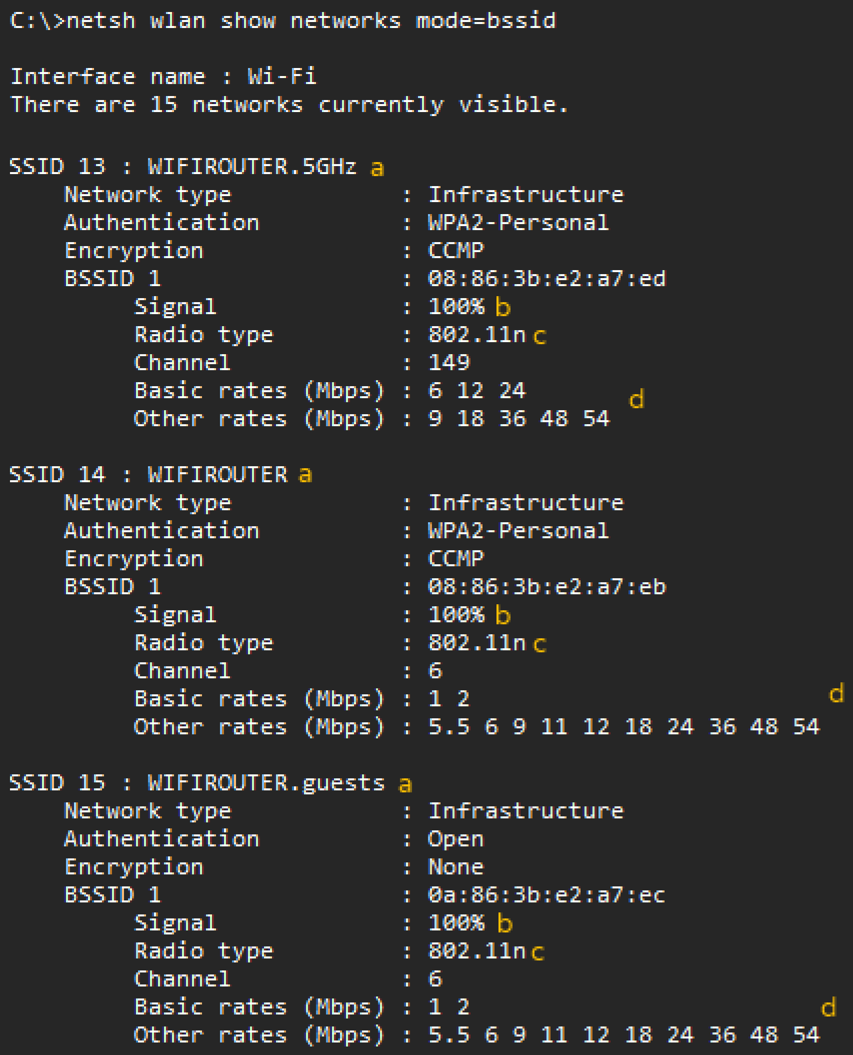
- A simple device (also called a Base Station) that centralizes wireless networks.
- Connects wireless networks to wired networks.
- Wireless Range Extenders are used to expand the coverage of wireless networks, supporting roaming.
- Depending on the model, wireless access points may offer features such as timed usage, user management, guest access, DHCP service, and firewall.
- Indoor APs are designed for use inside homes or small offices, providing limited coverage.
- Outdoor APs are built for long-distance coverage, such as on campuses or for building-to-building links.

Access Point

Outdoor Access Point

Wireless Range Extender

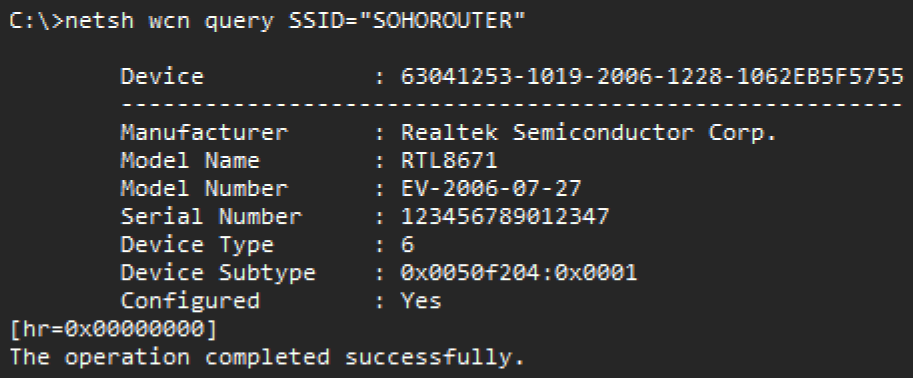
- View list of Wireless Networks:
  - CMD > netsh wlan show networks mode=bssid



```
C:\>netsh wlan show networks mode=bssid

Interface name : Wi-Fi
There are 15 networks currently visible.

SSID 13 : WIFIROUTER.5GHz a
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 08:86:3b:e2:a7:ed
         Signal             : 100% b
         Radio type         : 802.11n c
         Channel            : 149
         Basic rates (Mbps) : 6 12 24          d
         Other rates (Mbps) : 9 18 36 48 54

SSID 14 : WIFIROUTER a
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
    BSSID 1                 : 08:86:3b:e2:a7:eb
         Signal             : 100% b
         Radio type         : 802.11n c
         Channel            : 6
         Basic rates (Mbps) : 1 2                            d
         Other rates (Mbps) : 5.5 6 9 11 12 18 24 36 48 54

SSID 15 : WIFIROUTER.guests a
    Network type            : Infrastructure
    Authentication          : Open
    Encryption              : None
    BSSID 1                 : 0a:86:3b:e2:a7:ec
         Signal             : 100% b
         Radio type         : 802.11n c
         Channel            : 6
         Basic rates (Mbps) : 1 2                           d
         Other rates (Mbps) : 5.5 6 9 11 12 18 24 36 48 54
```

Output (edited to show limited results) listing a) all available Wireless networks, b) Signal strength, c) IEEE standards & d) supported speeds. This particular model supports both 2.4 GHz & 5 GHz.

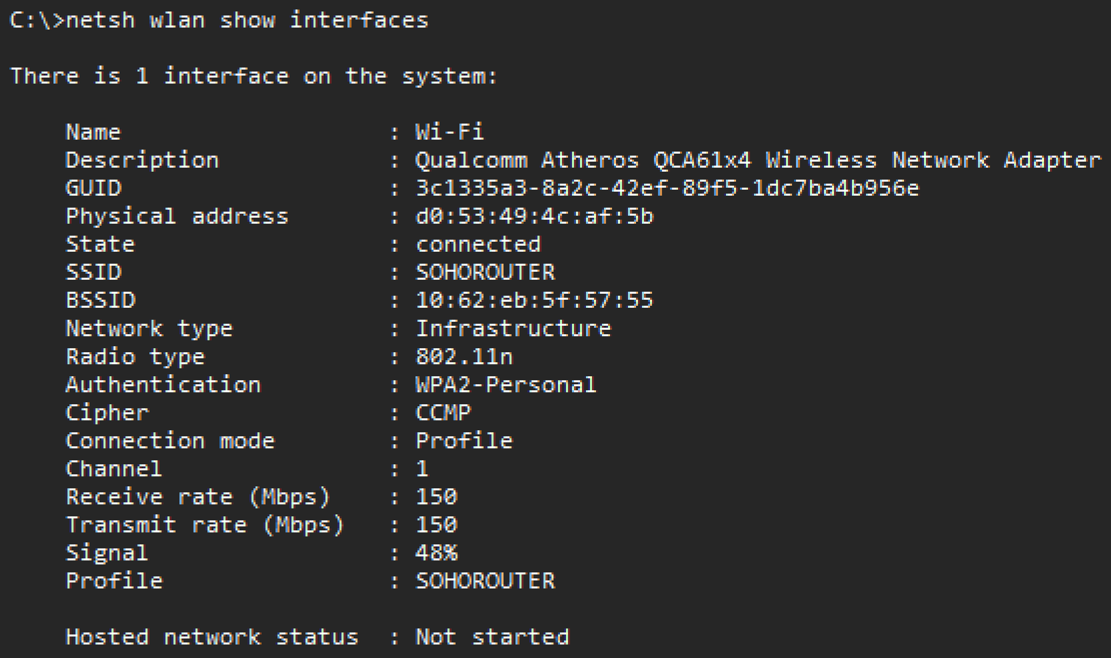
- View technical details of an access point or wireless router:
  - CMD > netsh wcn query SSID=”SSID”



```
C:\>netsh wcn query SSID="SOHOROUTER"

        Device              : 63041253-1019-2006-1228-1062EB5F5755
        --------------------------------------------------------
        Manufacturer        : Realtek Semiconductor Corp.
        Model Name          : RTL8671
        Model Number        : EV-2006-07-27
        Serial Number       : 123456789012347
        Device Type         : 6
        Device Subtype      : 0x0050f204:0x0001
        Configured          : Yes
[hr=0x00000000]
The operation completed successfully.
```

Output listing details of an Access Point/SOHO Router (from a WCN capable device)

- View Wi-Fi details (Associated):
  - CMD > netsh wlan show interfaces

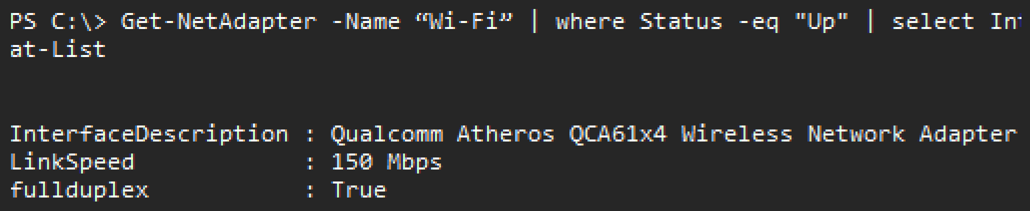


```
C:\>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : Wi-Fi
    Description            : Qualcomm Atheros QCA61x4 Wireless Network Adapter
    GUID                   : 3c1335a3-8a2c-42ef-89f5-1dc7ba4b956e
    Physical address       : d0:53:49:4c:af:5b
    State                  : connected
    SSID                   : SOHOROUTER
    BSSID                  : 10:62:eb:5f:57:55
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 1
    Receive rate (Mbps)    : 150
    Transmit rate (Mbps)   : 150
    Signal                 : 48%
    Profile                : SOHOROUTER

    Hosted network status  : Not started
```

Output listing Wi-Fi details based on a connection

Note: “Associated” is the term used in Wireless Networks, instead of “Connected”.

- View details for a specific connection:
  - CMD > Powershell > Get-NetAdapter -Name “CONNECTIONNAME” | where Status -eq "Up" | select InterfaceDescription, LinkSpeed, fullduplex | Format-List

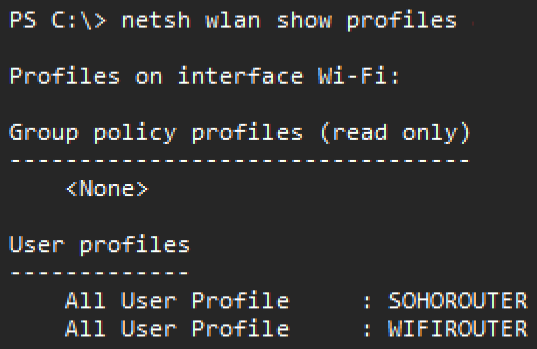


```
PS C:\> Get-NetAdapter -Name “Wi-Fi” | where Status -eq "Up" | select In
at-List


InterfaceDescription : Qualcomm Atheros QCA61x4 Wireless Network Adapter
LinkSpeed            : 150 Mbps
fullduplex           : True
```

Output listing Speed & Duplex details for a specific wireless connection

Microsoft Windows maintains details of wireless connections (if connected earlier) as “profiles”.

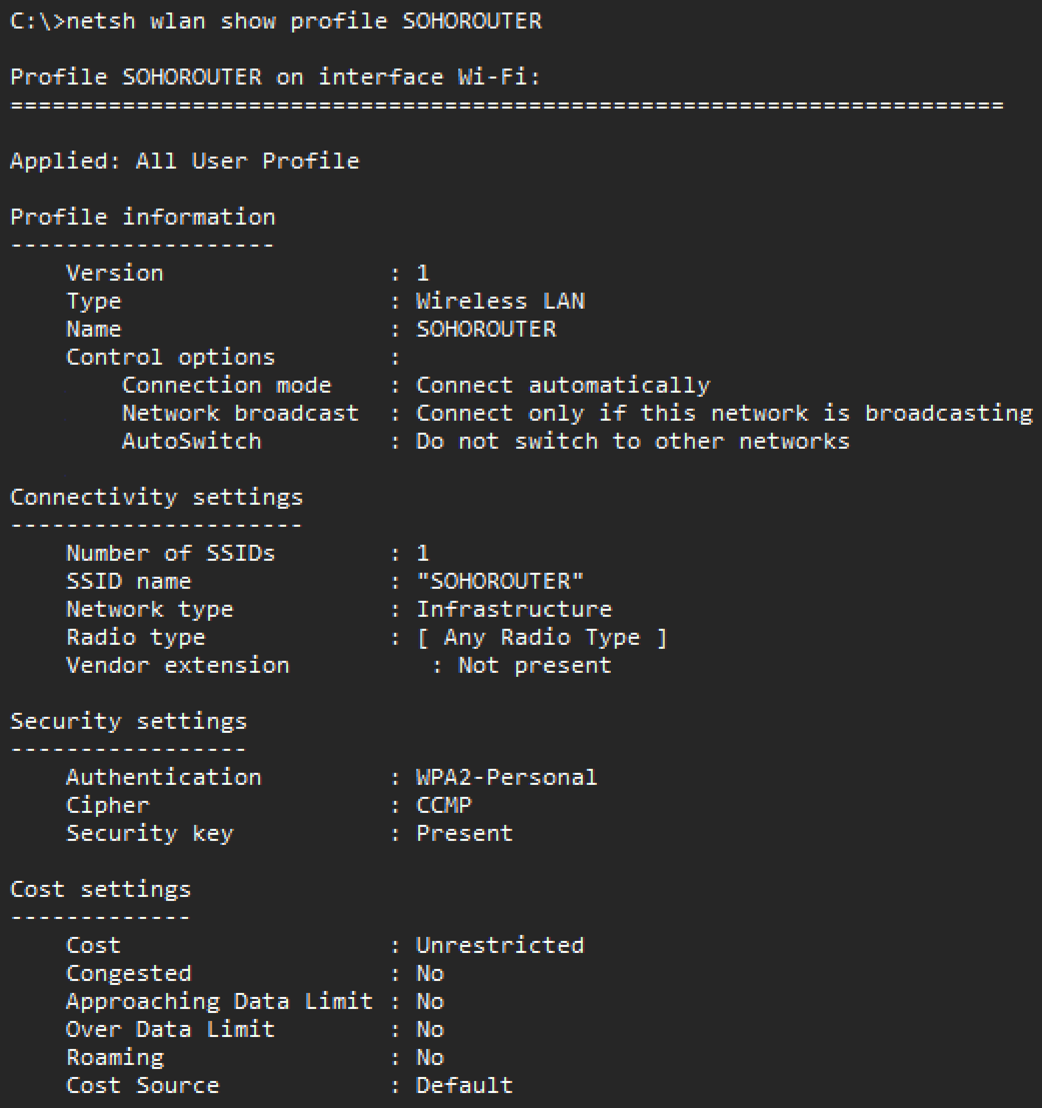
- View list of saved Wireless Profiles:
  - CMD > netsh wlan show profiles



```
PS C:\> netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : SOHOROUTER
    All User Profile     : WIFIROUTER
```

Output listing all stored profiles

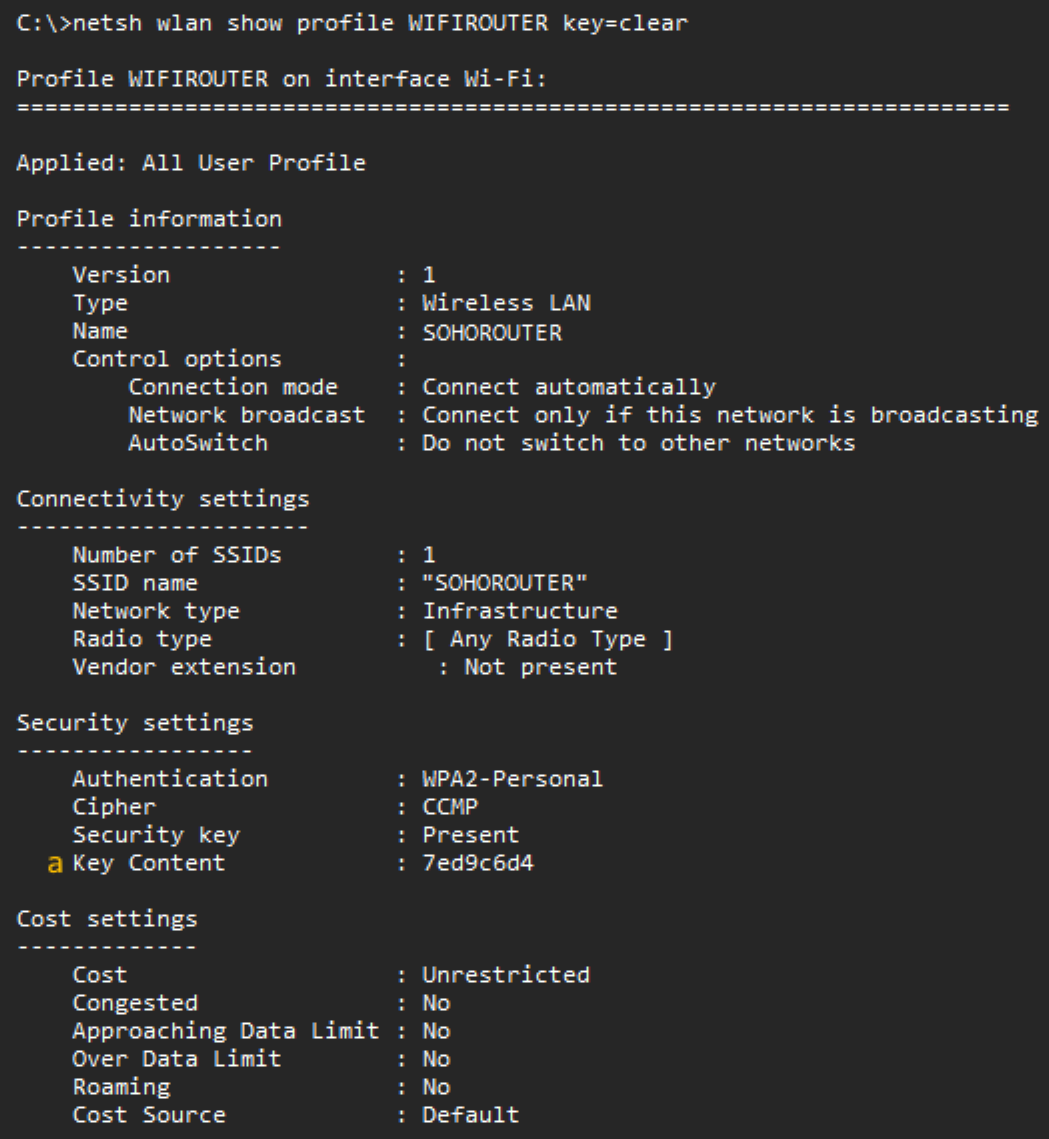
- Show details for a specific profile:
    - CMD > netsh wlan show profile PROFILENAME



```
C:\>netsh wlan show profile SOHOROUTER

Profile SOHOROUTER on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SOHOROUTER
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SOHOROUTER"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Security key           : Present

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default
```

Output listing preferences of a particular network, as stored on a computer

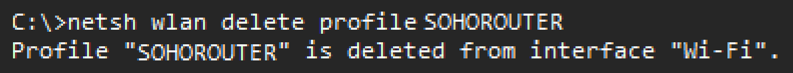
- Show Wi-Fi Password (Stored):
  - CMD > netsh wlan show profile PROFILENAME key=clear



```
C:\>netsh wlan show profile WIFIROUTER key=clear

Profile WIFIROUTER on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : SOHOROUTER
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "SOHOROUTER"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Security key           : Present
  a Key Content            : 7ed9c6d4

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default
```

Output showing stored wireless password for a specific profile saved earlier (key content)

- To delete a profile:
  - CMD > netsh wlan delete profile PROFILENAME



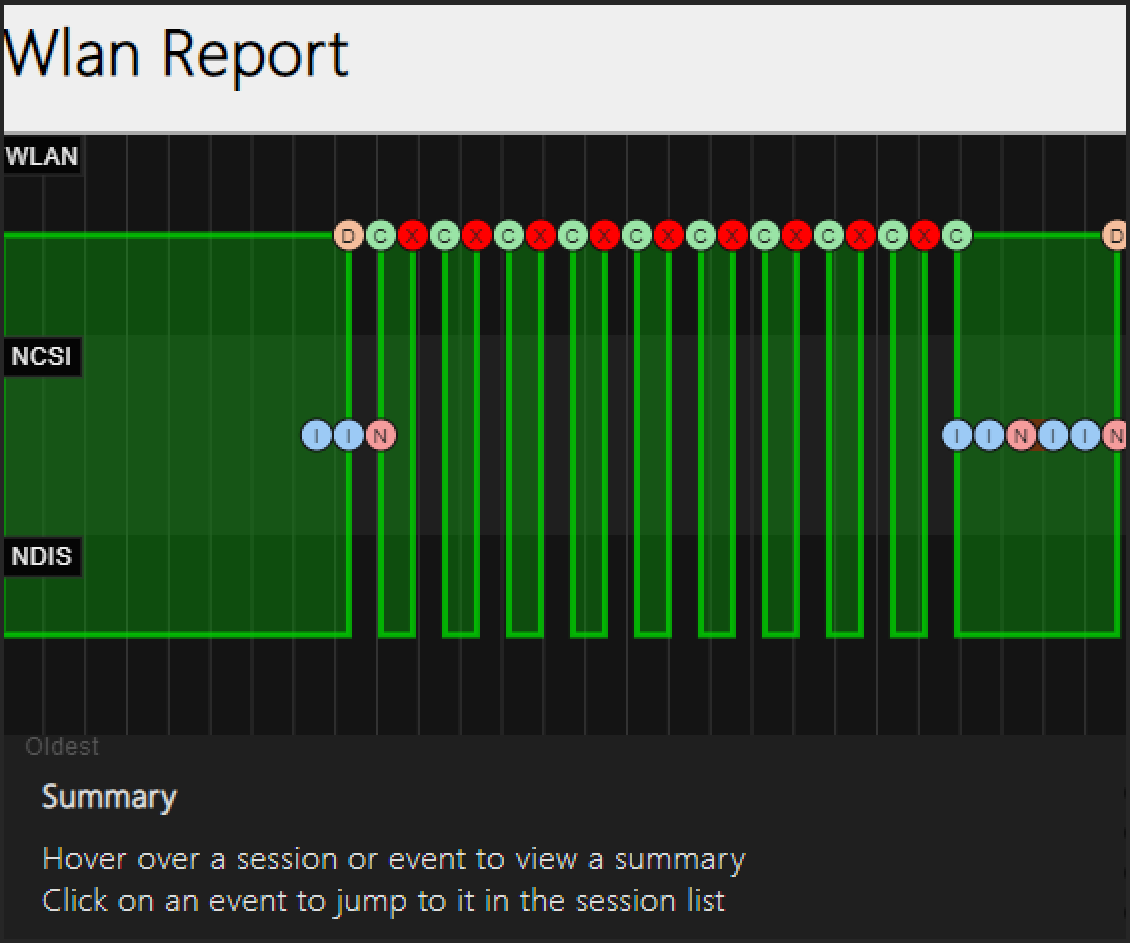
```
C:\>netsh wlan delete profile SOHOROUTER
Profile "SOHOROUTER" is deleted from interface "Wi-Fi".
```

Input to delete a profile

- View Wireless Report (Microsoft Windows 10):
  - CMD > netsh wlan show wlanreport
  - View C:\ProgramData\Microsoft\Windows\WLANReport\WLAN-report-latest.html

```
C:\>netsh wlan show wlanreport
Generating report ...
Querying WLAN Events ...
Querying NCSI Events ...
Querying NDIS Events ...
Querying EAP Events ...
Querying WCM Events ...
Querying Kernel Events ...
Querying System Events ...
Running ipconfig ...
Running netsh wlan show all ...
Querying Wireless Profiles ...
Querying System and User Certificates ...
Querying User Info ...
Querying Network Devices ...

Report written to: C:\ProgramData\Microsoft\Windows\WlanReport\wlan-report-latest.html
done.
```

/
nput to generate report (Microsoft Windows 10)



Wlan Report

Summary

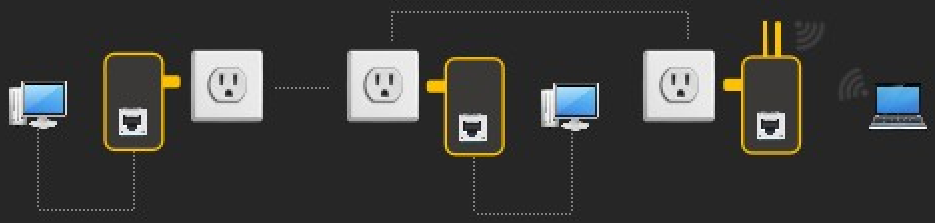
Hover over a session or event to view a summary
Click on an event to jump to it in the session list

WLAN Report Sample

Wireless Access Point Worksheet			
Vendor			
Model			
Firewall (Available / Not Available)			
Parental Control			
Beamforming			
Can be used as Wireless Extender? (Yes / No)			
Frequency			
2.4 GHz			
5 GHz			
Dual Band			
Tri Band			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
WPS			
Antennas			
1x1 SISO			
2x2 MIMO			
3x3 MIMO			
4x4 MIMO			
Detachable (Yes/No)			
Standard Compliance			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
IEEE 802.3z			
IEEE 802.1q			
IEEE 802.1p			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			
IEEE 802.11n			
IEEE 802.11ac			
IEEE 802.11ax			

Powerline

- Powerline networking allows devices to communicate over existing electrical wiring in a home or office, eliminating the need for additional network cables.
- It follows HomePlug AV and IEEE 1901 standards.
- Speeds can reach up to 500 Mbps or more, depending on the latest standards.
- Commercially available as a "kit" that includes at least two adapters.
- Supports up to 64 adapters on a single network, depending on the model.
- Usually does not work across closed circuit breakers.
- Performance can be affected by electrical noise from appliances such as refrigerators, microwaves, and other devices.



Two computers connected via Powerline Adapters through Ethernet & One Computer via Wireless

Powerline Adapter

Powerline Adapter, 3 LAN Ports

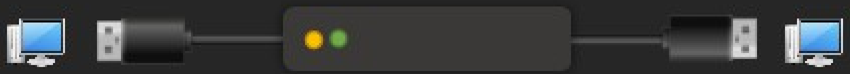
Powerline Adapter, Wi-Fi

For example:

1. Insert Straight-Through cable into LAN ports (of computer & Powerline adapter).
2. Connect Powerline adapter to power socket.
3. Configure network using the software provided along with Powerline adapter.

Powerline Adapters Worksheet			
Vendor			
Model			
Ports			
# of RJ-45 Ports			
# of Fiber Optic Ports			
Standard Compliance			
HomePlug AV			
HomePlug AV2			
IEEE 1901			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
IEEE 802.3z			
IEEE 802.1q			
IEEE 802.1p			
IEEE 802.11b			
IEEE 802.11a			
IEEE 802.11g			
IEEE 802.11n			
IEEE 802.11ac			
IEEE 802.11ax			

USB Ports



Connectivity using "Easy Transfer Cable" via USB

- Connecting computers via USB requires a special type of cable, such as an "Easy Transfer Cable."
- Typically, additional software (often bundled with the cable) is needed to set up the connection.

USB Bridge Cable

IEEE 1394

- IEEE 1394 is a high-speed serial interface standard designed for data transfer between devices like computers, cameras, and external storage. It is commonly known as FireWire, a term trademarked by Apple Inc.
- Typical speeds include 400 Mbps (FireWire 400) and 800 Mbps (FireWire 800). Newer versions of the standard can reach speeds up to 3.2 Gbps.

IEEE 1394 Cable

PCIe FireWire Card

Note: There are different types of connectors, not listed here.

Standards

Standard	Mbit/s	MB/s
FireWire (IEEE 1394) 100	98.304	12.288
FireWire (IEEE 1394) 200	196.608	24.576
FireWire (IEEE 1394) 400	393.216	49.152
FireWire (IEEE 1394b) 800	786.432	98.304
FireWire (IEEE 1394b) 1600	1.573	196.6
FireWire (IEEE 1394b) 3200	3.1457	393.216

Quiz 04

1. IEEE standards for WLAN (Wi-Fi):

A. 802.11 b/g B. 802.11 a C. 802.11 n D. 802.11 ac

2. Radio Frequency - IEEE 802.11 a:

A. 2.4 GHz B. 2.8 GHz C. 5 GHz D. None

3. Radio Frequency - IEEE 802.11 b/g:

A. 2.4 GHz B. 2.8 GHz C. 5 GHz D. Both A & C

4. Radio Frequency - IEEE 802.11 ac:

A. 2.4 GHz B. 2.8 GHz C. 5 GHz D. All of the above

5. Radio Frequency - IEEE 802.11 n:

A. 2.4 GHz B. 2.8 GHz C. 5 GHz D. Both A & C

6. Maximum speed supported by IEEE 802.11b:

A. 11 Mbps B. 54 Mbps C. 600 Mbps D. 1 Gbps

7. Maximum speed supported by IEEE 802.11a:

A. 11 Mbps B. 54 Mbps C. 600 Mbps D. 1 Gbps

8. Maximum speed supported by IEEE 802.11g:

A. 11 Mbps B. 54 Mbps C. 600 Mbps D. 1 Gbps

9. Maximum speed supported by IEEE 802.11n:

A. 11 Mbps B. 54 Mbps C. 600 Mbps D. 1 Gbps

10. Maximum speed supported by IEEE 802.11ac:

A. 11 Mbps B. 54 Mbps C. 600 Mbps D. 6.77 Gbps

11. WLAN utilizes _____ technologies for transmissions:

A. OFDM B. IR C. Bluetooth D. None

12. Tethering is also referred to as:

A. Mobile Hotspot B. Wireless Fidelity C. NFC D. None

13. Device required for setting up a Wi-Fi Network:

A. Repeater B. Access Point C. Hub D. Router

14. Peer-to-Peer wireless networks are referred to as:

A. Infrastructure Networks   B. ADHOC Networks
C. Peer Level Networks   D. All of the above

15. Infrastructure wireless networks require:

A. Repeater   B. Access Point   C. Hub   D. Router

16. Device that acts as a bridge between wired and wireless networks:

A. Repeater   B. Access Point   C. Hub   D. Router

17. Acronym - SSID:

A. Secure Set Identifier   B. Simple Set Identifier
C. Synchronous Set Identifier   D. Service Set Identifier

18. SSID - Maximum number of characters:

A. 8   B. 16   C. 32   D. 64

19. In wireless networks a device may be associated with _____ SSIDs:

A. 4   B. 1   C. 12   D. Unlimited

20. Dual band devices typically

A. Allow use of both 2.4 GHz and 5 GHz   B. Supports longer range
C. Supports more than 1 SSID   D. None of the above

21. Acronym - WAP:

A. Wired Access Point   B. Wireless Access Point
C. Wireless Area Point   D. Wired Area Point

22. _____ refers to unauthorized access of wireless networks.

A. Postpaid   B. Secure Connect   C. Piggybacking   D. None

23. Ways to protect wireless networks:

A. Disable SSID Broadcast   B. Implement WPA   C. Change default SSID   D. All of the above

24. Acronym - WEP

A. Wireless Equivalent Privacy   B. Wired Equivalent Privacy
C. Wi-Fi Equivalent Privacy   D. Wireless Encrypted Privacy

25. Acronym - WPA

A. Wireless Protected Access   B. Wired Protected Access
C. Wi-Fi Protected Access   D. Wi-Fi Protected Array

26. Acronym - TKIP

A. Temporal Key Integrity Practice B. Temporary Key Integrity Protocol
C. Temporal Key Intelligent Protocol D. Temporal Key Integrity Protocol

27. Items that cause interference to wireless signals:

A. Steel B. Concrete C. Wood D. All of the above

28. 64 bit WEP uses _____ hexadecimal characters.

A. 8 B. 12 C. 26 D. 10

29. 128 bit WEP uses _____ hexadecimal characters.

A. 8 B. 12 C. 26 D. 10

30. Most recent wireless encryption standard:

A. 128 bit WEP B. 64 bit WEP C. WPA D. WPA2

31. _____ utilizes per-packet key.

A. PoE B. WEP C. WPA D. NoN

32. Acronym - WPS

A. Wireless Protected Setup B. Wi-Fi Protected Setup
C. Wired Protected Setup D. Wired Protected Sync

33. Devices that cause interference to wireless signals:

A. Cordless Phones B. Microwave Ovens C. Baby Monitors D. All of the above

34. Acronym - AES

A. Analytical Encryption Standard B. Alternate Encryption Standard
C. Adverse Encryption Standard D. Advanced Encryption Standard

35. Acronym - MIMO.

A. Multiple-Input; Multiple-Out B. Minute-Input; Minute-Out
C. Micro-Input; Micro-Out D. Macro-Input; Macro-Out

36. MIMO technique is used in:

A. IEEE 802.11g B. IEEE 802.11b C. IEEE 802.11n D. Both A & B

37. Technique that allows connections only if a WAP finds matching address:

A. WEP B. WPA C. MAC Authentication D. IP Spoofing

38. The term 'IBSS' refers to:

A. Switched Networks B. Infrastructure Networks
C. ADHOC Networks D. Managed Networks

39. The term 'BSS' refers to:

A. Switched Networks B. Infrastructure Networks
C. ADHOC Networks D. Managed Networks

40. Acronym - ESS.

A. Emulated Service Set B. Extended Service Setup
C. Extended Service Set D. Emulated Service Setup

41. Acronym - IBSS.

A. Internet BSS B. Intranet BSS C. Inline BSS D. Independent BSS

42. Network access method used in wireless networks:

A. CSMA/CD B. CSMA/CA C. CSMA/Wi-Fi D. CSMA/CF

43. Acronym - CSMA/CA

A. Carrier Sense Multiple Access/Collision Avoidance
B. Career Sense Multiple Access/Collision Avoidance
C. Carrier Sense Multiple Access/Collision Access
D. Career Sense Multiple Access/Collision Access

44. Acronym - QAM

A. Quad Processor Modulation B. Quadrature Amplitude Modulation
C. Quad Amplifier D. None of the above

45. Technology that allows to form a network using electricity Lines:

A. Powerline B. DSL C. Cable D. ISDN

46. Standards related to Powerline

A. IEEE 1801 B. HomePlug AV C. IEEE 1901 D. IEEE 802.11

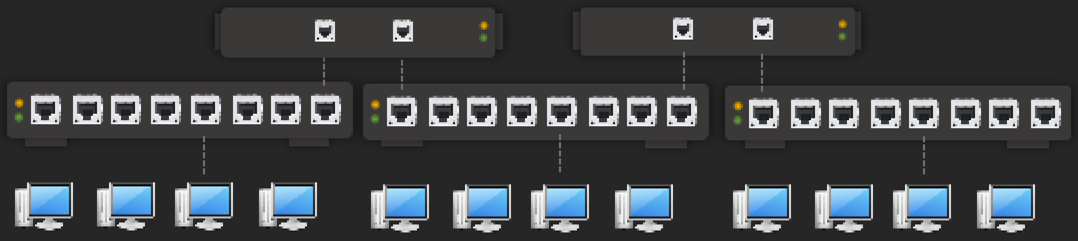
47. Standard related to FireWire

A. IEEE 1901 B. IEEE 802.11 C. IEEE 1284 D. IEEE 1394

48. Speeds supported by FireWire

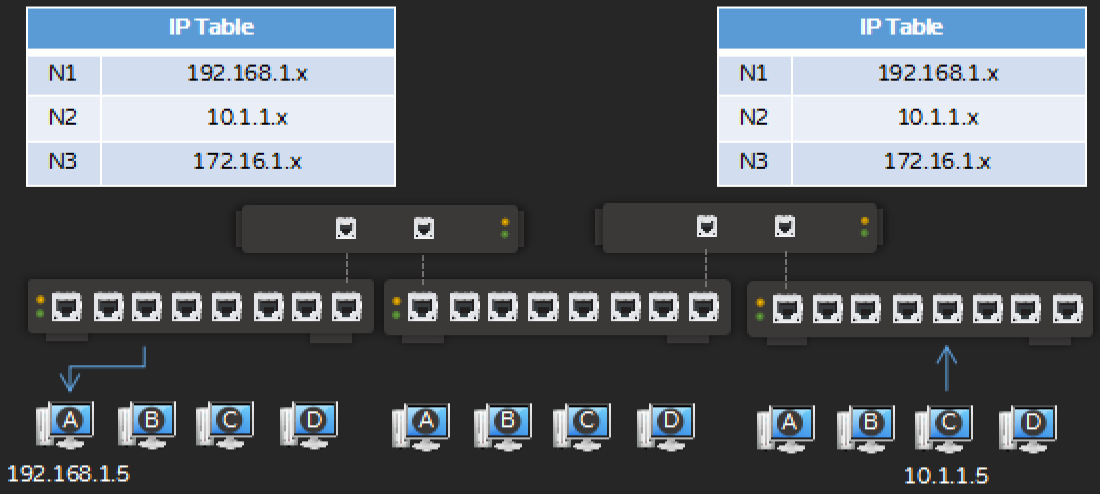
A. 400 Mbps B. 800 Mbps C. 1600 Mbps D. 400 Gbps

Router



3 Network Switches connected to 2 Routers

- Operates at Layer 3 (Network).
- Routes IP packets across different logical networks.
- Discovers and builds routing tables to direct packets efficiently.
- Used to manage enterprise networks and connect to external networks like the Internet.
- Routers are generally complex devices requiring specific technical expertise as per manufacturer specifications.
- May include features such as MAC/IP filtering, firewall, Access Control Lists (ACLs), VPN, and Quality of Service (QoS).
- Supports dynamic routing protocols like RIP, OSPF, EIGRP, and BGP.



IP Table	
N1	192.168.1.x
N2	10.1.1.x
N3	172.16.1.x

IP Table	
N1	192.168.1.x
N2	10.1.1.x
N3	172.16.1.x

Layer 3: Routers "exchange" routing tables, determine path and route packets

Note: Do not confuse enterprise routers with SOHO (Small Office/Home Office) or residential routers, which are typically simpler devices.

Feature	SOHO Router	Enterprise Router
Primary Focus	Home and small office networks	Large organizations, data centers, ISPs
Performance	10 – 50 devices	1000’s of devices
Routing Protocols	Basic static routing, NAT	OSPF, BGP, EIGRP, etc.
Security Features	Basic firewall, WPA2/WPA3	Advanced firewall, IPS/IDS, ACLs, VLAN, etc.

Enterprise Router

Protocols

- A protocol is a set of rules and conventions that define how devices communicate and exchange data across a network. Protocols govern everything from data formatting and transmission to routing and reception.
- Protocols are described and standardized primarily by the IETF (Internet Engineering Task Force), with contributions from organizations like IEEE, ISO, ITU, and W3C.
- Types
  - Proprietary
    - Owned by an organization and often subject to licensing restrictions.
    - Typically used in closed ecosystems or for specific vendor hardware/software.
    - Example: NETBEUI, IPX/SPX, AppleTalk.
  - Open Standard
    - Publicly available for implementation, sometimes with licensing terms.
    - Widely used in modern Internet and enterprise networking.
    - Example: TCP, IP, HTTP, FTP, etc.

Definitions

- Non-Routable Protocol
  - Lacks network addressing, so it cannot be routed between different networks—only within the same local segment.
  - Suitable for small, isolated networks.
  - Example: NETBEUI, DLC, LAT.
- Routable Protocol
  - Includes both host and network addresses, enabling data transmission across multiple networks via routers.
  - Packets are routed based on routing tables.
  - Supports scalable communication in large or wide area networks.
  - Example: IP, IPX, AppleTalk.
- Routing Protocol
  - Used by routers to build and maintain routing tables, helping determine the best path for packet delivery.
  - Example: RIP (Routing Information Protocol) , OSPF (Open Shortest Path First) , IGRP (Interior Gateway Routing Protocol – Cisco) .

Reference(s):

- https://tools.ietf.org/html/rfc1180
- https://en.wikipedia.org/wiki/List_of_RFCs

Proprietary Protocols

These protocols were developed and owned by specific companies. They are typically not openly available for public implementation and often require licensing. While once widely used, most proprietary protocols listed here are now obsolete.

NETBEUI

- NETBEUI (NetBIOS Extended User Interface) protocol is designed for LAN environments.
- Primarily used in legacy Microsoft OS (Windows 95, 98, NT).
- Non-routable, limited to local networks.
- Very fast and lightweight but not scalable.

IPX/SPX

- Internetwork Packet Exchange (Layer 3) / Sequenced Packet Exchange (Layer 4).
- Used in Novell NetWare networks and older Microsoft Windows versions.
- Routable protocol designed for large enterprise LANs.

AppleTalk

- Supports automatic addressing and routing.
- Used in Mac networks before the transition to TCP/IP.
- Routable, but now fully replaced by IP-based protocols.

Note: NETBEUI, IPX/SPX, and AppleTalk are now obsolete and included here for historical and reference purposes.

Open Standard

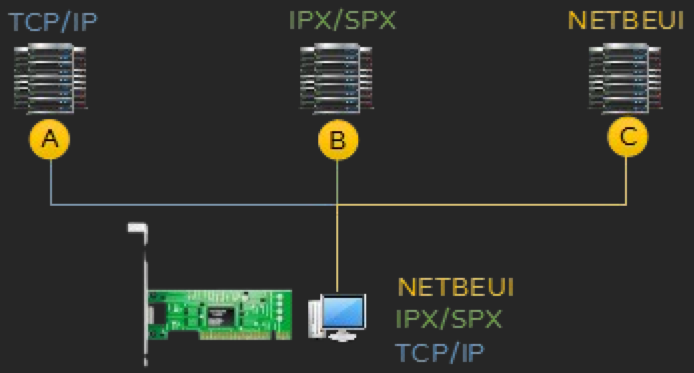
These protocols are publicly documented and available for anyone to use and implement. They promote interoperability and are widely supported across platforms and vendors.

TCP/IP

- A routable, open standard protocol suite.
- Foundation of the modern Internet and networking.
- Universally supported in modern operating systems (Windows, Linux, macOS, Android, iOS, etc.).

Protocol Binding

- Protocol binding is the process of associating a network protocol with a network adapter (such as Ethernet or Wi-Fi), enabling communication between devices over a network.
- At least one protocol must be bound to a network adapter for devices/computers to connect.
- The bound protocol can be routable (e.g., TCP/IP) or non-routable (e.g., NETBEUI).
- A single network adapter can have multiple protocols bound simultaneously, allowing communication using different protocol stacks.
- Network services (such as file sharing and printing) are bound to specific protocols, so the service works only over the protocols it is linked with.

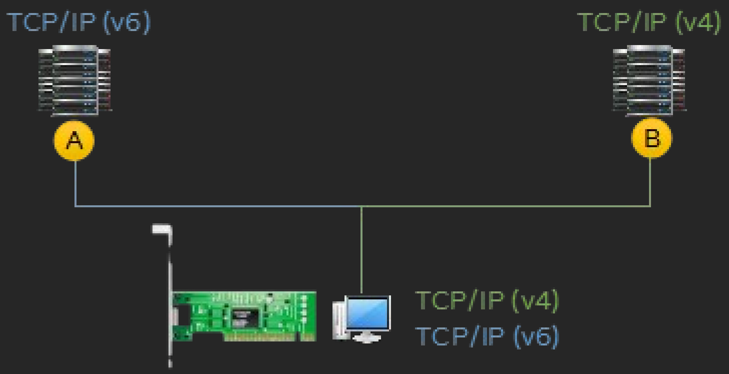


Computer with Single NIC & Multiple Protocols bound

For example:

- Client can communicate using NETBEUI protocol (Microsoft Windows 9x).
- Client can communicate using IPX/SPX protocol (Novell NetWare).
- Client can communicate using TCP/IP protocol (Unix, Linux).

Note: Most of the operating systems support TCP/IP (IPv4 & IPv6), eliminating the need for NETBEUI or IPX/SPX. Above is an example of a legacy network for understanding purposes. Internet runs on TCP/IP v4, some servers/websites support TCP/IP v6.

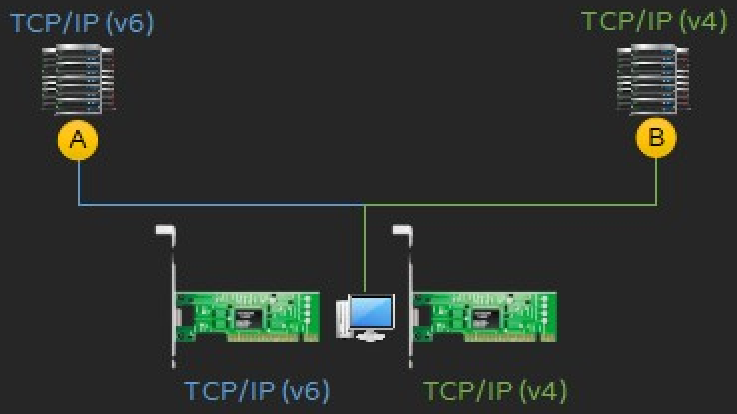


Computer with Single NIC & TCP/IP protocol versions

For example:

Computers can communicate using TCP/IP v4 or TCP/IP v6 protocol with each other, depending on the protocol installed & available on respective computers.

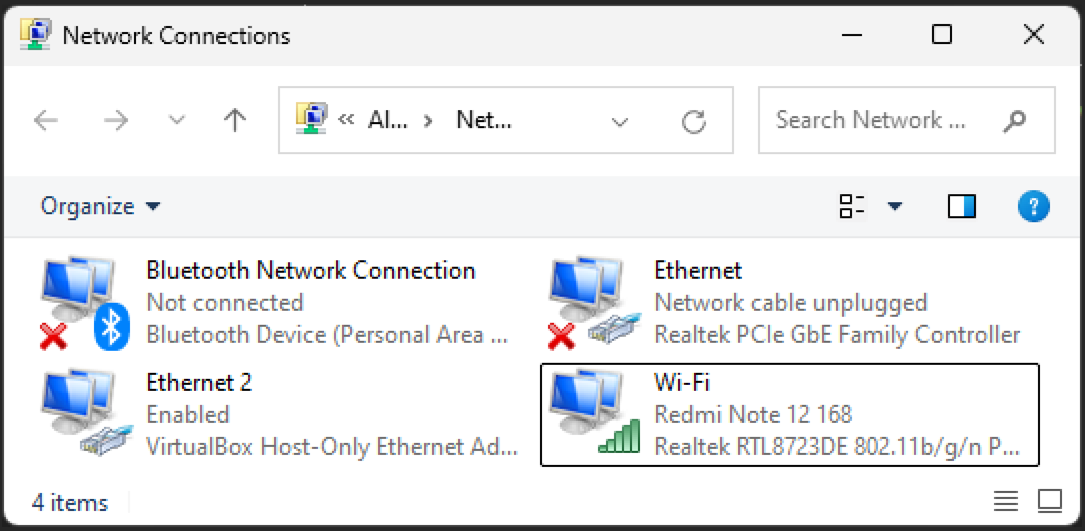
Individual protocols can be bound to separate adapters:



Computer with 2 NIC, each bound to different TCP/IP versions

To view protocol(s) bound to all NIC:

- START > NCPA.CPL
- Select available connection. For example, "Local Area Connection", "Wi-Fi", etc.



Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

Ethernet
Network cable unplugged
Realtek PCIe GbE Family Controller

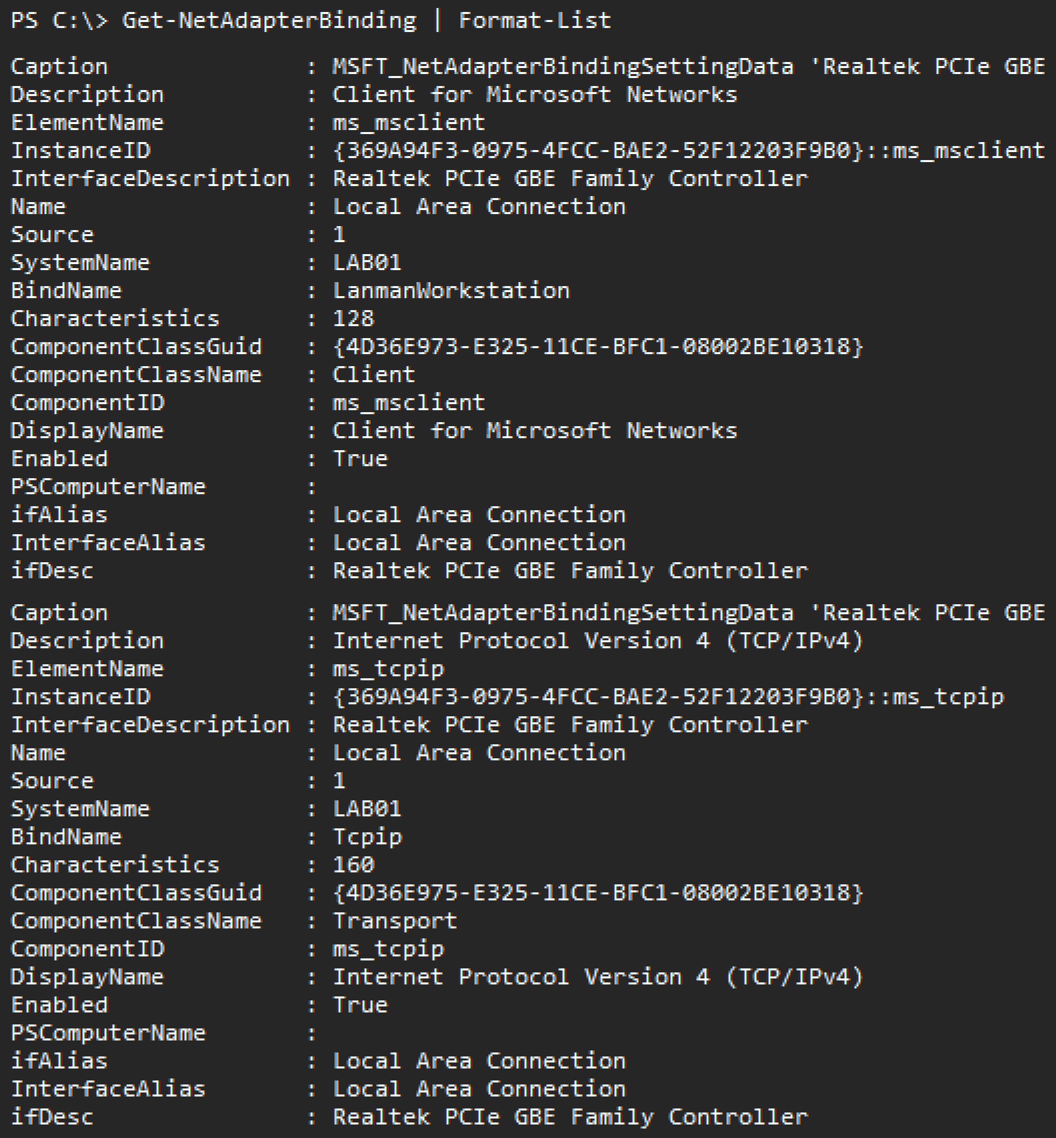
Ethernet 2
Enabled
VirtualBox Host-Only Ethernet Ad...

Wi-Fi
Redmi Note 12 168
Realtek RTL8723DE 802.11b/g/n P...

4 items

- Right-click > Select Properties.
- Observe different protocols (TCP/IP v4, etc.) & Services (Client for Microsoft Services, File and Printer Sharing for Microsoft Networks, etc.) bound to this Network Adapter.

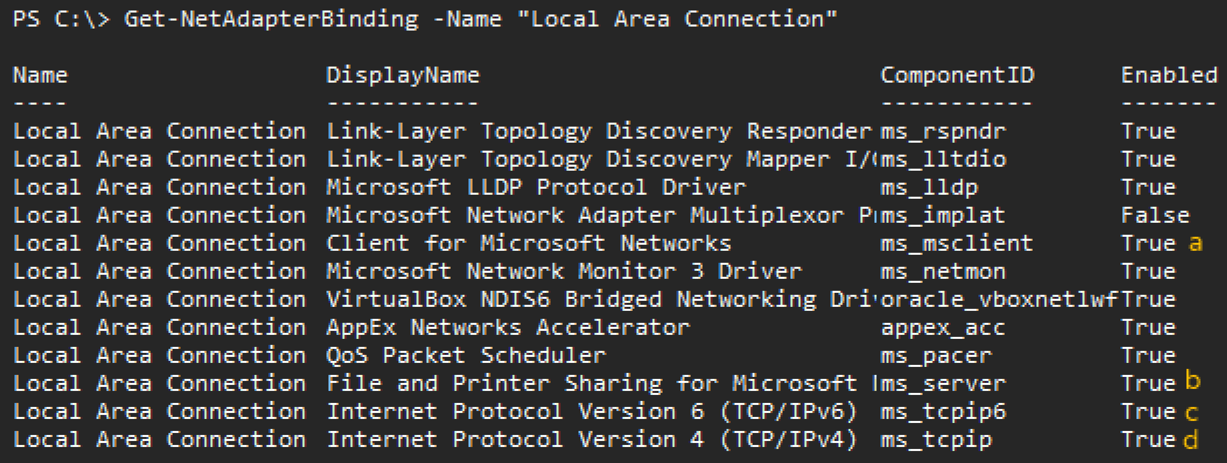
- To view protocol(s) bound to all NIC:
    - CMD > Powershell > Get-NetAdapterBinding | Format-List



```
PS C:\> Get-NetAdapterBinding | Format-List

Caption              : MSFT_NetAdapterBindingSettingData 'Realtek PCIe GBE
Description          : Client for Microsoft Networks
ElementName          : ms_msclient
InstanceID           : {369A94F3-0975-4FCC-BAE2-52F12203F9B0}::ms_msclient
InterfaceDescription : Realtek PCIe GBE Family Controller
Name                 : Local Area Connection
Source               : 1
SystemName           : LAB01
BindName             : LanmanWorkstation
Characteristics      : 128
ComponentClassGuid   : {4D36E973-E325-11CE-BFC1-08002BE10318}
ComponentClassName   : Client
ComponentID          : ms_msclient
DisplayName          : Client for Microsoft Networks
Enabled              : True
PSComputerName       :
ifAlias              : Local Area Connection
InterfaceAlias       : Local Area Connection
ifDesc               : Realtek PCIe GBE Family Controller

Caption              : MSFT_NetAdapterBindingSettingData 'Realtek PCIe GBE
Description          : Internet Protocol Version 4 (TCP/IPv4)
ElementName          : ms_tcpip
InstanceID           : {369A94F3-0975-4FCC-BAE2-52F12203F9B0}::ms_tcpip
InterfaceDescription : Realtek PCIe GBE Family Controller
Name                 : Local Area Connection
Source               : 1
SystemName           : LAB01
BindName             : Tcpip
Characteristics      : 160
ComponentClassGuid   : {4D36E975-E325-11CE-BFC1-08002BE10318}
ComponentClassName   : Transport
ComponentID          : ms_tcpip
DisplayName          : Internet Protocol Version 4 (TCP/IPv4)
Enabled              : True
PSComputerName       :
ifAlias              : Local Area Connection
InterfaceAlias       : Local Area Connection
ifDesc               : Realtek PCIe GBE Family Controller
```

Output listing protocols & services bound to all adapters

- To view protocol(s) bound to a particular NIC:
    - CMD > Powershell > Get-NetAdapterBinding - Name “CONNECTIONNAME” | Format-List



```
PS C:\> Get-NetAdapterBinding -Name "Local Area Connection"

Name                  DisplayName                               ComponentID      Enabled
----                  -----------                               -----------      -------
Local Area Connection Link-Layer Topology Discovery Responder ms_rspndr        True
Local Area Connection Link-Layer Topology Discovery Mapper I/(ms_lltdio        True
Local Area Connection Microsoft LLDP Protocol Driver            ms_lldp          True
Local Area Connection Microsoft Network Adapter Multiplexor P ms_implat        False
Local Area Connection Client for Microsoft Networks             ms_msclient      True a
Local Area Connection Microsoft Network Monitor 3 Driver        ms_netmon        True
Local Area Connection VirtualBox NDIS6 Bridged Networking Dri oracle_vboxnetlwfTrue
Local Area Connection AppEx Networks Accelerator                appex_acc        True
Local Area Connection QoS Packet Scheduler                      ms_pacer         True
Local Area Connection File and Printer Sharing for Microsoft I ms_server        True b
Local Area Connection Internet Protocol Version 6 (TCP/IPv6)    ms_tcpip6        True c
Local Area Connection Internet Protocol Version 4 (TCP/IPv4)    ms_tcpip         True d
```

Output listing protocols & services bound to a specific adapter - d) TCP/IPv4, C)TCP/IPv6, b) File and Printer sharing for Microsoft Networks, a) Client for Microsoft Networks and others

- TCP/IPv4 is a protocol stack required for IPv4 connections.
- TCP/IPv6 is a protocol stack required for IPv6 connections.
- File and Printer sharing for Microsoft Networks is a service required for sharing folders, printers and other resources (Microsoft Networks & Microsoft Compatible Networks).
- Client for Microsoft Networks is a service required for accessing resources available on remote computers (Microsoft Networks & Microsoft Compatible Networks).

In simple terms:

A. Client for Microsoft Networks Service is bound to TCP/IPv4 & TCP/IPv6.
B. File and Printer Sharing Service is bound to TCP/IPv4 & TCP/IPv6.
C. & D. TCP/IPv4 & TCP/IPv6 is bound to Local Area Connection (which refers to one NIC).

Note: There are many protocols & services bound as per example, not covered here.

IP

- Internet Protocol is a Layer 3 (Network Layer) protocol in the OSI model responsible for logical addressing and routing of data across networks.
- Connectionless protocol — it does not establish a dedicated connection before sending data.
- Provides logical addressing and routing.
- Offers best-effort delivery — does not guarantee delivery, order, or prevention of duplicates.
- Error checking, sequencing, and retransmission are handled by higher-level protocols like TCP or by applications.
- Variants
  - IPv4 (IP Version 4)
  - IPv6 (IP Version 6)

IPv4

- Fourth major version and first widely used version of IP.
- Uses 32-bit addressing Scheme, 4,294,967,296 (2^{32}) possible addresses.
- Has two parts - Network ID (identifies Network segment) and Host ID (identifies a host on that network). Subnet Mask is used to distinguish between Network and Host portions of the address.
- IP Address assignments can be Classful or Classless.

Classful

- Based on fixed boundaries.
- Divided into Classes A, B, C, D, E.
- Largely deprecated in favor of classless addressing.

Classless

- Uses variable-length subnet masks (VLSM).
- Example: `192.168.1.0/24` (where `/24` specifies the number of network bits).
- More efficient IP address allocation, supports better routing aggregation.

Public IP

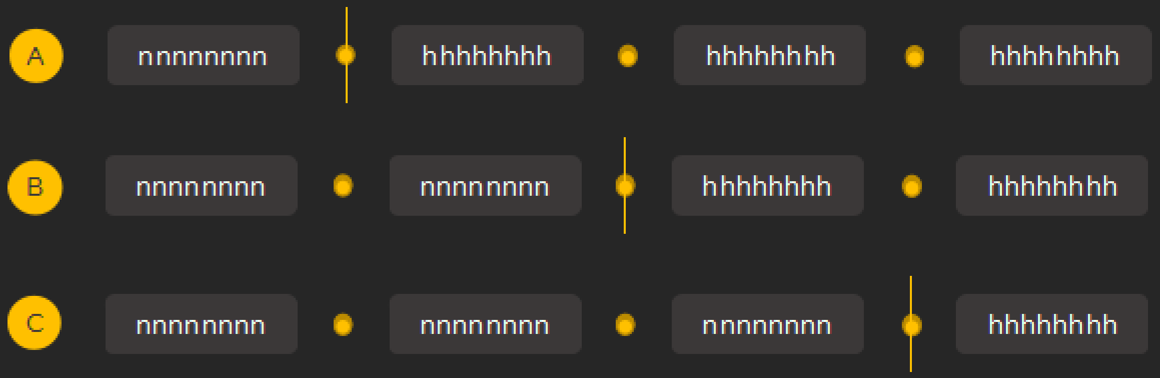
- Globally unique and cannot be duplicated.
- Required for communication over the Internet (public network).
- Managed by IANA (Internet Assigned Numbers Authority), a department of ICANN (Internet Corporation for Assigned Names and Numbers).
- IANA allocates IP blocks to RIRs (Regional Internet Registries) such as ARIN, RIPE, APNIC, etc.
- Public IP addresses are assigned by Internet Service Providers to users / organizations.

Private IP

- Reserved for use within private networks (LANs), such as home and office networks.
- Not routable on the public Internet.
- Managed internally by network administrators.

Note: Devices assigned private IP addresses cannot communicate directly with devices using public IP addresses and vice versa. NAT (Network Address Translation) is required to enable communication between them.

Classful Networks is an addressing scheme introduced in 1981, address space divided into 5 classes:



IP Address Class A, B & C - Network & Host Portions

- Class A
  - First bit set to “0”, leaving the range from 0.0.0.0 to 127.255.255.255 for network ID.
  - Number of Networks: 2^7 - 2 = 126.
  - Number of Hosts Per Network: 2^{24} - 2 = 16,777,214.
  - 127.x.x.x reserved for loopback purposes.
  - Default Subnet Mask: 255.0.0.0 .
  - Private IP Address range: 10.0.0.0 – 10.255.255.255
- Class B
  - First bit set to “10”, leaving the range from 128.0.0.0 to 191.255.255.255 for network ID
  - Number of Networks: 2^{14} = 16,384
  - Number of Hosts Per Network: 2^{16} - 2 = 65,534
  - Default Subnet Mask: 255.255.0.0
  - Private IP Address range: 172.16.0.0 – 172.31.255.255
- Class C
  - First bit set to “110”, leaving the range from 192.0.0.0 to 223.255.255.255 for network ID
  - Number of Networks: 2^{21} = 2,097,152
  - Number of Hosts Per Network: 2^8 -2 = 254
  - Default Subnet Mask: 255.255.255.0
  - Private IP Address range: 192.168.0.0 – 192.168.255.255
- Class D
  - First bit set to “1110”, leaving the range from 224.0.0.0 to 239.255.255.255 for network ID
  - Reserved for multicast, cannot be used
- Class E
  - First bit set to “1111”, leaving the range from 240.0.0.0 to 255.255.255.255 for network ID
  - Reserved, cannot be used

Note: Cannot use all zeros or ones (binary) for host/network ID.

Special IP addresses:

- These are reserved IP addresses with specific functions, not used for normal host-to-host communication on the Internet.
- 255.255.255.255 - Used for broadcasting, particularly DHCP clients.
- 169.254.x.x - Reserved for APIPA. Automatically assigned when a device fails to obtain an IP address from a DHCP server. Enables basic communication within the same subnet, often used in home or small networks. Only local communication; no Internet access.

Note: Understanding IP addressing may take time, additional tutorials may be explored.

CIDR (Classless Inter-Domain Routing)

- Replacement for classful method of allocating IP addresses and routing.
- Uses variable-length subnet masking (VLSM) to allocate IP addresses more efficiently.
- Network & Host ID determined based on Subnet Mask as assigned by an admin.
- Enables more efficient IP address management and reduces the size of routing tables by aggregating routes (route summarization).

To understand, imagine a network with 10 computers:

If Classful method is used, then for:

IP address range: 10.x.x.x
Default Subnet Mask: 255.0.0.0
# of IP addresses available: 16,777,214
If # of IP hosts or computers = 10
Wastage: 16,777,214 - 10 = 16,777,204

In case of CIDR, VLSM applied:

IP address range: 10.x.x.x
If Subnet Mask (VLSM) = 255.255.255.0
# of IP addresses available: 254
Wastage: 254 - 10 = 244

Note:

- The number of usable IP addresses subtracts 2 for network and broadcast addresses, which you implicitly accounted for.
- CIDR notation is often written as `/N` where N is the number of network bits (e.g., /24).
- CIDR also helps route aggregation, which reduces the size of global routing tables, a key benefit beyond just IP allocation efficiency.

Converting Binary to Decimal, Simple Method

Factor	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value	128	64	32	16	8	4	2	1

Reference: Power Factor & Value

- If True, then carry forward the actual value
- If False, then leave the value (Write as “0”)

Binary	1	1	1	1	1	1	1	1
Decimal	128	64	32	16	8	4	2	1

Boolean	T	T	T	T	T	T	T	T
Result	128	64	32	16	8	4	2	1
Total	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255							

Example 01: All bits = 1

Binary	0	0	0	0	0	0	0	0
Decimal	128	64	32	16	8	4	2	1

Boolean	F	F	F	F	F	F	F	F
Result	0	0	0	0	0	0	0	0
Total	0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0							

Example 02: All bits = 0

Binary	0	0	0	0	1	0	1	0
Decimal	128	64	32	16	8	4	2	1

Boolean	F	F	F	F	T	F	T	F
Result	0	0	0	0	8	0	2	0
Total	0 + 0 + 0 + 0 + 8 + 0 + 2 + 0 = 10							

Example 03: Selective bits = 1

Example to understand Network & Host portions of an IP Address

Computer A
IP address: 10.1.1.1
Subnet Mask: 255.0.0.0

	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
IP	10	1	1	1
Subnet Mask	255	0	0	0
IP Decimal	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1
Subnet Mask Decimal	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	10	0	0	0
Host ID	0	1	1	1

Computer B
IP address: 10.1.1.2
Subnet Mask: 255.0.0.0

	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
IP	10	1	1	2
Subnet Mask	255	0	0	0
IP Decimal	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1	0 0 0 0 0 0 1 0
Subnet Mask Decimal	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	10	0	0	0
Host ID	0	1	1	2

Computer C
IP address: 11.1.1.1
Subnet Mask: 255.0.0.0

	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
IP	11	1	1	1
Subnet Mask	255	0	0	0
IP Decimal	0 0 0 0 1 0 1 1	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1
Subnet Mask Decimal	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	0 0 0 0 1 0 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Network ID	11	0	0	0
Host ID	0	1	1	1

	Network ID	Host ID
Computer A	10	1.1.1
Computer B	10	1.1.2
Computer C	11	1.1.1

In above example, network ID’s for computer A & B is 10 indicating they are on same logical network; computer c is on a different logical network hence require IP routing to communicate with computer A and/or B.

Worksheet

A: Convert Binary to Decimal

Octet 1	Octet 2	Octet 3	Octet 4	IP
00001010	00000000	00000000	00000000	10.0.0.0
00001010	00000000	00000000	00000001	10.0.0.1
10001000	00000000	00000000	00001000	
01010101	10001000	00100000	00001001	
11001100	00110011	00111100	00001100	

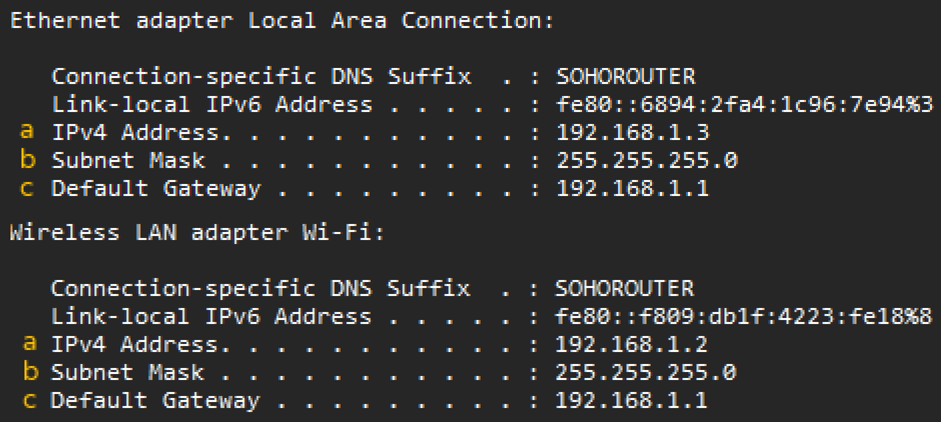
B. Convert Decimal to Binary

IP	Octet 1	Octet 2	Octet 3	Octet 4
10.0.0.1	00001010	00000000	00000000	00000001
202.64.32.8				
12.4.8.16				
192.168.1.1				
222.22.2.22				

C. Identify Network & Host ID for IP addresses

IP address	Subnet Mask	Network ID	Host ID
10.1.5.1	255.0.0.0		
10.6.1.5	255.0.0.0		
10.10.10.5	255.255.0.0		
10.10.11.6	255.255.0.0		

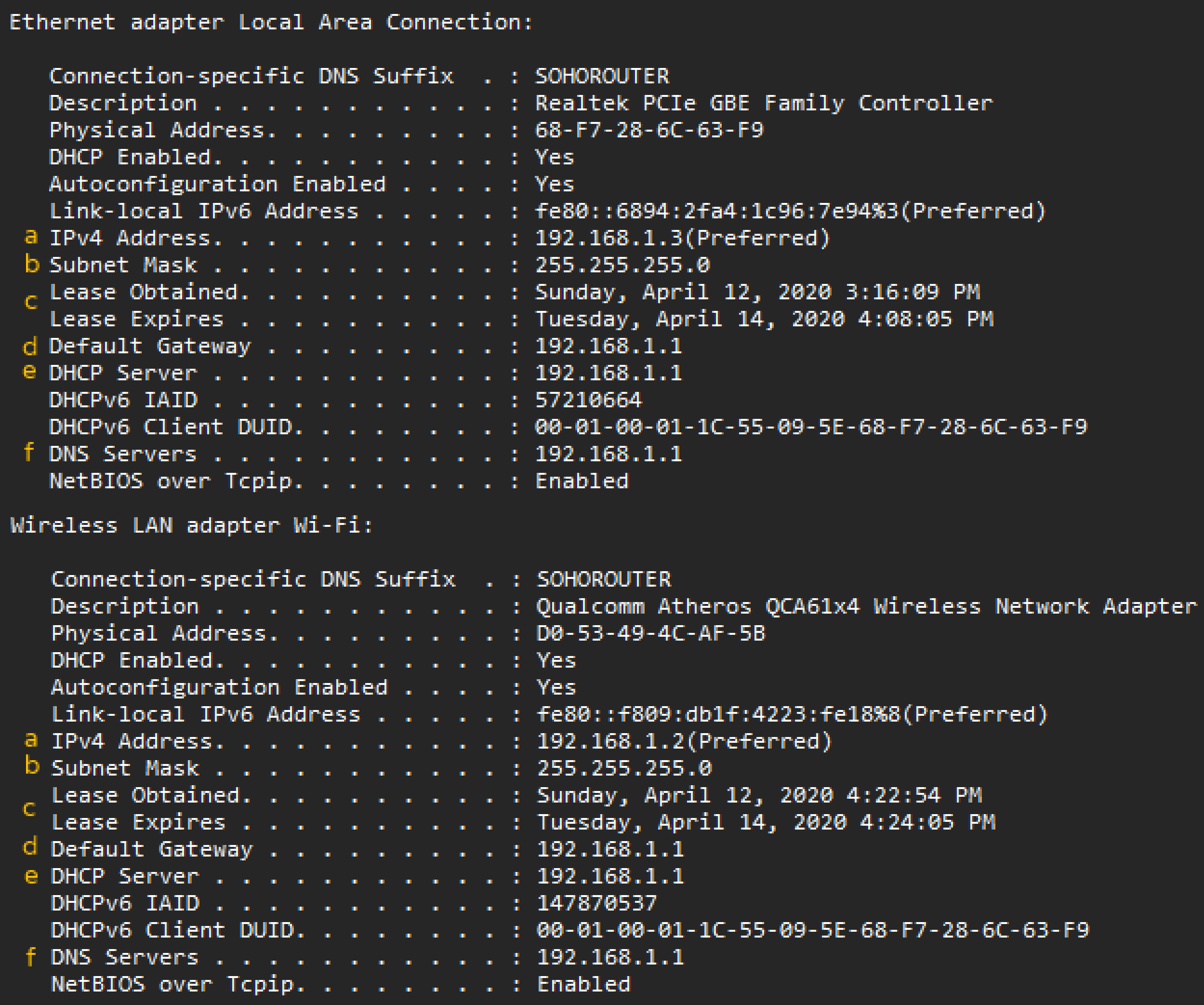
- View all IP Addresses:
  - CMD > ipconfig



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3
 a IPv4 Address. . . . . . . . . . . : 192.168.1.3
 b Subnet Mask . . . . . . . . . . . : 255.255.255.0
 c Default Gateway . . . . . . . . . : 192.168.1.1

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Link-local IPv6 Address . . . . . : fe80::f809:db1f:4223:fe18%8
 a IPv4 Address. . . . . . . . . . . : 192.168.1.2
 b Subnet Mask . . . . . . . . . . . : 255.255.255.0
 c Default Gateway . . . . . . . . . : 192.168.1.1
```

Output listing a) IPv4 Address, b)Subnet Mask & c) Default Gateway

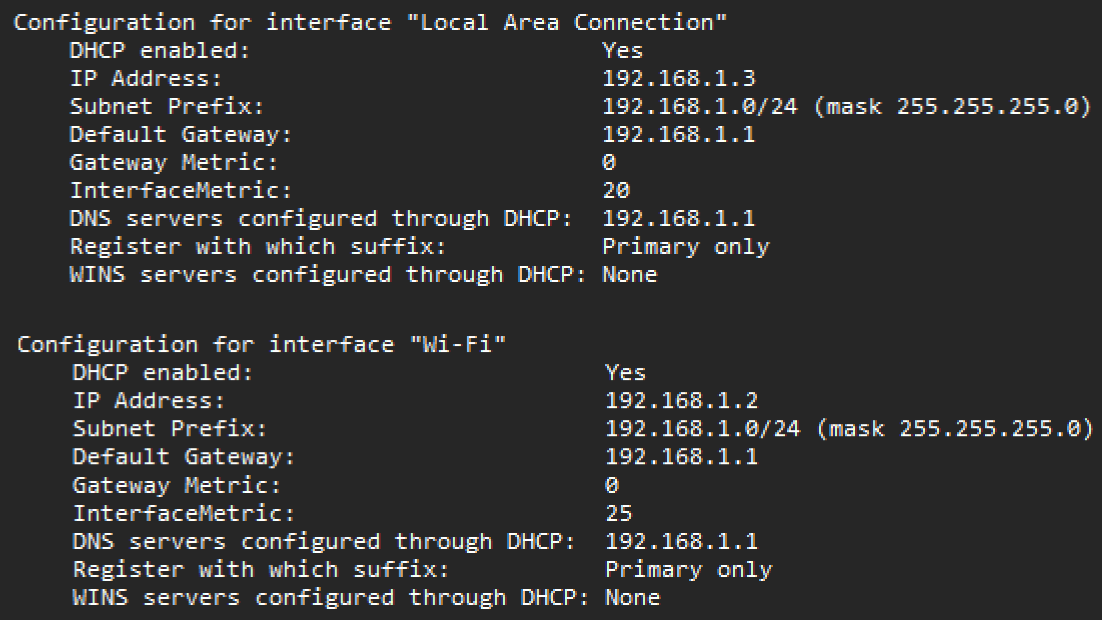
- View all IP Addresses (all details):
    - CMD > ipconfig /all



```
Ethernet adapter Local Area Connection:

     Connection-specific DNS Suffix  . : SOHOROUTER
     Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
     Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
     DHCP Enabled. . . . . . . . . . . : Yes
     Autoconfiguration Enabled . . . . : Yes
     Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   a IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   b Subnet Mask . . . . . . . . . . . : 255.255.255.0
   c Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 3:16:09 PM
     Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 4:08:05 PM
   d Default Gateway . . . . . . . . . : 192.168.1.1
   e DHCP Server . . . . . . . . . . . : 192.168.1.1
     DHCPv6 IAID . . . . . . . . . . . : 57210664
     DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   f DNS Servers . . . . . . . . . . . : 192.168.1.1
     NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

     Connection-specific DNS Suffix  . : SOHOROUTER
     Description . . . . . . . . . . . : Qualcomm Atheros QCA61x4 Wireless Network Adapter
     Physical Address. . . . . . . . . : D0-53-49-4C-AF-5B
     DHCP Enabled. . . . . . . . . . . : Yes
     Autoconfiguration Enabled . . . . : Yes
     Link-local IPv6 Address . . . . . : fe80::f809:db1f:4223:fe18%8(Preferred)
   a IPv4 Address. . . . . . . . . . . : 192.168.1.2(Preferred)
   b Subnet Mask . . . . . . . . . . . : 255.255.255.0
   c Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 4:22:54 PM
     Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 4:24:05 PM
   d Default Gateway . . . . . . . . . : 192.168.1.1
   e DHCP Server . . . . . . . . . . . : 192.168.1.1
     DHCPv6 IAID . . . . . . . . . . . : 147870537
     DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   f DNS Servers . . . . . . . . . . . : 192.168.1.1
     NetBIOS over Tcpip. . . . . . . . : Enabled
```

Output listed a) IPv4 Address assigned by the DHCP server, b) Subnet Mask, c) Lease details, d) Gateway's IP, e) DHCP Server's IP address & f) DNS Server's IP address

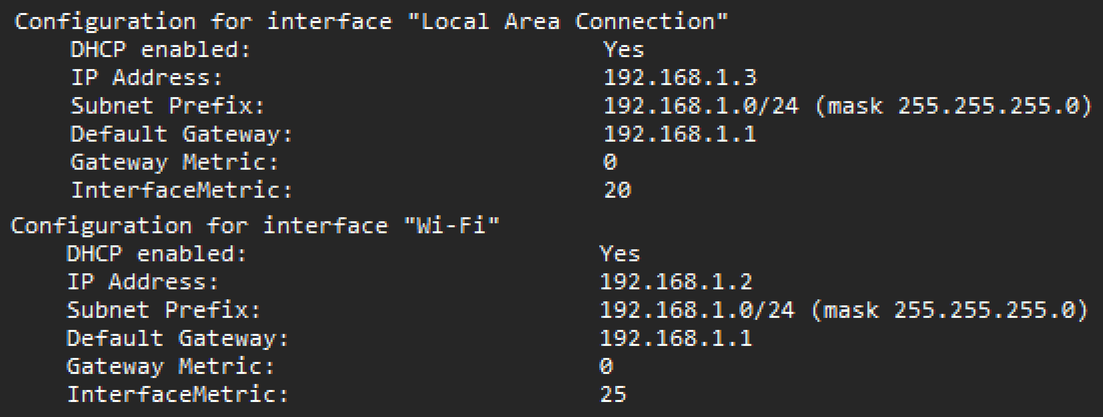
- View IP addresses for all connections:
  - CMD > netsh interface ip show config



```
Configuration for interface "Local Area Connection"
    DHCP enabled:                         Yes
    IP Address:                           192.168.1.3
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.1.1
    Gateway Metric:                       0
    InterfaceMetric:                      20
    DNS servers configured through DHCP:  192.168.1.1
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None

Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.1.2
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.1.1
    Gateway Metric:                       0
    InterfaceMetric:                      25
    DNS servers configured through DHCP:  192.168.1.1
    Register with which suffix:           Primary only
    WINS servers configured through DHCP: None
```

Output listed using NETSH

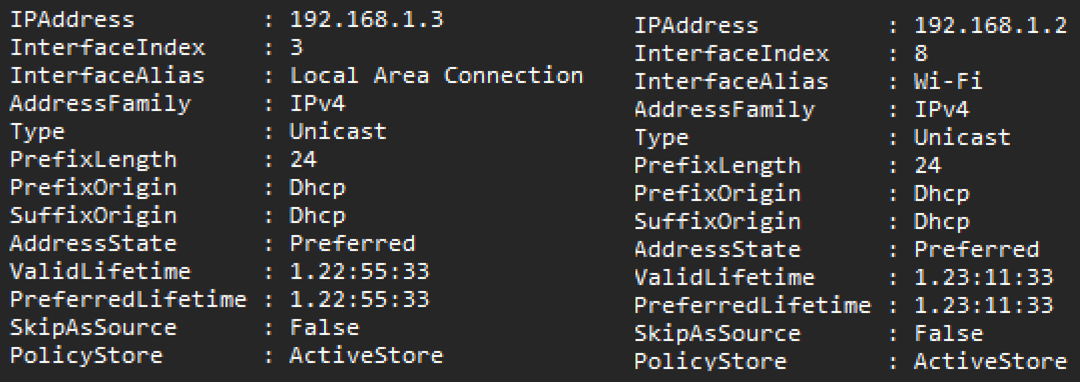
  - CMD > netsh interface ipv4 show addresses



```
Configuration for interface "Local Area Connection"
    DHCP enabled:                         Yes
    IP Address:                           192.168.1.3
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.1.1
    Gateway Metric:                       0
    InterfaceMetric:                      20
Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           192.168.1.2
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:                      192.168.1.1
    Gateway Metric:                       0
    InterfaceMetric:                      25
```

Output listing IPv4 addresses

- View IPv4 addresses:
    - CMD > Powershell > Get-NetIPAddress -AddressFamily IPv4

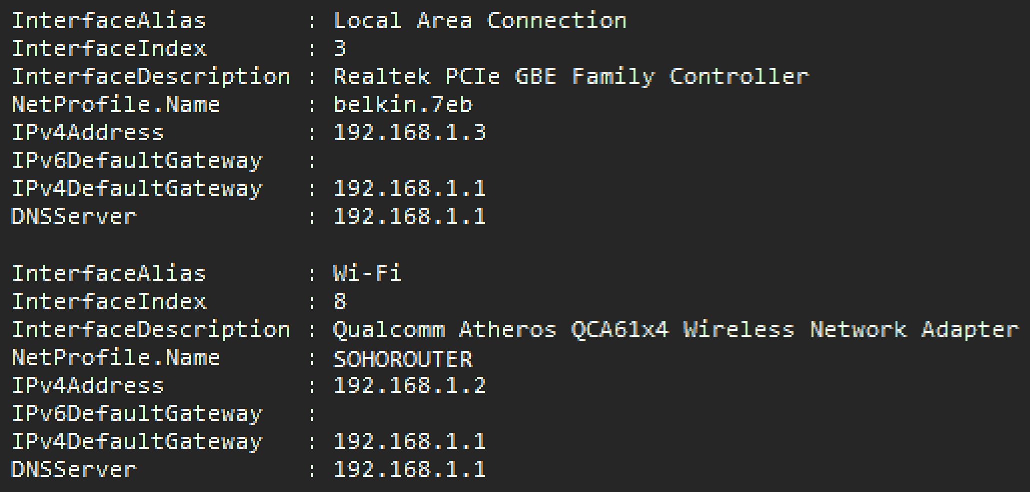


```
IPAddress         : 192.168.1.3
InterfaceIndex    : 3
InterfaceAlias    : Local Area Connection
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Dhcp
SuffixOrigin      : Dhcp
AddressState      : Preferred
ValidLifetime     : 1.22:55:33
PreferredLifetime : 1.22:55:33
SkipAsSource      : False
PolicyStore       : ActiveStore
```

```
IPAddress         : 192.168.1.2
InterfaceIndex    : 8
InterfaceAlias    : Wi-Fi
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Dhcp
SuffixOrigin      : Dhcp
AddressState      : Preferred
ValidLifetime     : 1.23:11:33
PreferredLifetime : 1.23:11:33
SkipAsSource      : False
PolicyStore       : ActiveStore
```

Output listing IPv4 Addresses for Wired (Left) & Wireless (Right) Connections

- View network configuration, including usable interfaces, IP addresses, and DNS servers:
    - CMD > Powershell > Get-NetIPConfiguration -All

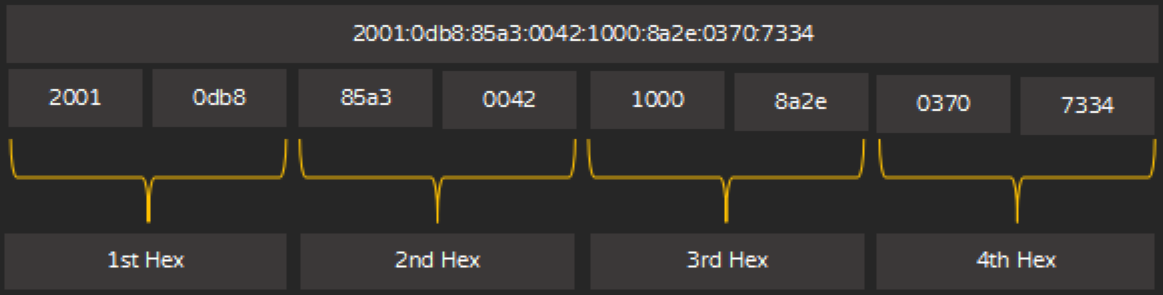


```
InterfaceAlias       : Local Area Connection
InterfaceIndex       : 3
InterfaceDescription : Realtek PCIe GBE Family Controller
NetProfile.Name      : belkin.7eb
IPv4Address          : 192.168.1.3
IPv6DefaultGateway   :
IPv4DefaultGateway   : 192.168.1.1
DNSServer            : 192.168.1.1

InterfaceAlias       : Wi-Fi
InterfaceIndex       : 8
InterfaceDescription : Qualcomm Atheros QCA61x4 Wireless Network Adapter
NetProfile.Name      : SOHOROUTER
IPv4Address          : 192.168.1.2
IPv6DefaultGateway   :
IPv4DefaultGateway   : 192.168.1.1
DNSServer            : 192.168.1.1
```

Output listing network configuration, including usable interfaces, IP addresses, and DNS servers

IPv6

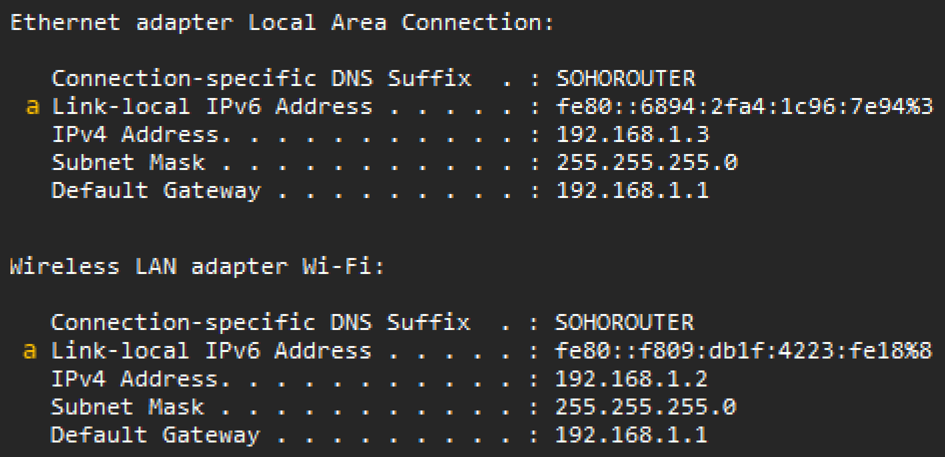
- Most recent version of the Internet Protocol.
- Designed to replace IPv4 due to IPv4 address exhaustion.
- Uses a 128-bit addressing scheme.
- 2^{128}, or approximately 3.4×10^{38} addresses.
- IPv6 hosts can configure themselves automatically using Stateless Address Autoconfiguration (SLAAC) or via DHCPv6.
- IPv6 addresses are represented as eight groups of four hexadecimal digits, separated by colons.
- Example address: `2001:0db8:85a3:0042:1000:8a2e:0370:7334`
- Leading zeros in each group can be omitted, and consecutive groups of zeros can be compressed with `::` once per address.



IPv6: Address in 8 groups and 4 hexadecimal values

Note: IPv6 is bit complex for beginners, not covered here.

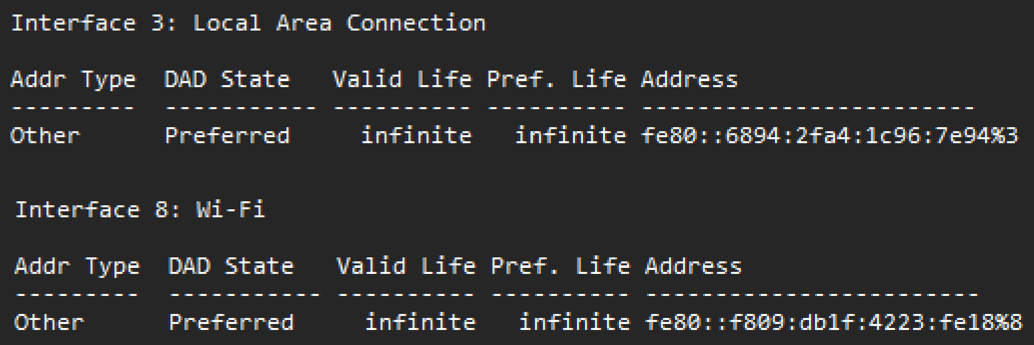
- View IP address:
  - CMD > ipconfig /all



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
 a Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1


Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : SOHOROUTER
 a Link-local IPv6 Address . . . . . : fe80::f809:db1f:4223:fe18%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Output listing IPv6 Address

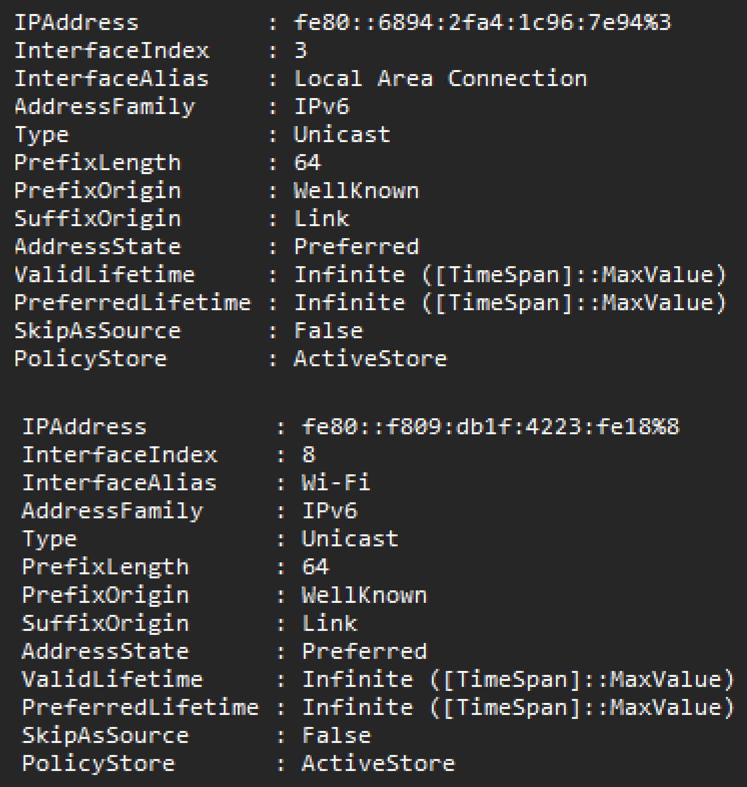
- View only IPv6 Addresses:
  - CMD > netsh interface ipv6 show addresses



```
Interface 3: Local Area Connection

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Preferred     infinite   infinite fe80::6894:2fa4:1c96:7e94%3

Interface 8: Wi-Fi

Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Other      Preferred     infinite   infinite fe80::f809:db1f:4223:fe18%8
```

Output listing IPv6 Addresses

- View IPv6 Addresses:
  - CMD > Powershell > Get-NetIPAddress -AddressFamily IPv6



```
IPAddress         : fe80::6894:2fa4:1c96:7e94%3
InterfaceIndex    : 3
InterfaceAlias    : Local Area Connection
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : fe80::f809:db1f:4223:fe18%8
InterfaceIndex    : 8
InterfaceAlias    : Wi-Fi
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore
```

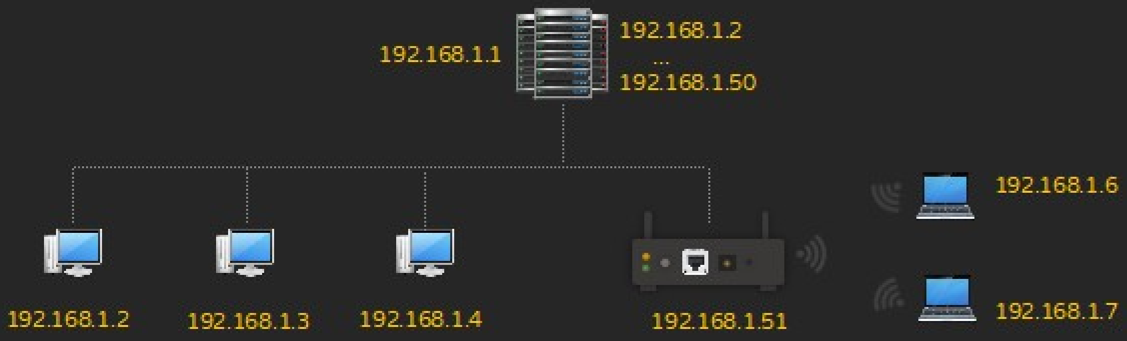
Output listing IPv6 Addresses

DHCP

Devices on a IP network require unique IP address. IP addresses are assigned manually (Static) or automated using DHCP service (Dynamic) by an administrator; assigning IP addresses manually to each computer in a medium or large network is tedious (and increases chances of duplicates due to human error), and using DHCP service is the preferred method as it reduces administrative efforts. Network configuration details such as addresses of DNS servers, IP Gateway, etc. can be pushed along to IP clients.

DHCP is widely used in almost every home & office network. DHCP is also used in places that require temporary connectivity such as hotspots (IP addresses are reassigned to different clients time-to-time).

- Dynamic Host Configuration Protocol, automates IP address assignments.
- DHCP Service is usually included in Wi-Fi/Home Routers, Server Operating Systems, Enterprise Routers & Layer 3 Switches but require specific technical expertise to configure depending on the product. DHCP service is mostly automated on devices designed for home use, requiring no administrative effort or technical expertise.
- Connection-less, UDP Ports 67 & 68.
- IP addresses are “leased” for a particular duration (like 2 hour or 2 days) as set by the administrator. IP assigned through DHCP are renewed once the lease expires. There are no guarantees that a DHCP client will receive the same IP as before during renewals (except if it is reserved through a specific mechanism). Lease duration may be adjusted depending on business cases; for example, shorter lease duration like 60 minutes can be set for hot-spots or guest networks at office/home.

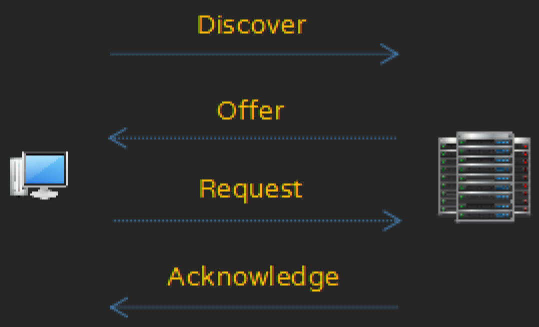


DHCP Server (service) 192.168.2.1, allocating IP address to wired and wireless clients from the DHCP range 192.168.1.2 to 192.168.1.254

In above scenario:

A. DHCP Server is assigned the IP 192.168.2.1.
B. DHCP range is configured to assign 192.168.2.2 to 192.168.2.50 for its clients.
C. Wired clients receive IP address from DHCP server.
D. Wireless AP is assigned with static IP 192.168.2.51.
E. Wireless clients receive IP address from DHCP Server through the Wireless Access Point.

DHCP Process (DORA)



1. DHCP**D**ISCOVER - Client broadcasts, requesting for IP.
2. DHCP**O**FFER - DHCP Server(s) responds with IP.
3. DHCP**R**EQUEST - DHCP client replies to DHCP server that has sent first (if there are multiple DHCP Servers).
4. DHCP**A**CK - DHCP Server sends acknowledgment to DHCP client, based on its selection.

Link-Local Address

If there are NO IP address assigned (static or dynamic), modern operating systems self-assign an IP address in the range of 169.254.x.x (Subnet mask set as 255.255.0.0) automatically. This facility is designed as a fallback mechanism for devices to self-assign non-conflicting IP address automatically in order to communicate with each other.

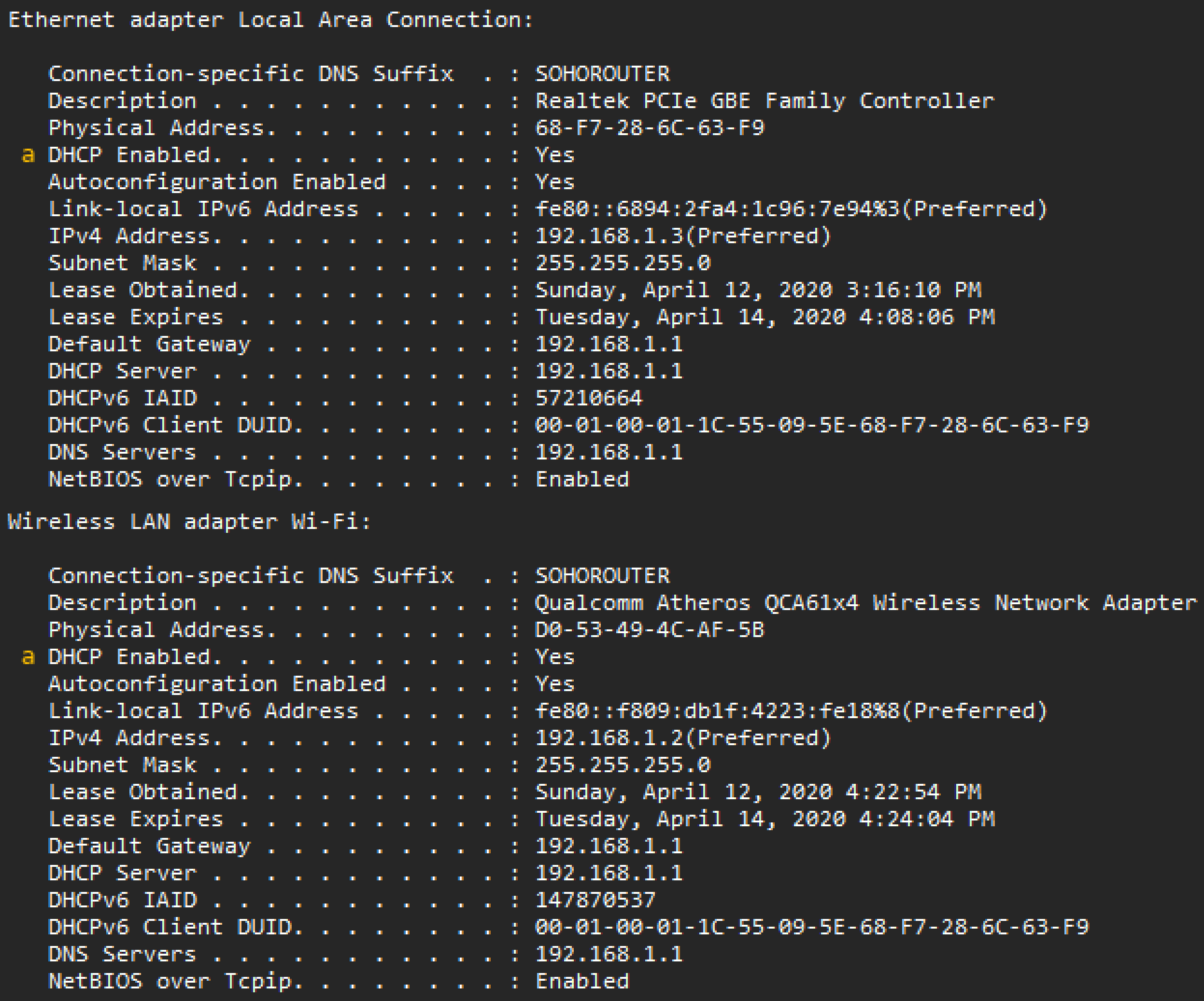
- Reserved IP range: 169.254.0.0 – 169.254.255.255.
- Also referred to as “Auto-IP” or “APIPA”.
- Range can also be manually assigned by the administrator.

For example:

1. DHCP is set to assign 192.168.1.1 to 192.168.1.254.
2. DHCP server fails to issue IP addresses to its clients.
3. DHCP clients self-assign non-conflicting unique IP addresses automatically (DHCP Client 1 may self-assign 169.254.1.12, DHCP Client 2 may self-assign 169.254.3.30 and so on).
4. DHCP clients can communicate with each other (but may not browse the Internet, etc.)

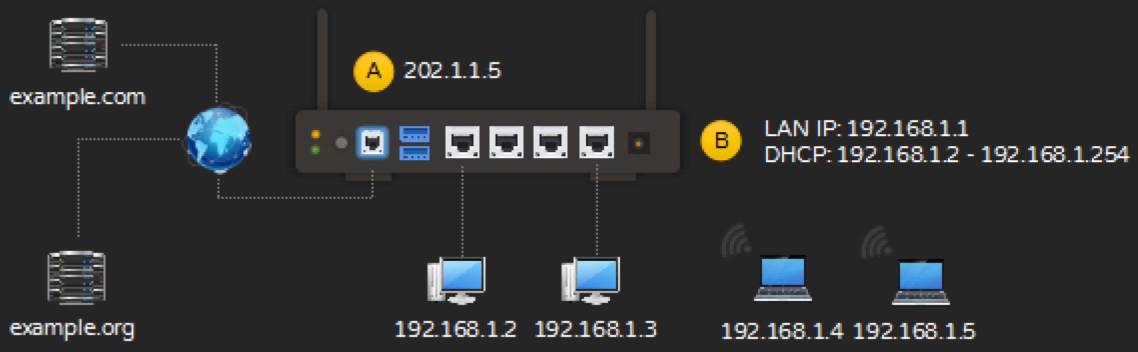
Note: APIPA (Automatic Private IP Addressing) is a term used in Microsoft Windows.

- Check if a computer is configured as a DHCP Client
  - CMD > ipconfig /all Check status: DHCP Enabled: Yes (Indicates its a DHCP client)



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
 a DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 3:16:10 PM
   Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 4:08:06 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Description . . . . . . . . . . . : Qualcomm Atheros QCA61x4 Wireless Network Adapter
   Physical Address. . . . . . . . . : D0-53-49-4C-AF-5B
 a DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f809:db1f:4223:fe18%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 4:22:54 PM
   Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 4:24:04 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 147870537
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Output listing a) DHCP status

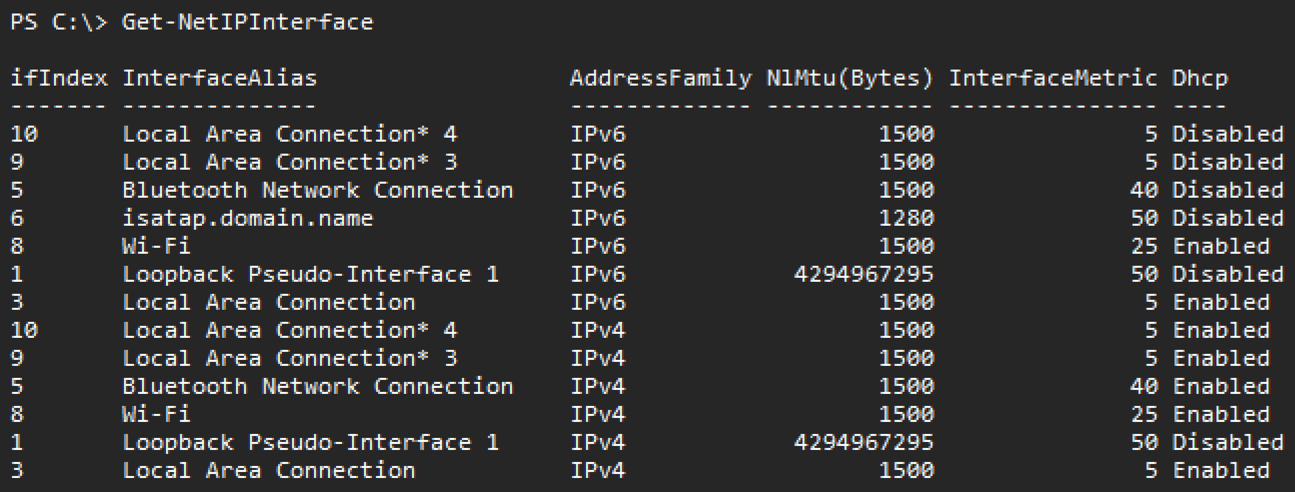


Example

a. IPv4 address: IP address assigned by the DHCP Server (from DHCP pool 192.168.1.1 to 192.168.1.254).
b. Subnet Mask: Subnet Mask assigned by the DHCP Server.
c. DHCP Lease:
   a) Lease Obtained: Start date & time as set on DHCP Server.
   b) Lease Expires: End date & time as set on DHCP Server.
d. Default Gateway: IP through which packets to be routed, if the host is on an external network. To communicate with example.com or example.org, 192.168.1.2 will send the packet to 192.168.1.1 which in turn is sent to external host/network.
e. DHCP Server: IP address of the DHCP Server.
f. DNS Server: IP address of the DNS server. To resolve example.com's IP address, 192.168.1.2 will send name resolution request to 192.168.1.1; 192.168.1.1 will process the request (internal cache or external DNS) and reply to 192.168.1.2.

Note: IP address range, Subnet Mask, DHCP Lease duration & DNS Server values can be set on a DHCP Server or any device such as a SOHO Router that supports DHCP Service.

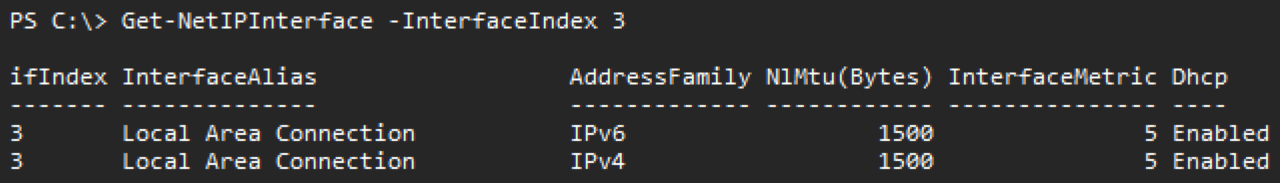
- To check if DHCP is enabled or disabled
  - CMD > Powershell > Get-NetIPInterface



```
PS C:\> Get-NetIPInterface

ifIndex InterfaceAlias                  AddressFamily NlMtu(Bytes) InterfaceMetric Dhcp
------- --------------                  ------------- ------------ --------------- ----
10      Local Area Connection* 4        IPv6                  1500               5 Disabled
9       Local Area Connection* 3        IPv6                  1500               5 Disabled
5       Bluetooth Network Connection    IPv6                  1500              40 Disabled
6       isatap.domain.name              IPv6                  1280              50 Disabled
8       Wi-Fi                           IPv6                  1500              25 Enabled
1       Loopback Pseudo-Interface 1     IPv6            4294967295              50 Disabled
3       Local Area Connection           IPv6                  1500               5 Enabled
10      Local Area Connection* 4        IPv4                  1500               5 Enabled
9       Local Area Connection* 3        IPv4                  1500               5 Enabled
5       Bluetooth Network Connection    IPv4                  1500              40 Enabled
8       Wi-Fi                           IPv4                  1500              25 Enabled
1       Loopback Pseudo-Interface 1     IPv4            4294967295              50 Disabled
3       Local Area Connection           IPv4                  1500               5 Enabled
```

Output listing DHCP Status (last column)

- To check DHCP status for a particular adapter
  - CMD > Powershell > Get-NetIPInterface -InterfaceIndex IFINDEX#

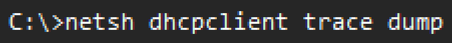


```
PS C:\> Get-NetIPInterface -InterfaceIndex 3

ifIndex InterfaceAlias                  AddressFamily NlMtu(Bytes) InterfaceMetric Dhcp
------- --------------                  ------------- ------------ --------------- ----
3       Local Area Connection           IPv6                  1500               5 Enabled
3       Local Area Connection           IPv4                  1500               5 Enabled
```

Output listing status for a specific adapter using IFINDEX

Microsoft Windows 7 & above include facility to trace network events, through the NETSH utility; this facility can be helpful in understanding and diagnosing network related issues.

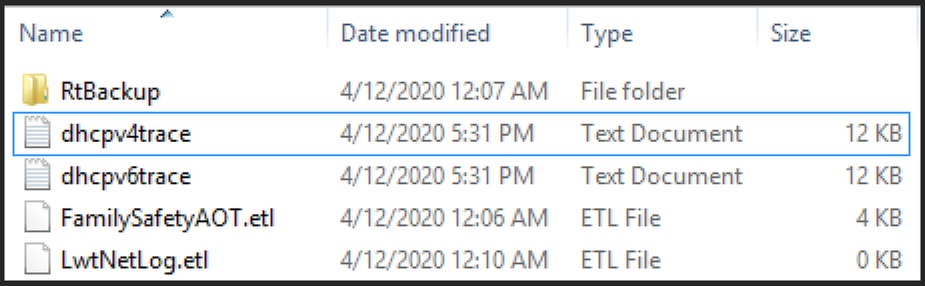
- Use NETSH to collect & view DHCP events
  - CMD > netsh dhcpclient trace dump



```
C:\>netsh dhcpclient trace dump
```

Input to create DHCP trace dump

  - View DHCP log file: C:\Windows\System32\LogFiles\WMI\



Name	Date modified	Type	Size
RtBackup	4/12/2020 12:07 AM	File folder	
dhcpv4trace	4/12/2020 5:31 PM	Text Document	12 KB
dhcpv6trace	4/12/2020 5:31 PM	Text Document	12 KB
FamilySafetyAOT.etl	4/12/2020 12:06 AM	ETL File	4 KB
LwtNetLog.etl	4/12/2020 12:10 AM	ETL File	0 KB

Folder containing log files

  - Open dhcpv4trace.txt & dhcpv6trace.txt in a text editor to observe DHCP process

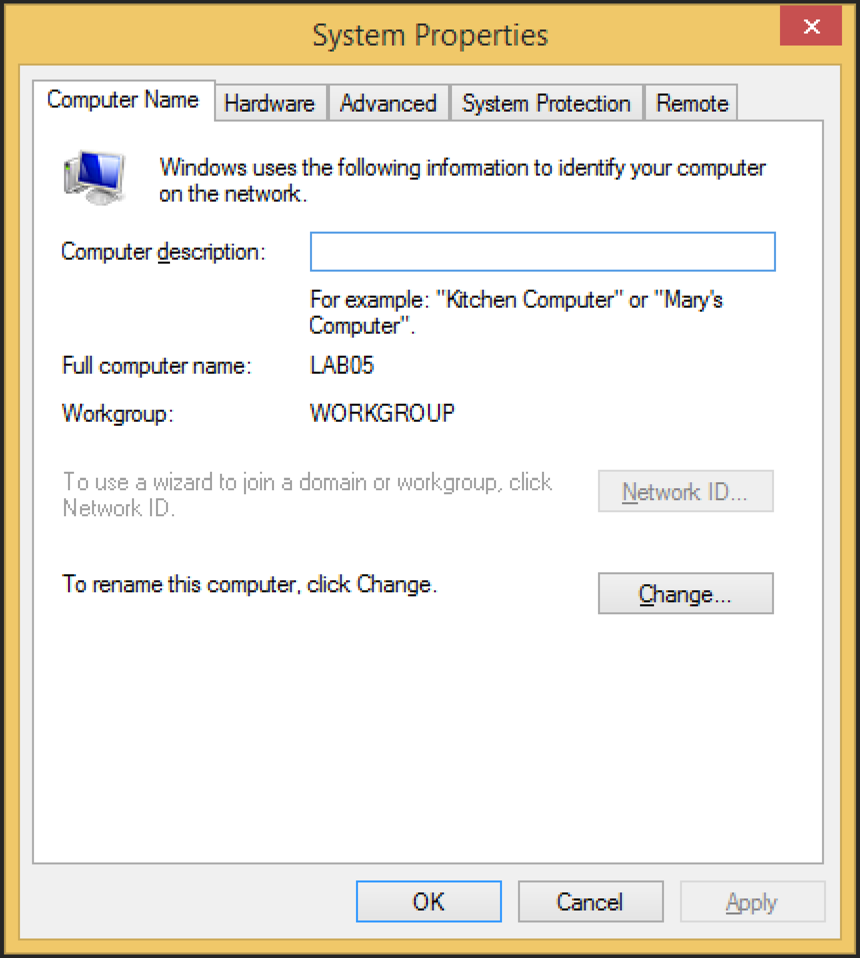
PKTMON is another utility:

- pktmon start –etw
- pktmon stop
- pktmon format pktmon.etl -o output.txt

Computer Names (Microsoft Windows)

- Used for identifying workstations by name on a Microsoft Windows Network.
- Each computer must have a unique name.
- Also referred to as “hostname”, “NetBIOS name” or “Computer Name”.
- Limited to 15 characters.

- To View or change Computer name:
  - START > RUN > SYSDM.CPL



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: LAB05

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer, click Change.

- Select “Change...” (If computer name needs to be changed).
- Specify a name under “Computer name:” (for example: LAB01).
- Select “OK” Twice and Select “Close”.
- Restart the computer.

- View Computer name:
  - CMD > hostname

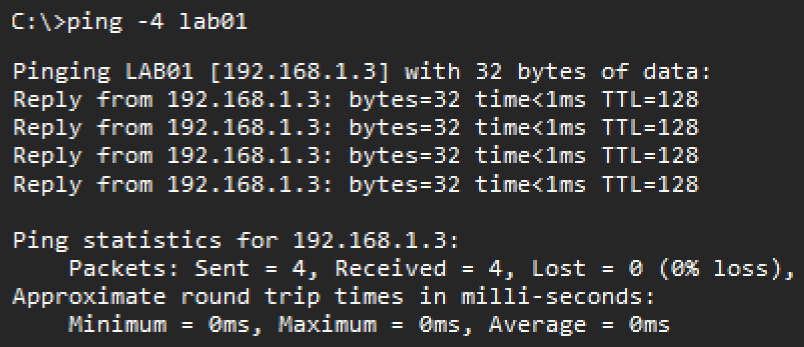
```
C:\>hostname
LAB01
```

Output displaying Computer Name

PING is a command line utility used for testing reach-ability of a host. PING uses ICMP (Internet Control Message Protocol) to send echo request packets, reports statistical summary including round-trip duration, packet loss & errors. This utility works at Network Layer.

ICMP Reference (https://tools.ietf.org/html/rfc792).

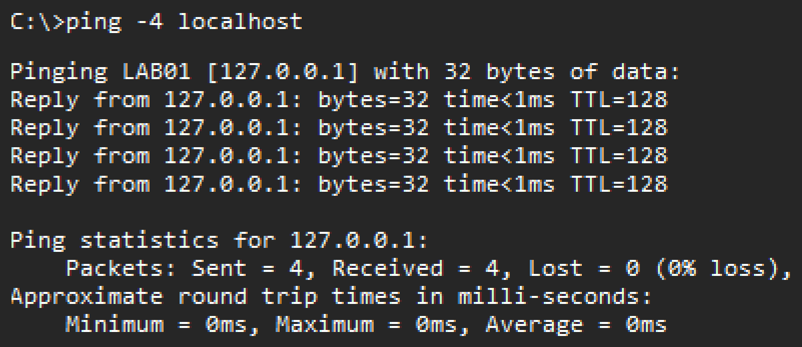
- To check local computer (IPv4):
  - CMD > ping -4 COMPUTERNAME (or)



```
C:\>ping -4 lab01

Pinging LAB01 [192.168.1.3] with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Observe computer name resolved to an IP address & replies

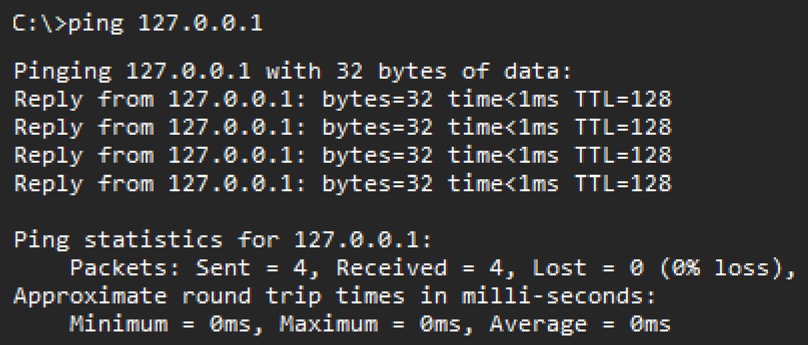
  - CMD > ping -4 localhost (or)



```
C:\>ping -4 localhost

Pinging LAB01 [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Output indicates successful replies, observe LOCALHOST resolved to 127.0.0.1

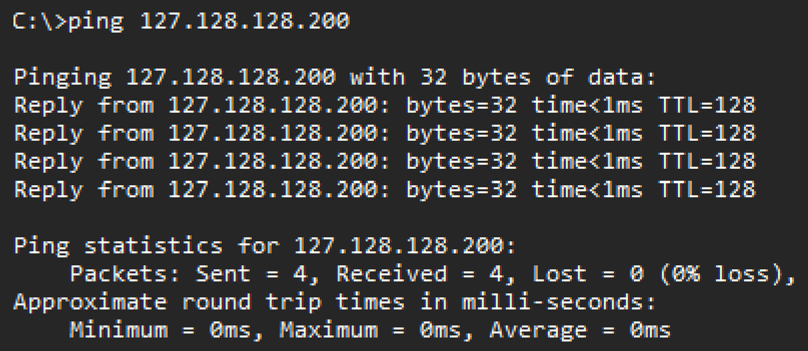
- CMD > ping 127.0.0.1 (or)



```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Output based on default loopback address

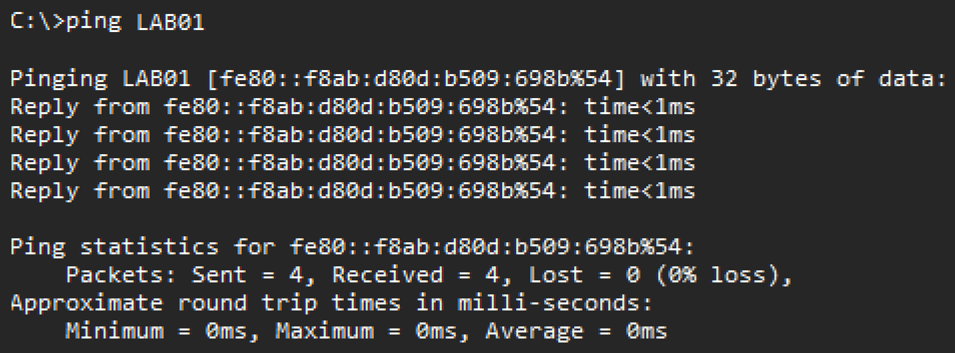
- CMD > ping 127.128.128.200



```
C:\>ping 127.128.128.200

Pinging 127.128.128.200 with 32 bytes of data:
Reply from 127.128.128.200: bytes=32 time<1ms TTL=128
Reply from 127.128.128.200: bytes=32 time<1ms TTL=128
Reply from 127.128.128.200: bytes=32 time<1ms TTL=128
Reply from 127.128.128.200: bytes=32 time<1ms TTL=128

Ping statistics for 127.128.128.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Observe results based on any IPv4 loopback range

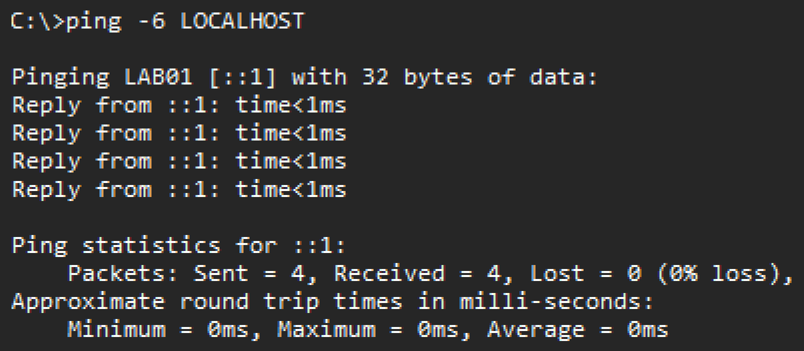
- To check local computer (IPv6):
    - CMD > ping COMPUTERNAME (or)



```
C:\>ping LAB01

Pinging LAB01 [fe80::f8ab:d80d:b509:698b%54] with 32 bytes of data:
Reply from fe80::f8ab:d80d:b509:698b%54: time<1ms
Reply from fe80::f8ab:d80d:b509:698b%54: time<1ms
Reply from fe80::f8ab:d80d:b509:698b%54: time<1ms
Reply from fe80::f8ab:d80d:b509:698b%54: time<1ms

Ping statistics for fe80::f8ab:d80d:b509:698b%54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Observe computer name resolved to an IPv6 address & replies

- CMD > ping -6 LOCALHOST



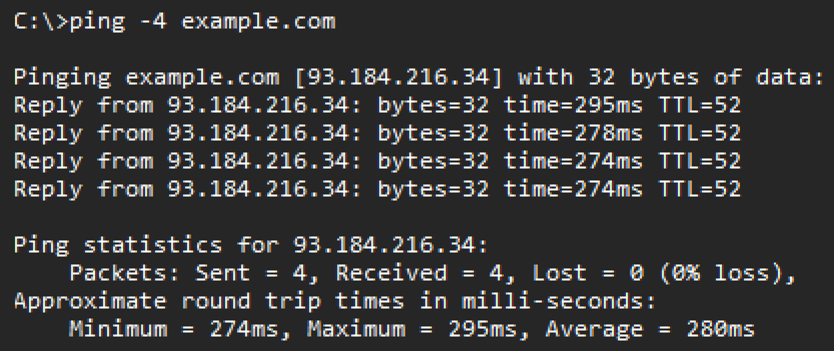
```
C:\>ping -6 LOCALHOST

Pinging LAB01 [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Output indicates successful replies, observe LOCALHOST resolved to ::1 (loopback address for IPv6)

Interpreting PING Echo replies, a general approach (additional steps required to understand specific issue):

- Reply from… - Indicates the host has replied.
- Request Timed Out - Indicates a variety of situations:
    - Firewall blocking request.
    - Remote host configured not to respond.
    - Remote host may be down.
- Destination Host Unreachable - Indicates no route to the remote host.
- Network Unreachable - Indicates a there is no route to that particular network.

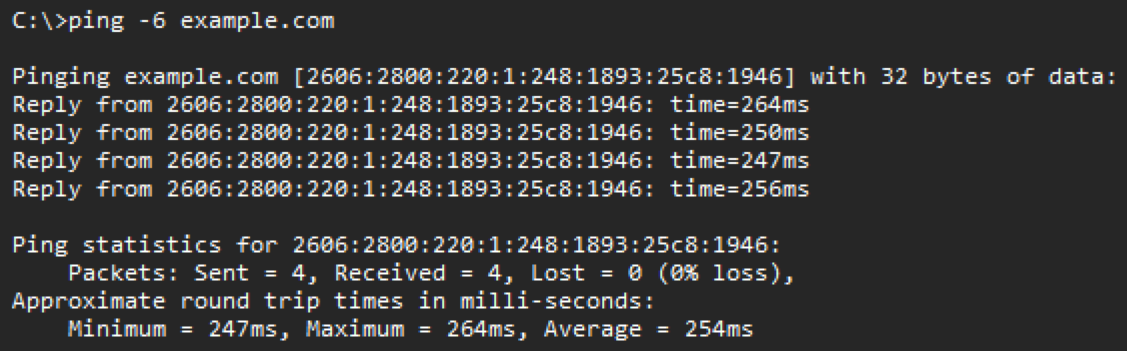
- To check a domain name using IPv4
  - CMD > ping -4 domainname



```
C:\>ping -4 example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=295ms TTL=52
Reply from 93.184.216.34: bytes=32 time=278ms TTL=52
Reply from 93.184.216.34: bytes=32 time=274ms TTL=52
Reply from 93.184.216.34: bytes=32 time=274ms TTL=52

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 274ms, Maximum = 295ms, Average = 280ms
```

Input to test connectivity to a remote device or computer using IPv4

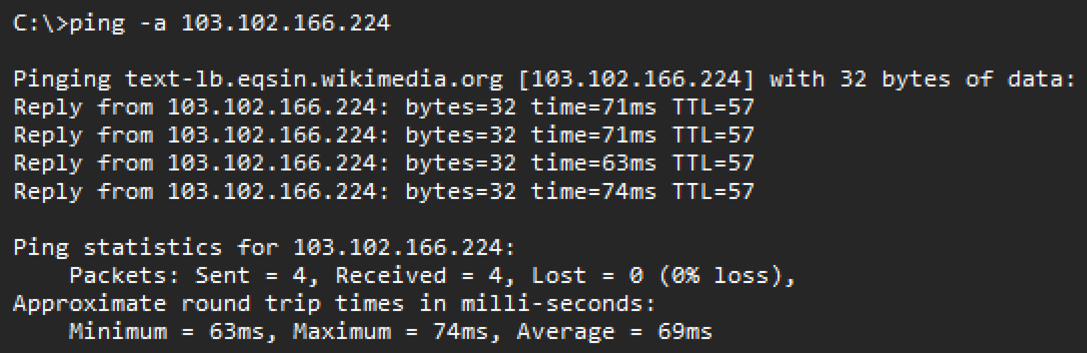
- To check a domain name using IPv6 (If available)
  - CMD > ping -6 domainname



```
C:\>ping -6 example.com

Pinging example.com [2606:2800:220:1:248:1893:25c8:1946] with 32 bytes of data:
Reply from 2606:2800:220:1:248:1893:25c8:1946: time=264ms
Reply from 2606:2800:220:1:248:1893:25c8:1946: time=250ms
Reply from 2606:2800:220:1:248:1893:25c8:1946: time=247ms
Reply from 2606:2800:220:1:248:1893:25c8:1946: time=256ms

Ping statistics for 2606:2800:220:1:248:1893:25c8:1946:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 247ms, Maximum = 264ms, Average = 254ms
```

Input to test connectivity to a remote device or computer using IPv6

- To check using a IPv4 address (and to resolve to a domain name)
  - CMD > ping -a IPv4

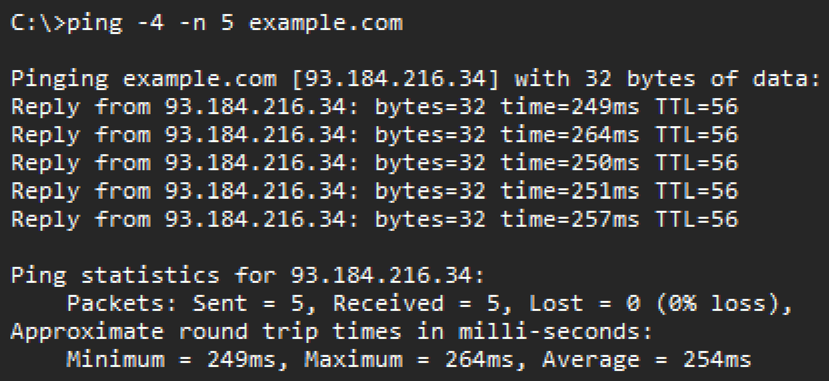


```
C:\>ping -a 103.102.166.224

Pinging text-lb.eqsin.wikimedia.org [103.102.166.224] with 32 bytes of data:
Reply from 103.102.166.224: bytes=32 time=71ms TTL=57
Reply from 103.102.166.224: bytes=32 time=71ms TTL=57
Reply from 103.102.166.224: bytes=32 time=63ms TTL=57
Reply from 103.102.166.224: bytes=32 time=74ms TTL=57

Ping statistics for 103.102.166.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 74ms, Average = 69ms
```

Input to test connectivity using IPv4 address, and to resolve associated domain name

PING limits 4 echo requests by default, which can be increased or decreased.

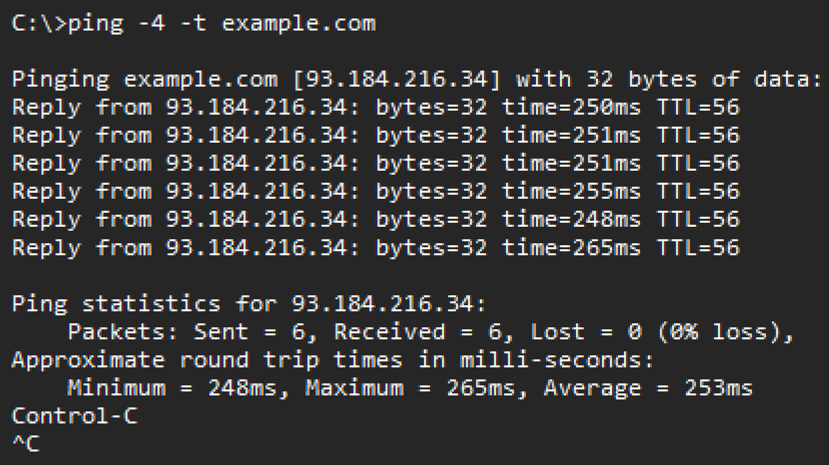
- For 5 requests (IPv4)
  - CMD > ping -4 -n # domainname



```
C:\>ping -4 -n 5 example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=249ms TTL=56
Reply from 93.184.216.34: bytes=32 time=264ms TTL=56
Reply from 93.184.216.34: bytes=32 time=250ms TTL=56
Reply from 93.184.216.34: bytes=32 time=251ms TTL=56
Reply from 93.184.216.34: bytes=32 time=257ms TTL=56

Ping statistics for 93.184.216.34:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 249ms, Maximum = 264ms, Average = 254ms
```

Input to limit max. 5 requests

- For unlimited (until interruption) requests (IPv4) - Use CTRL+C to stop
  - CMD > ping -4 -t domainname

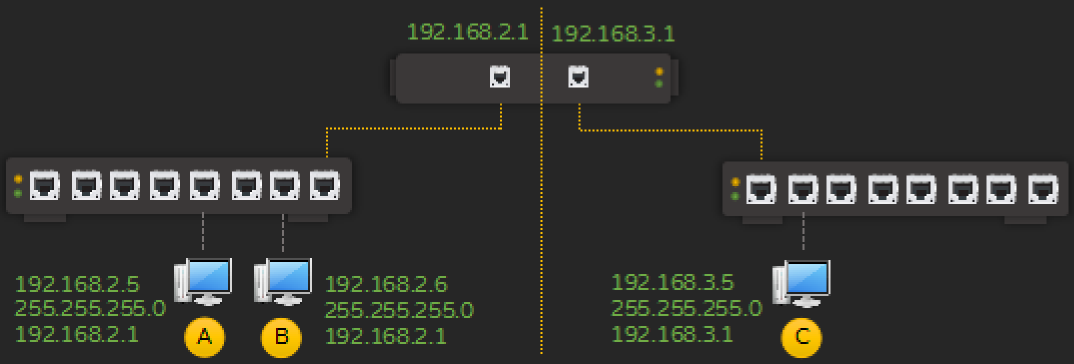


```
C:\>ping -4 -t example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=250ms TTL=56
Reply from 93.184.216.34: bytes=32 time=251ms TTL=56
Reply from 93.184.216.34: bytes=32 time=251ms TTL=56
Reply from 93.184.216.34: bytes=32 time=255ms TTL=56
Reply from 93.184.216.34: bytes=32 time=248ms TTL=56
Reply from 93.184.216.34: bytes=32 time=265ms TTL=56

Ping statistics for 93.184.216.34:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 248ms, Maximum = 265ms, Average = 253ms
Control-C
^C
```

Output listing 6 replies, a) break applied using CTRL+C

IP Routing

- Process of data transfer by selecting a path across networks.
- Routers exchange data to maintain a route table.
- Routers route packets from source to destination based on the forwarding table.
- Types
  - Static Routing
    - Packets are routed only through fixed path set by an administrator.
    - Packets may not reach the destination if there is problem in fixed path.
    - Suitable for smaller networks or network setups that never change.
  - Dynamic Routing
    - Path automatically determined based on routing table.
    - Packets may take different routes to reach the destination.
    - Alternate path selected automatically if there are traffic or network problems.
    - Suitable for medium, large & very large networks.
    - Utilize protocols such as RIP, OSPF, etc.



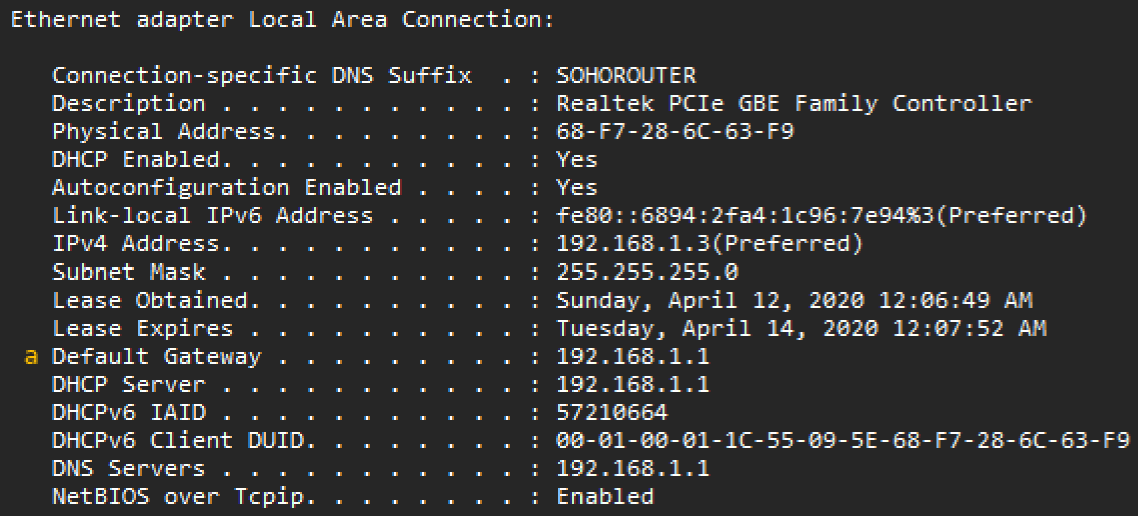
Scenario: Two logical networks (192.168.2.x & 192.168.3.x), connected via Router

- OSPF (Open Shortest Path First) uses link state routing algorithm to find the best shortest route; widely used on large enterprise and service provider networks.
- RIP (Routing Information Protocol) uses hop count to find shortest path.

Note: “Hop” refers to passing of packet from one network to another, in general lesser the hop faster the network performance as the path is shorter.

Packets are routed to external IP networks, through the IP specified in “Default Gateway”.

- View Gateway IP:
    - CMD > ipconfig /all

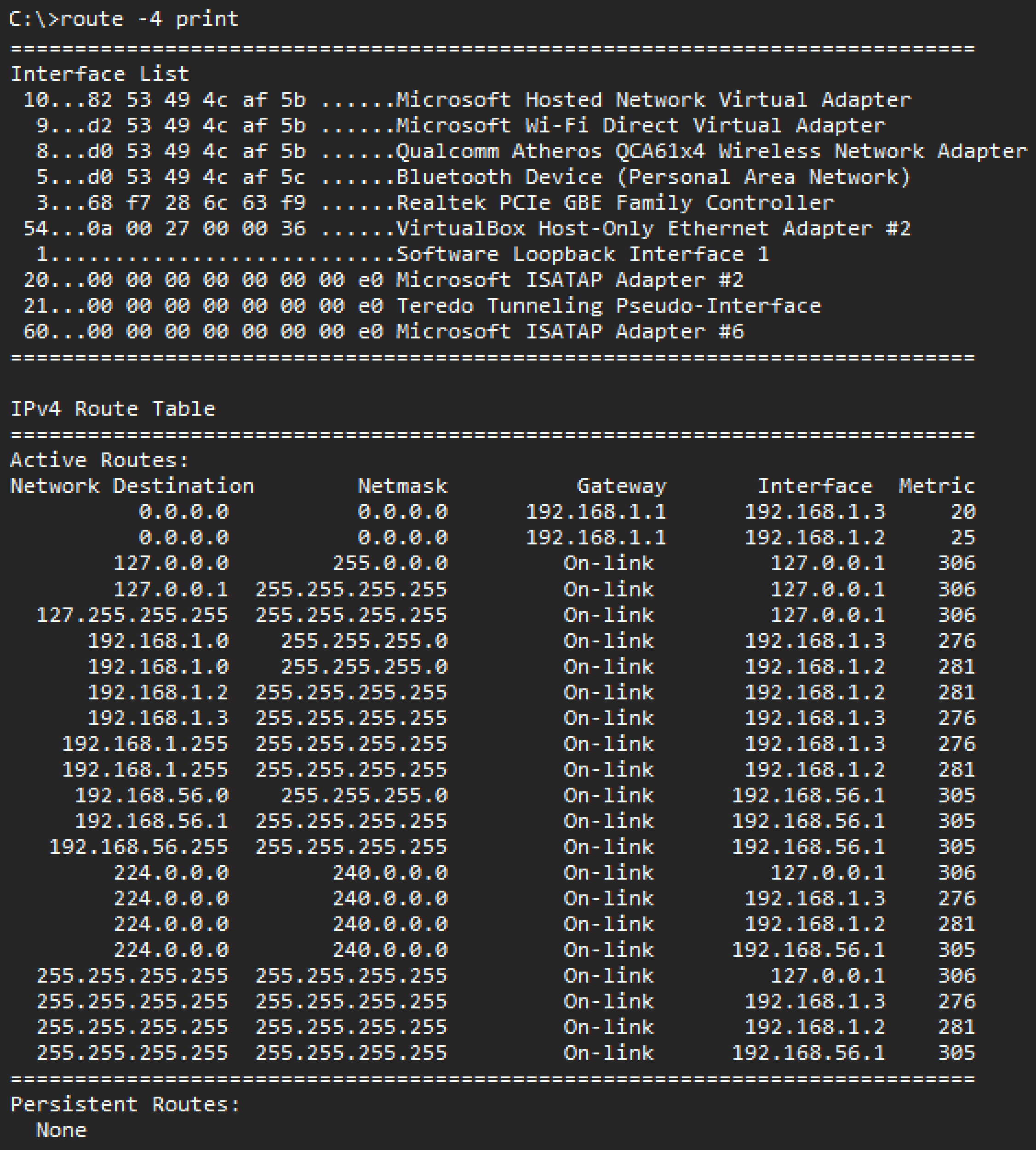


```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 12:06:49 AM
   Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 12:07:52 AM
 a Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Output listing a) Default Gateway IP address

ROUTE command is used for viewing, setting up & modifying (for static routing) routing tables.

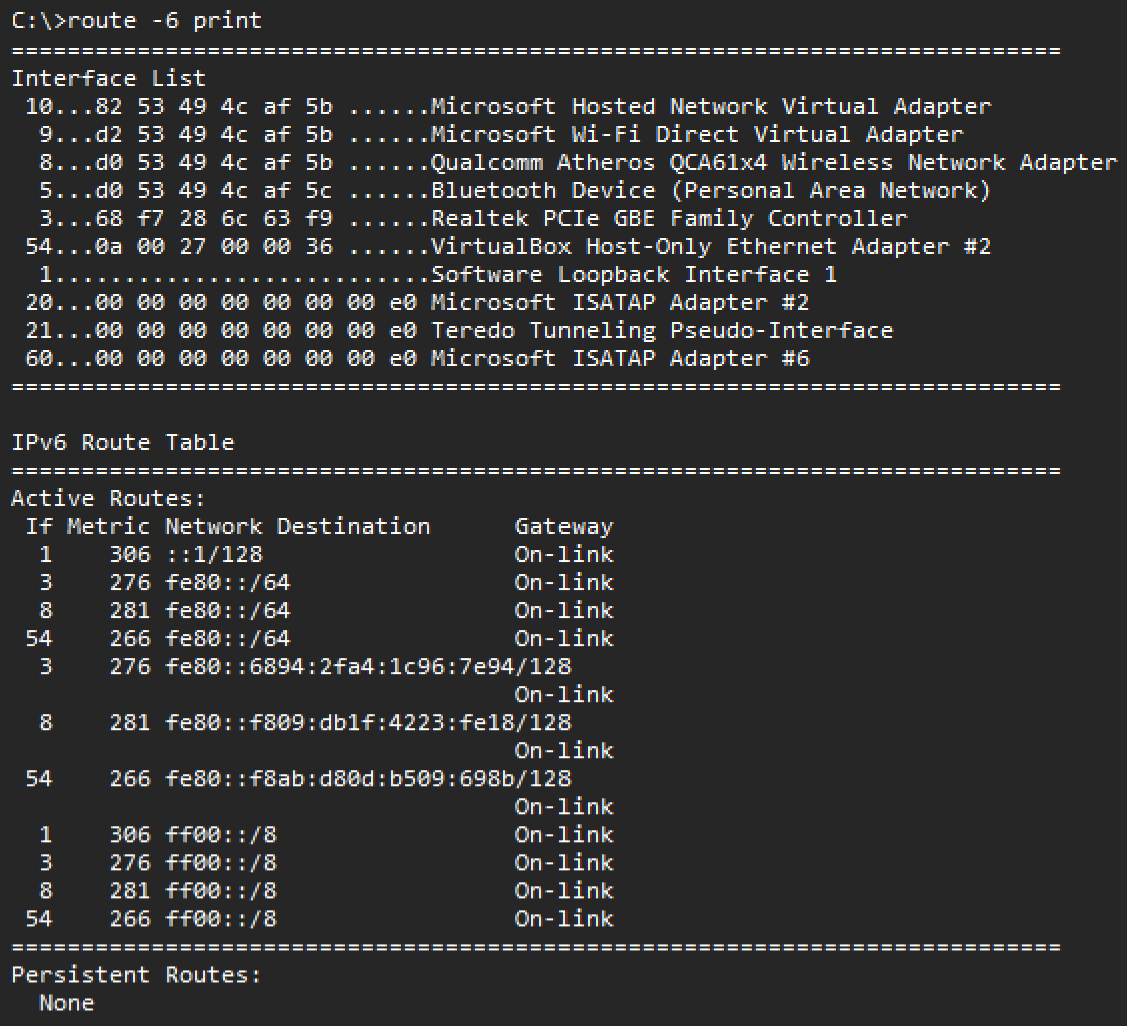
- View Route Table (IPv4):
  - CMD > route -4 print



```
C:\>route -4 print
===========================================================================
Interface List
 10...82 53 49 4c af 5b ......Microsoft Hosted Network Virtual Adapter
  9...d2 53 49 4c af 5b ......Microsoft Wi-Fi Direct Virtual Adapter
  8...d0 53 49 4c af 5b ......Qualcomm Atheros QCA61x4 Wireless Network Adapter
  5...d0 53 49 4c af 5c ......Bluetooth Device (Personal Area Network)
  3...68 f7 28 6c 63 f9 ......Realtek PCIe GBE Family Controller
 54...0a 00 27 00 00 36 ......VirtualBox Host-Only Ethernet Adapter #2
  1...........................Software Loopback Interface 1
 20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 21...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 60...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.3     20
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.2     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link       192.168.1.3    276
      192.168.1.0    255.255.255.0         On-link       192.168.1.2    281
      192.168.1.2  255.255.255.255         On-link       192.168.1.2    281
      192.168.1.3  255.255.255.255         On-link       192.168.1.3    276
    192.168.1.255  255.255.255.255         On-link       192.168.1.3    276
    192.168.1.255  255.255.255.255         On-link       192.168.1.2    281
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    305
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    305
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    305
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       192.168.1.3    276
        224.0.0.0        240.0.0.0         On-link       192.168.1.2    281
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    305
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       192.168.1.3    276
  255.255.255.255  255.255.255.255         On-link       192.168.1.2    281
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    305
===========================================================================
Persistent Routes:
  None
```

Output listing IPv4 route table (cache)

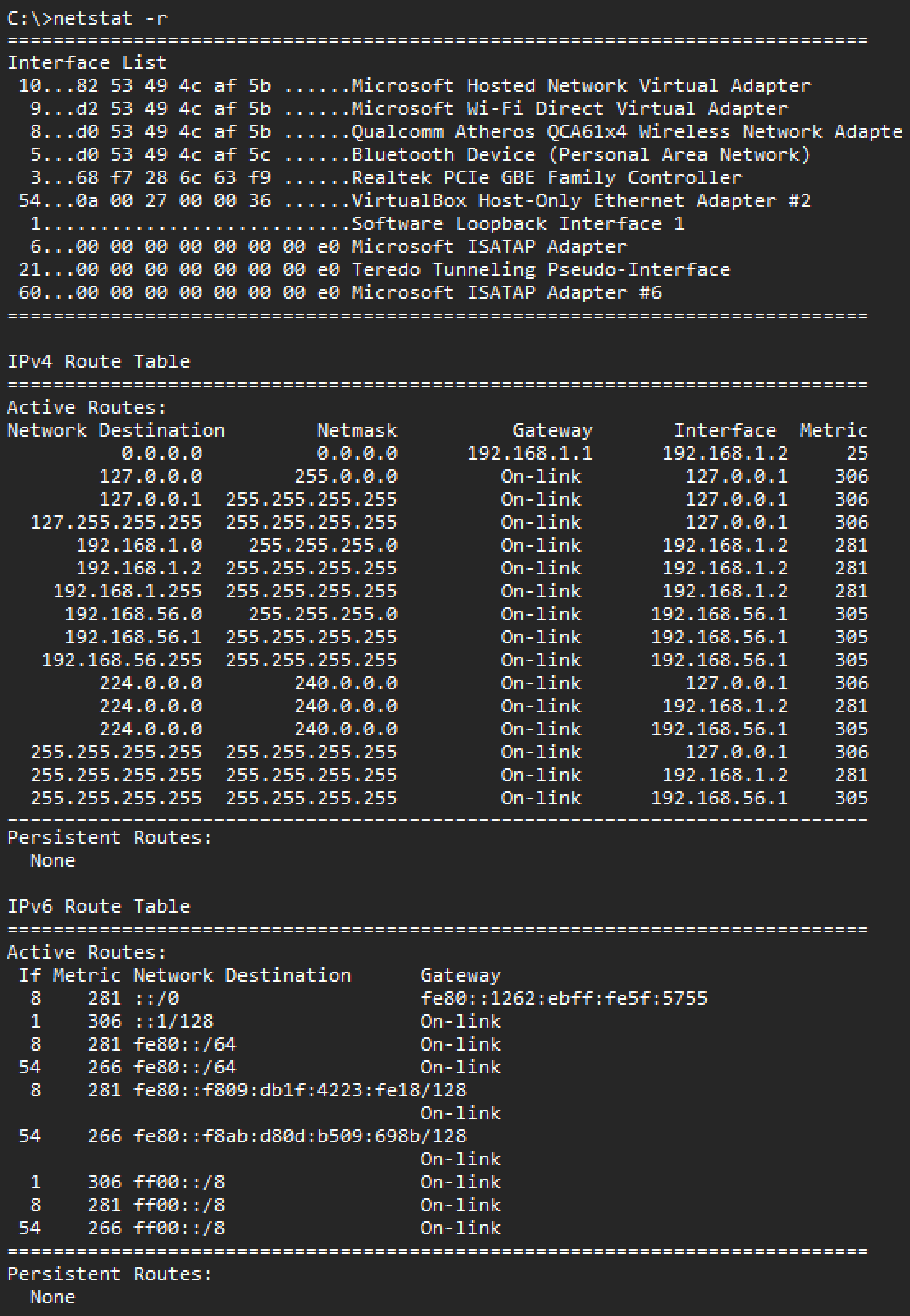
- View Route Table (IPv6):
    - CMD > route -6 print



```
C:\>route -6 print
===========================================================================
Interface List
 10...82 53 49 4c af 5b ......Microsoft Hosted Network Virtual Adapter
  9...d2 53 49 4c af 5b ......Microsoft Wi-Fi Direct Virtual Adapter
  8...d0 53 49 4c af 5b ......Qualcomm Atheros QCA61x4 Wireless Network Adapter
  5...d0 53 49 4c af 5c ......Bluetooth Device (Personal Area Network)
  3...68 f7 28 6c 63 f9 ......Realtek PCIe GBE Family Controller
 54...0a 00 27 00 00 36 ......VirtualBox Host-Only Ethernet Adapter #2
  1...........................Software Loopback Interface 1
 20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 21...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 60...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
  3    276 fe80::/64                On-link
  8    281 fe80::/64                On-link
 54    266 fe80::/64                On-link
  3    276 fe80::6894:2fa4:1c96:7e94/128
                                    On-link
  8    281 fe80::f809:db1f:4223:fe18/128
                                    On-link
 54    266 fe80::f8ab:d80d:b509:698b/128
                                    On-link
  1    306 ff00::/8                 On-link
  3    276 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
 54    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Output listing IPv6 Route Table (Cache)

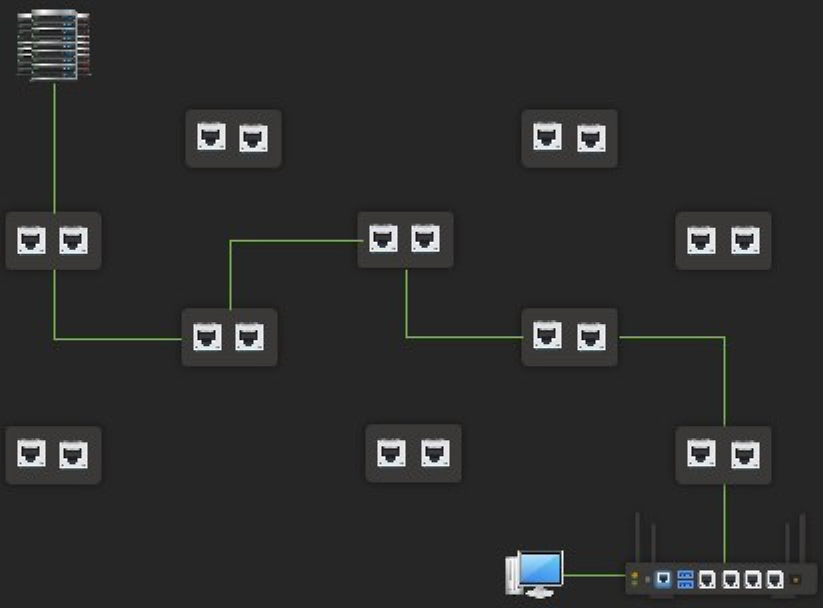
- View Routing Table (IPv4 & IPv6):
  - CMD > netstat -r



```
C:\>netstat -r
===========================================================================
Interface List
 10...82 53 49 4c af 5b ......Microsoft Hosted Network Virtual Adapter
  9...d2 53 49 4c af 5b ......Microsoft Wi-Fi Direct Virtual Adapter
  8...d0 53 49 4c af 5b ......Qualcomm Atheros QCA61x4 Wireless Network Adapte
  5...d0 53 49 4c af 5c ......Bluetooth Device (Personal Area Network)
  3...68 f7 28 6c 63 f9 ......Realtek PCIe GBE Family Controller
 54...0a 00 27 00 00 36 ......VirtualBox Host-Only Ethernet Adapter #2
  1...........................Software Loopback Interface 1
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 21...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 60...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.2     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.1.0    255.255.255.0         On-link       192.168.1.2    281
      192.168.1.2  255.255.255.255         On-link       192.168.1.2    281
    192.168.1.255  255.255.255.255         On-link       192.168.1.2    281
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    305
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    305
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    305
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link       192.168.1.2    281
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    305
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       192.168.1.2    281
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    305
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8    281 ::/0                     fe80::1262:ebff:fe5f:5755
  1    306 ::1/128                  On-link
  8    281 fe80::/64                On-link
 54    266 fe80::/64                On-link
  8    281 fe80::f809:db1f:4223:fe18/128
                                    On-link
 54    266 fe80::f8ab:d80d:b509:698b/128
                                    On-link
  1    306 ff00::/8                 On-link
  8    281 ff00::/8                 On-link
 54    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

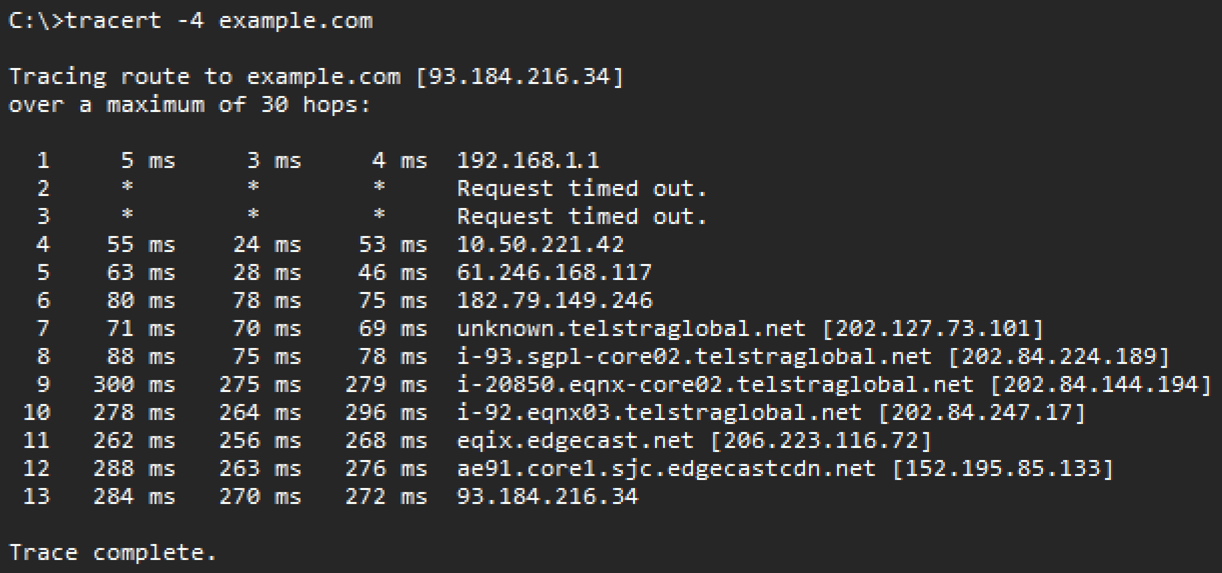
Output displaying IPv4 & IPv6 table

TRACERT (Trace Route) is a command used to display the route that packets take from the source to the destination, along with transit delays at each hop. Each hop corresponds to a router or network device along the route. TRACERT measures the round-trip time (RTT) to each hop along the path, which helps in identifying network bottlenecks, routing issues, or unreachable hosts. This tool is commonly used for troubleshooting network congestion and path-related problems.



A packet may take different path from source to destination

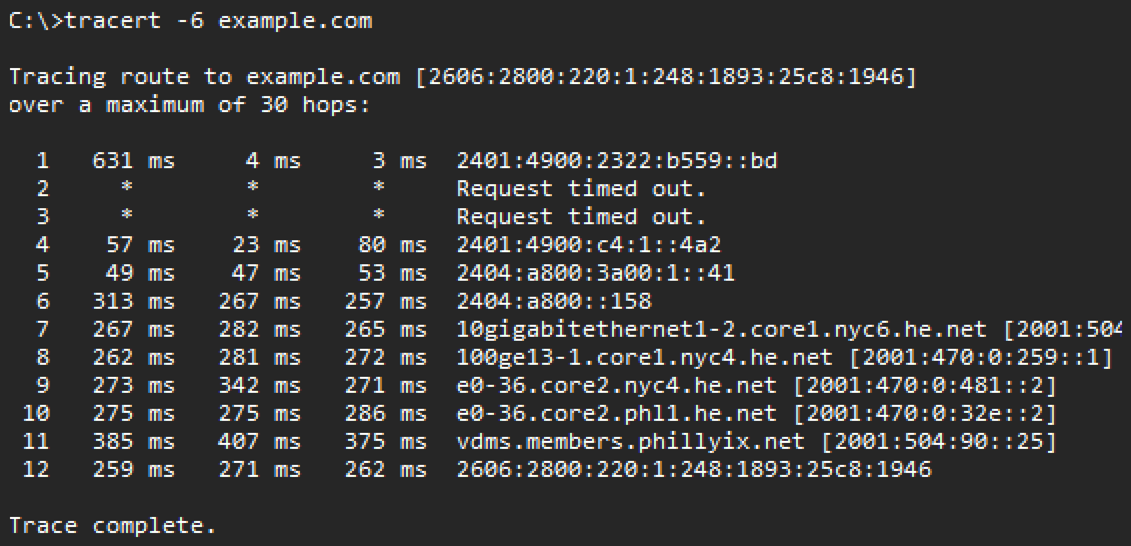
- View route taken (IPv4):
  - CMD > tracert -4 domainname



```
C:\>tracert -4 example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     5 ms     3 ms     4 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    55 ms    24 ms    53 ms  10.50.221.42
  5    63 ms    28 ms    46 ms  61.246.168.117
  6    80 ms    78 ms    75 ms  182.79.149.246
  7    71 ms    70 ms    69 ms  unknown.telstraglobal.net [202.127.73.101]
  8    88 ms    75 ms    78 ms  i-93.sgpl-core02.telstraglobal.net [202.84.224.189]
  9   300 ms   275 ms   279 ms  i-20850.eqnx-core02.telstraglobal.net [202.84.144.194]
 10   278 ms   264 ms   296 ms  i-92.eqnx03.telstraglobal.net [202.84.247.17]
 11   262 ms   256 ms   268 ms  eqix.edgecast.net [206.223.116.72]
 12   288 ms   263 ms   276 ms  ae91.core1.sjc.edgecastcdn.net [152.195.85.133]
 13   284 ms   270 ms   272 ms  93.184.216.34

Trace complete.
```

Output listing route taken by a packet using IPv4

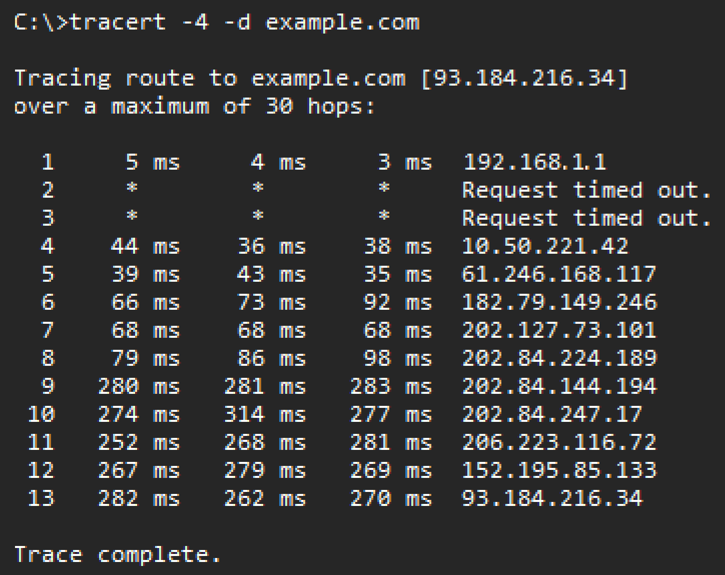
- View route taken (IPv6):
  - CMD > tracert -6 domainname



```
C:\>tracert -6 example.com

Tracing route to example.com [2606:2800:220:1:248:1893:25c8:1946]
over a maximum of 30 hops:

  1   631 ms     4 ms     3 ms  2401:4900:2322:b559::bd
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    57 ms    23 ms    80 ms  2401:4900:c4:1::4a2
  5    49 ms    47 ms    53 ms  2404:a800:3a00:1::41
  6   313 ms   267 ms   257 ms  2404:a800::158
  7   267 ms   282 ms   265 ms  10gigabitethernet1-2.core1.nyc6.he.net [2001:504
  8   262 ms   281 ms   272 ms  100ge13-1.core1.nyc4.he.net [2001:470:0:259::1]
  9   273 ms   342 ms   271 ms  e0-36.core2.nyc4.he.net [2001:470:0:481::2]
 10   275 ms   275 ms   286 ms  e0-36.core2.phl1.he.net [2001:470:0:32e::2]
 11   385 ms   407 ms   375 ms  vdms.members.phillyix.net [2001:504:90::25]
 12   259 ms   271 ms   262 ms  2606:2800:220:1:248:1893:25c8:1946

Trace complete.
```

Output listing route taken by a packet using IPv6

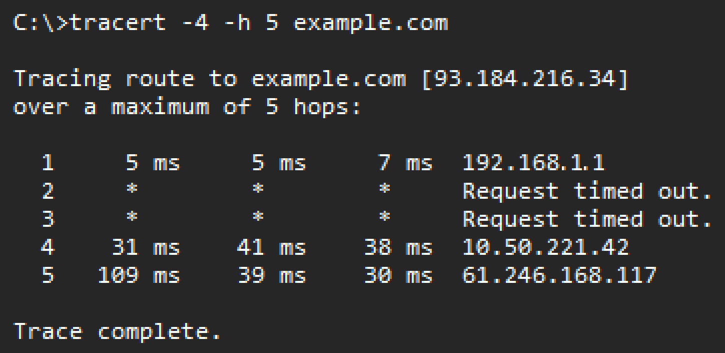
- View route without displaying domain names
    - CMD > tracert -d domainname



```
C:\>tracert -4 -d example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     5 ms     4 ms     3 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    44 ms    36 ms    38 ms  10.50.221.42
  5    39 ms    43 ms    35 ms  61.246.168.117
  6    66 ms    73 ms    92 ms  182.79.149.246
  7    68 ms    68 ms    68 ms  202.127.73.101
  8    79 ms    86 ms    98 ms  202.84.224.189
  9   280 ms   281 ms   283 ms  202.84.144.194
 10   274 ms   314 ms   277 ms  202.84.247.17
 11   252 ms   268 ms   281 ms  206.223.116.72
 12   267 ms   279 ms   269 ms  152.195.85.133
 13   282 ms   262 ms   270 ms  93.184.216.34

Trace complete.
```

Output listing route without resolving domain names

- Set maximum hops (IPv4)
    - CMD > tracert -4 -h #hops domainname

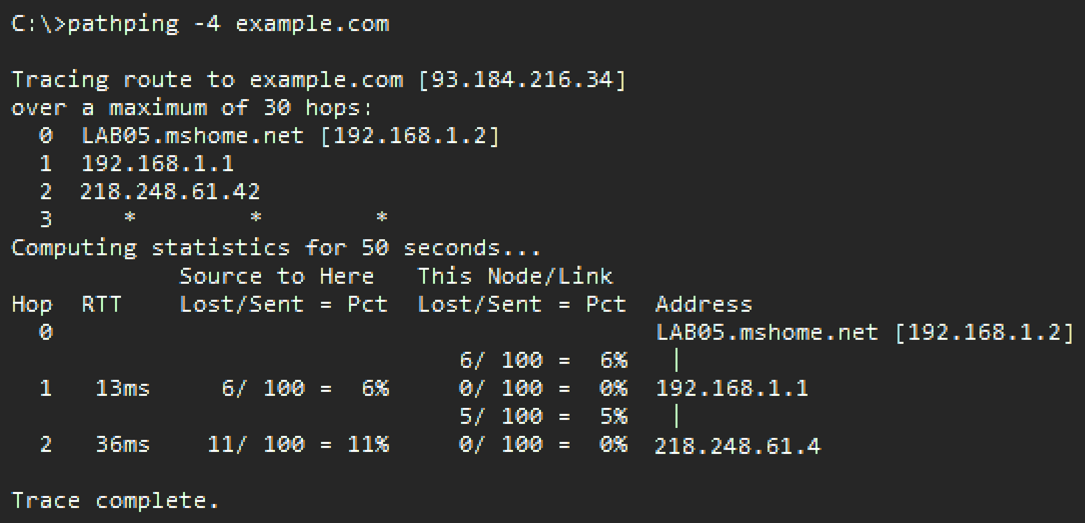


```
C:\>tracert -4 -h 5 example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 5 hops:

  1     5 ms     5 ms     7 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4    31 ms    41 ms    38 ms  10.50.221.42
  5   109 ms    39 ms    30 ms  61.246.168.117

Trace complete.
```

Output listing with results - maximum 5 hops

PATHPING is more than just a combination of PING and TRACERT. It provides detailed statistics for each hop along the path from the source to the destination, helping to identify routing issues and related problems such as packet loss and latency. PATHPING first uses TRACERT to map the route, then sends PING requests to each hop to gather data on packet loss and delay (latency).

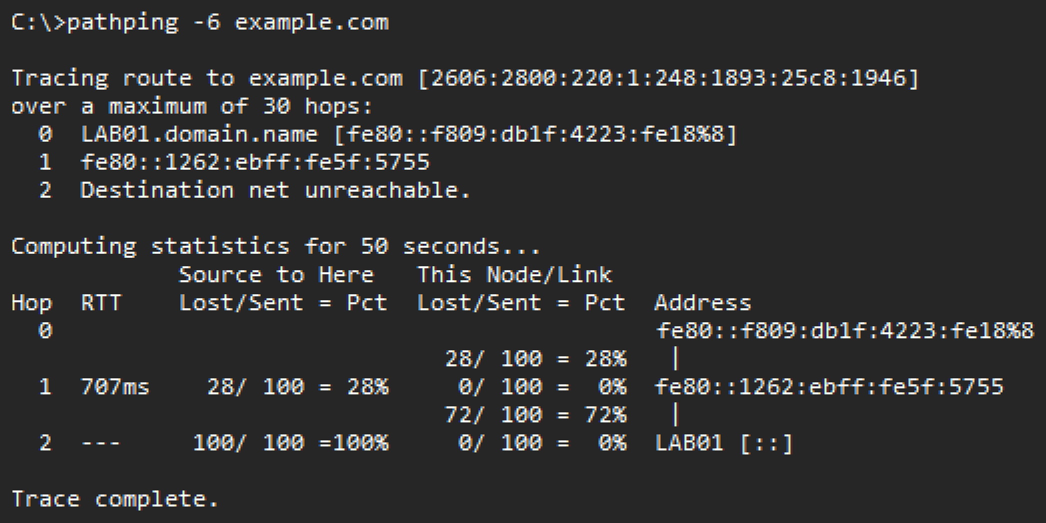
- View statistics (IPv4):
  - CMD > pathping -4 domainame



```
C:\>pathping -4 example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:
  0  LAB05.mshome.net [192.168.1.2]
  1  192.168.1.1
  2  218.248.61.42
  3     *        *        *
Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAB05.mshome.net [192.168.1.2]
                                6/ 100 =  6%   |
  1   13ms     6/ 100 =  6%     0/ 100 =  0%  192.168.1.1
                                5/ 100 =  5%   |
  2   36ms    11/ 100 = 11%     0/ 100 =  0%  218.248.61.4

Trace complete.
```

Output listing results of route & packet statistics for IPv4

- View statistics (IPv6):
  - CMD > pathping -6 domainname



```
C:\>pathping -6 example.com

Tracing route to example.com [2606:2800:220:1:248:1893:25c8:1946]
over a maximum of 30 hops:
  0  LAB01.domain.name [fe80::f809:db1f:4223:fe18%8]
  1  fe80::1262:ebff:fe5f:5755
  2  Destination net unreachable.

Computing statistics for 50 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           fe80::f809:db1f:4223:fe18%8
                               28/ 100 = 28%   |
  1  707ms    28/ 100 = 28%     0/ 100 =  0%  fe80::1262:ebff:fe5f:5755
                               72/ 100 = 72%   |
  2  ---     100/ 100 =100%     0/ 100 =  0%  LAB01 [::]

Trace complete.
```

Output listing results of route & packet statistics for IPv6

Quiz 05

1. 'Set of rules for communication' refers to _____.

A. Protocol B. Service C. Interface D. Network Device

2. Protocols at Layer 3 _____.

A. IP B. ICMP C. IGMP D. DSL

3. _____ layer of the OSI model refers to logical addressing and routing.

A. Physical B. Data-link C. Network D. Session

4. Examples of Proprietary protocols:

A. NetBEUI B. IPX/SPX C. AppleTalk D. All of the above

5. Examples of Open standard protocol:

A. NetBEUI B. IPX/SPX C. AppleTalk D. TCP/IP

6. Acronym - NetBEUI.

A. NetBIOS Extended User Interface
B. Network Extended User Interface
C. NetBIOS Expanded User Interface
D. Network Expanded User Interface

7. Acronym - IPX/SPX.

A. Internetwork Packet Exchange/Sequenced Packet Exchange
B. Intranetwork Packet Exchange/Sequenced Packet Exchange
C. Internetwork Protocol Exchange/Sequenced Protocol Exchange
D. Intranetwork Protocol Exchange/Sequenced Protocol Exchange

8. Acronym - TCP/IP.

A. Transmission Connection Protocol / Internet Protocol
B. Transmission Control Packet / Internet Packet
C. Transmission Control Protocol / Internet Protocol
D. Transmission Control Protocol / Internet Packet

9. Advantages of TCP/IP.

A. Open Standard
B. Multiple Network framework
C. Routable
D. All of the above

10. Proprietary protocol used in early Microsoft Windows networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

11. Proprietary protocol used in Apple computer networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

12. Proprietary protocol used on Novell NetWare networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

13. IPv4 uses _____ bit addressing scheme.

A. 4 B. 8 C. 32 D. 64

14. IPv6 uses _____ bit addressing scheme.

A. 8 B. 32 C. 64 D. 128

15. _____ is the entity that oversees global IP address allocation.

A. IEEE B. IETF C. IANA D. ISO

16. Acronym - IANA.

A. Internet Assigned Numeric Authority
B. Intranet Assigned Numbers Authority
C. Internet Automated Numbers Authority
D. Internet Assigned Numbers Authority

17. Maximum number of IP addresses in IPv4

A. 65536 B. 4294967296 C. 256 D. 16

18. Maximum number of IP addresses in IPv6:

A. 4294967296
B. 340282366920938463463374607431768211456
C. 42949672964294967296
D. 340282366920938463463

19. Class reserved for multicasting:

A. Class A B. Class B C. Class C D. Class D

20. IP address range for Class A:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

21. IP address range for Class B:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

22. IP address range for Class C:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

23. IP address range for Class D:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

24. IP address range for Class E:

A. 128.0.0.0 - 191.255.255.255
B. 192.0.0.0 - 223.255.255.255
C. 224.0.0.0 - 239.255.255.255
D. 240.0.0.0 - 255.255.255.255

25. _____ addresses are used for communicating between computers on the Internet.

A. Multicast B. Private C. Public D. Broadcast

26. _____ addresses are used for communicating between computers on a LAN.

A. Multicast B. Private C. Public D. Broadcast

27. IP addresses reserved for private networks:

A. 10.0.0.0 – 10.255.255.255 B. 172.16.0.0 - 172.31.255.255
C. 192.168.0.0 – 192.168.255.255 D. All of the above

28. _____ is used for identifying the network and host ID portions of an IP address.

A. Gateway B. Subnet Mask C. DNS Address D. WINS Address

29. Range reserved for loopback addresses:

A. 10.0.0.0 – 10.255.255.255 B. 172.16.0.0 - 172.31.255.2
C. 127.0.0.1 – 127.255.255.255 D. 240.0.0.0 - 255.255.255.255

30. Default subnet mask for Class A range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

31. Default subnet mask for Class B range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

32. Default subnet mask for Class C range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

33. 169. 255.255.255.255 address represents:

A. A Unicast address B. A Multicast address
C. A Broadcast address D. A Gateway address

34. Example of an IPv6 address:

A. 123.123.123.123
B. 2001:0db8:85a3:0042:1000:8a2e:0370:7334
C. A0:10:20:10:12:14
D. V6:123.123.123.133

35. Protocol used for automating IP configuration:

A. ARP B. DHCP C. DNS D. WINS

36. _____ are protocols that do not resolve names to IP addresses.

A. DDNS B. DNS C. WINS D. None

37. _____ indicates network messages or timeouts at layer 3.

A. ARP B. ICMP C. IGMP D. BOOTP

38. DHCP Sequence:

A. Offer; Discover; Request; Acknowledge
B. Discover; Request; Acknowledge; Offer
C. Discover; Offer; Request; Acknowledge
D. Request; Offer; Discover; Acknowledge

39. Purpose of APIPA:

A. Assigns IP address to each computer from a SOHO Router
B. Self-assigns each computer a private IP address
C. Assigns DNS addresses on a DHCP enabled network
D. Routes packets from one logical network to another

40. Acronym - APIPA.

A. Automatic Public IP Addressing B. Activated Private IP Addressing
C. Activated Public IP Addressing D. Automatic Private IP Addressing

41. Range reserved for APIPA:

A. 10.0.0.0 – 10.255.255.255 B. 192.168.0.0. - 192.168.255.255
C. 169.254.1.0 – 169.254.254.255 D. 172.16.0.0 - 172.16.255.255

42. Command utility for viewing IP address:

A. GETMAC B. IPCONFIG C. TELNET D. IPMAC

43. Utility & Syntax for viewing complete IP configuration:

A. IPMAC /Complete B. IPMAC /ALL
C. IPCONFIG /Complete D. IPCONFIG /ALL

44. Command line utility for checking network connectivity:

A. NETSTAT B. IPCONFIG C. PING D. NBTSTAT

45. PING uses _____ protocol.

A. IP B. ICMP C. IGMP D. HTTP

46. Syntax for unlimited packets:

A. PING address -n B. PING address -t
C. PING address -l D. PING address -p

47. Command line utility for managing ARP cache table:

A. IP2MAC B. ARP C. PING D. All of the above

48. Syntax for testing local machine's IP:

A. Ping 127.0.0.1 B. Ping localhost C. Ping 127.1.2.3 D. All of the above

49. Syntax for releasing IP address:

A. IPCONFIG /RELEASE B. IPCONFIG /RENEW
C. IPCONFIG /ALL D. IPCONFIG /REFRESH

50. Syntax for renewing IP address:

A. IPCONFIG /RELEASE B. IPCONFIG /RENEW
C. IPCONFIG /ALL D. IPCONFIG /REFRESH

51. Acronym - CIDR.

A. Classful Inter Domain Routing B. Classful Intra Domain Routing
C. Classless Inter Domain Routing D. Classless Intra Domain Routing

52. Purpose of CIDR:

A. Manipulates MAC address B. Manipulates DNS address
C. Replaces IPv4 with IPv6 D. Allows variable Network and host addresses

53. In _____ routing packets are transmitted through fixed routes.

A. Dynamic B. Static C. Variable D. Fixed

54. In _____ routing routing of packets are determined by routers.

A. Dynamic B. Static C. Variable D. Fixed

55. Command line utility for viewing route and to measure transit delays of a packet:

A. TRACERT B. PATHPING C. ROUTE D. IPCONFIG

56. Command line utility for viewing and manipulating routing tables:

A. TRACERT B. PATHPING C. ROUTE D. IPCONFIG

57. Command line utility that combines the power of both PING and TRACERT:

A. TRACEPING B. TRACEPATH C. PINGPATH D. PATHPING

58. Syntax for viewing routing table:

A. Route Print B. Router Print C. Routing Print D. Routable Print

59. Examples of routable protocols:

A. IPX/SPX B. TCP/IP C. OSPF D. RIP

60. Examples of routing protocols:

A. OSPF B. RIP C. IS-IS D. All of the above

TCP & UDP

- TCP (Transmission Control Protocol)
  - Operates at Layer 4.
  - Provides reliable, orderly, flow-controlled and error-checked delivery of packets.
  - Connection Oriented (handshake between parties before communication).
  - Suitable for critical applications that require guaranteed delivery of packets.
  - Popular applications that utilize TCP include Web browsers, email client software, etc.
- UDP (User Datagram Protocol)
  - Operates at Layer 4.
  - Connection-less (doesn’t check if the receiver is ready or not).
  - No error checking or orderly delivery of packets, not reliable.
  - Suitable for non-critical & bandwidth intensive applications.
  - Application to be programmed to take care of error checking, if UDP is used.
  - Used where occasional loss is acceptable, such as DNS requests, video streaming, etc.

TCP	UDP
Reliable	Unreliable
Connection Oriented	Connection-less
Segment Sequencing	No Sequencing
Acknowledge Segments	No Acknowledgment
Segment re-transmission and Flow control	No re-transmission

TCP Handshake

TCP requires connection to be established before communication, referred to as TCP Handshake:

- Clients initiate by sending “SYN” packet to a server.
- Server responds by replying with “SYN, ACK” to the client.
- Client sends “ACK” packet to the server (Acknowledgment).

TCP states - TCP connections goes through different changes between end-points:

- CLOSE_WAIT
- CLOSED
- ESTABLISHED
- FIN_WAIT_1
- FIN_WAIT_2
- LAST_ACK
- LISTEN
- SYN_RECEIVED
- SYN_SEND
- TIMED_WAIT

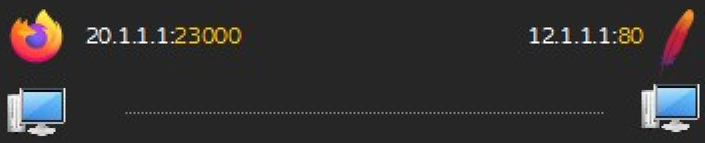
For example, LISTEN indicates that a computer/device is waiting for an incoming request.

Reference(s):

- https://tools.ietf.org/html/rfc793
- https://en.wikipedia.org/wiki/Transmission_Control_Protocol

Ports & Sockets

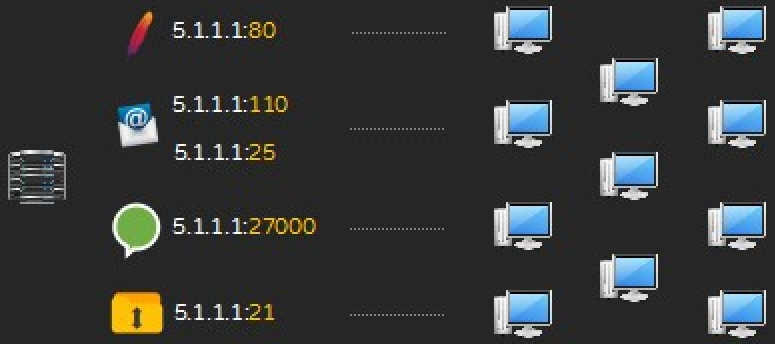
- Logical path between network applications, similar to a pipeline.
- Port uses 16-bit scheme, 2^{16} = 65,536 ports.
- Port “0” reserved, usable ports 1 - 65,535 for each IP address.
- Network application may use a single port or, a range of ports for communication.
- Protocol may use TCP or UDP.
- IP Address + Port Number = Socket.



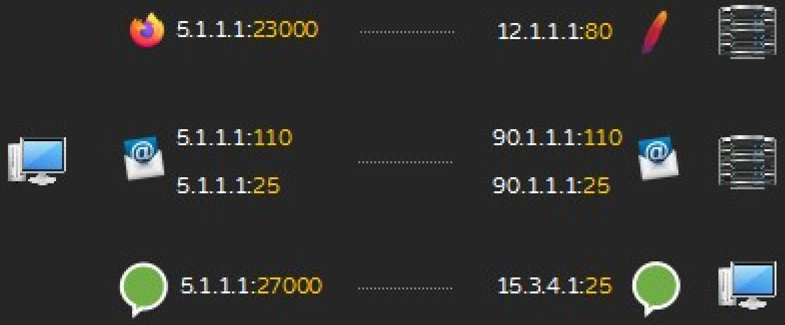
Web Browser sending request from port 23000 to a HTTP server listening on port 80

Example:

1. A HTTP Server “listens” for incoming requests on Port 80 (Default HTTP Port) or 443 (HTTPS).
2. A HTTP Client (Typically a web browser) sends request from a random port to the HTTP Server.
3. HTTP Server replies to HTTP Client.



Run multiple services using a Single IP address through multiple ports, serve multiple clients and/or client applications



Multiple ports usage between computers on a network

Ports are classified:

- Well-known ports: 0 - 1023
- Registered ports: 1024 - 49151
- Dynamic ports: 49152 - 65535

Port	Description
20	FTP
21	FTP
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP3
119	NNTP
143	IMAP
443	HTTPS

Well Known Ports, Examples

Port	Description
1080	SOCKS
1194	OpenVPN
1220	QuickTime
1293	Internet Protocol Security (IPSec)
1433	Microsoft SQL Server
1503	Windows Live Messenger
1512	Windows Internet Name Service (WINS)
1761	Novell ZENworks

Registered Ports, Examples

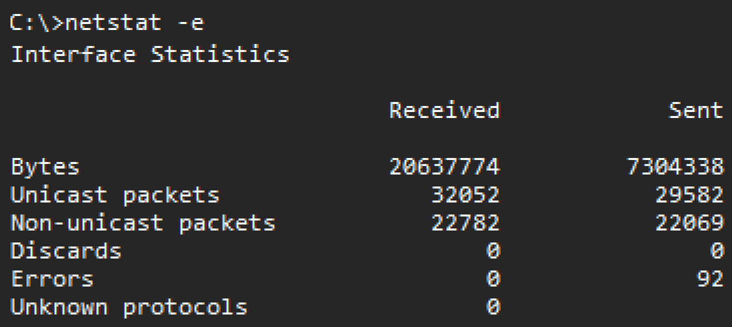
Well-known ports are standardized and serve as a guide for network application programmers. These ports are typically assigned for specific services and are industry standards. However, a network application can use any port number within the allowed range, as defined by the administrator, rather than the standard port numbers. For example, a web server can use port 14000 instead of the standard port 80. In this case, the client must be configured to send requests to port 14000 instead of the default port 80. (Web browsers are typically programmed to send HTTP requests to port 80 by default, and HTTPS requests to port 443.)

Application Layer Protocols

Protocol	Description
HTTP	Hypertext Transfer Protocol, foundation for World Wide Web
FTP	File Transfer Protocol, used for transferring files using TCP
TFTP	Trivial File Transfer Protocol, used for transferring files using UDP
NTP	Network Time Protocol, used for synchronizing time
NNTP	Network News Transfer Protocol, used in USENET applications (articles)
SMTP	Simple Mail Transfer Protocol, used for sending & relaying messages
POP	Post Office Protocol, used for retrieving emails
IMAP	Internet Message Access Protocol, similar to POP designed for multiple email clients
LDAP	Lightweight Directory Access Protocol, used for directory information services
RDP	Remote Desktop Protocol, used for remote connections in Microsoft Windows
SNMP	Simple Network Management Protocol, used for managing devices
SSL	Secure Sockets Layer, cryptographic protocol provides security
TLS	Transport Layer Security, supersedes SSL

NETSTAT command is used to view network interface statistics, listening ports, routing tables, and active connections.

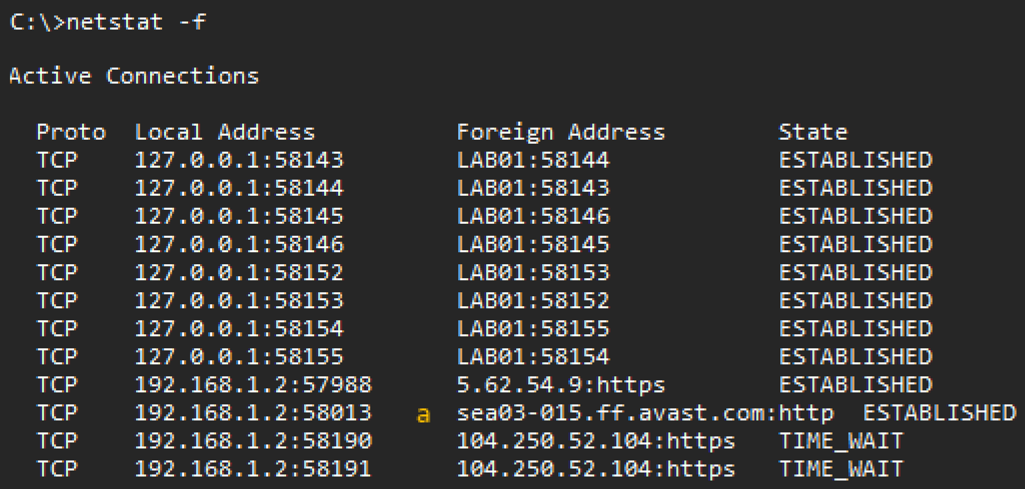
- View Ethernet Statistics:
  - CMD > netstat -e



```
C:\>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      20637774         7304338
Unicast packets               32052           29582
Non-unicast packets           22782           22069
Discards                          0               0
Errors                            0              92
Unknown protocols                 0
```

Output displaying Ethernet statistics

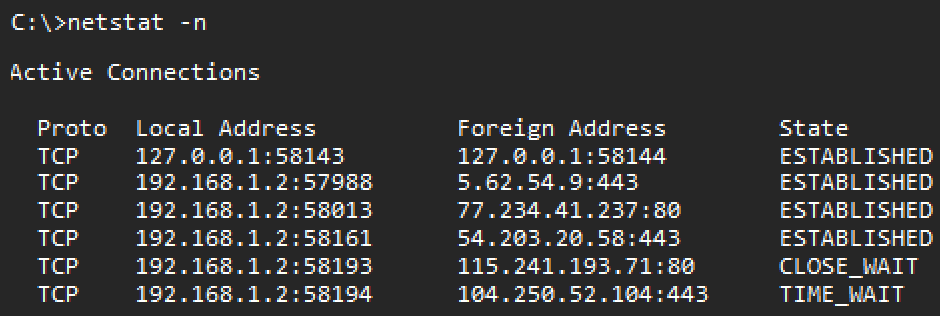
- View statistics (display FQDN):
  - CMD > netstat -f



```
C:\>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:58143        LAB01:58144            ESTABLISHED
  TCP    127.0.0.1:58144        LAB01:58143            ESTABLISHED
  TCP    127.0.0.1:58145        LAB01:58146            ESTABLISHED
  TCP    127.0.0.1:58146        LAB01:58145            ESTABLISHED
  TCP    127.0.0.1:58152        LAB01:58153            ESTABLISHED
  TCP    127.0.0.1:58153        LAB01:58152            ESTABLISHED
  TCP    127.0.0.1:58154        LAB01:58155            ESTABLISHED
  TCP    127.0.0.1:58155        LAB01:58154            ESTABLISHED
  TCP    192.168.1.2:57988      5.62.54.9:https        ESTABLISHED
  TCP    192.168.1.2:58013    a sea03-015.ff.avast.com:http  ESTABLISHED
  TCP    192.168.1.2:58190      104.250.52.104:https   TIME_WAIT
  TCP    192.168.1.2:58191      104.250.52.104:https   TIME_WAIT
```

Output listing open ports with domain names, a) Anti-virus software update from a server

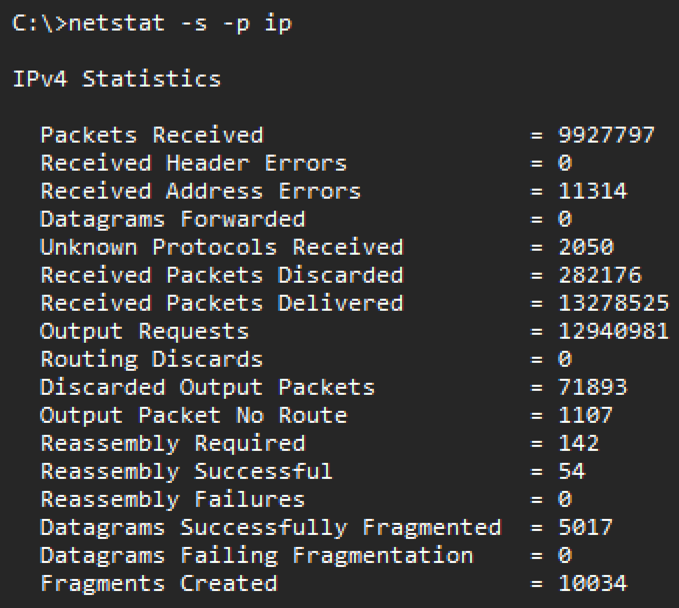
- View statistics (resolved to IP):
  - CMD > netstat -n



```
C:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:58143        127.0.0.1:58144        ESTABLISHED
  TCP    192.168.1.2:57988      5.62.54.9:443          ESTABLISHED
  TCP    192.168.1.2:58013      77.234.41.237:80       ESTABLISHED
  TCP    192.168.1.2:58161      54.203.20.58:443       ESTABLISHED
  TCP    192.168.1.2:58193      115.241.193.71:80      CLOSE_WAIT
  TCP    192.168.1.2:58194      104.250.52.104:443     TIME_WAIT
```

Output displaying resolved IP addresses

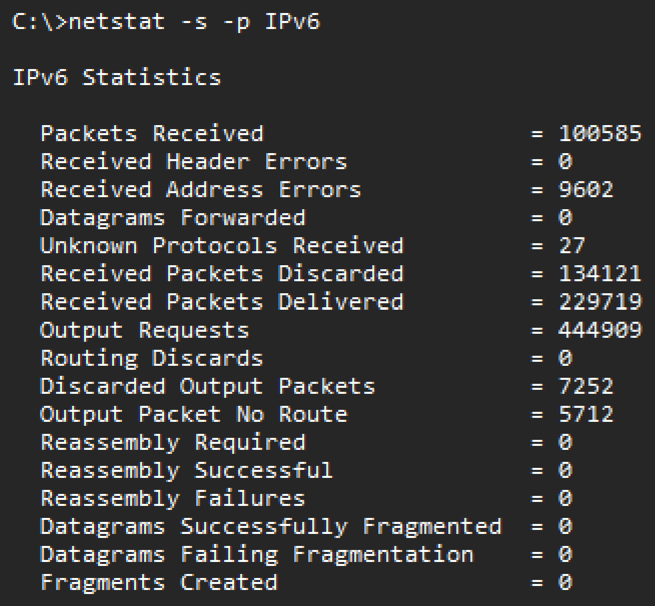
- View IPv4 Statistics:
  - CMD > netstat -s -p ip



```
C:\>netstat -s -p ip

IPv4 Statistics

  Packets Received                   = 9927797
  Received Header Errors             = 0
  Received Address Errors            = 11314
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 2050
  Received Packets Discarded         = 282176
  Received Packets Delivered         = 13278525
  Output Requests                    = 12940981
  Routing Discards                   = 0
  Discarded Output Packets           = 71893
  Output Packet No Route             = 1107
  Reassembly Required                = 142
  Reassembly Successful              = 54
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 5017
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 10034
```

Output listing IPv4 Statistics

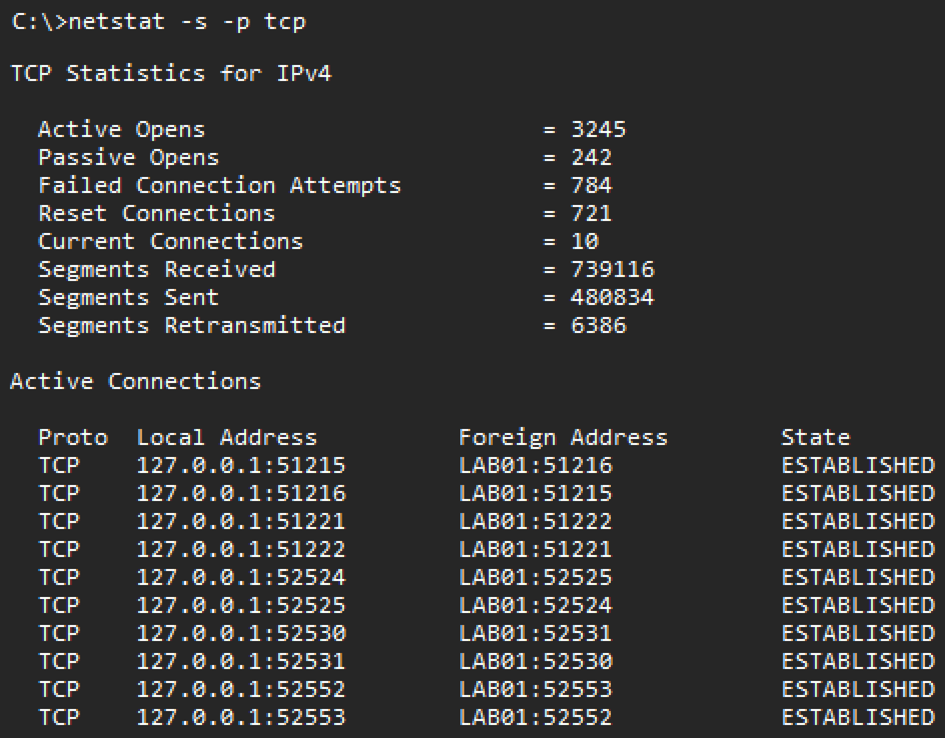
- View IPv6 Statistics:
  - CMD > netstat -s -p IPv6



```
C:\>netstat -s -p IPv6

IPv6 Statistics

  Packets Received                   = 100585
  Received Header Errors             = 0
  Received Address Errors            = 9602
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 27
  Received Packets Discarded         = 134121
  Received Packets Delivered         = 229719
  Output Requests                    = 444909
  Routing Discards                   = 0
  Discarded Output Packets           = 7252
  Output Packet No Route             = 5712
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

Output listing IPv6 Statistics

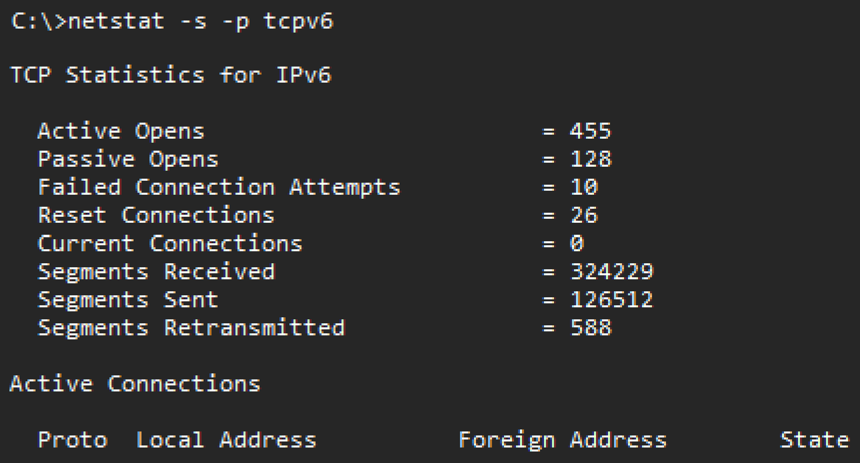
- View TCP Statistics for IPv4:
  - CMD > netstat -s -p tcp



```
C:\>netstat -s -p tcp

TCP Statistics for IPv4

  Active Opens                        = 3245
  Passive Opens                       = 242
  Failed Connection Attempts          = 784
  Reset Connections                   = 721
  Current Connections                 = 10
  Segments Received                   = 739116
  Segments Sent                       = 480834
  Segments Retransmitted              = 6386

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:51215        LAB01:51216            ESTABLISHED
  TCP    127.0.0.1:51216        LAB01:51215            ESTABLISHED
  TCP    127.0.0.1:51221        LAB01:51222            ESTABLISHED
  TCP    127.0.0.1:51222        LAB01:51221            ESTABLISHED
  TCP    127.0.0.1:52524        LAB01:52525            ESTABLISHED
  TCP    127.0.0.1:52525        LAB01:52524            ESTABLISHED
  TCP    127.0.0.1:52530        LAB01:52531            ESTABLISHED
  TCP    127.0.0.1:52531        LAB01:52530            ESTABLISHED
  TCP    127.0.0.1:52552        LAB01:52553            ESTABLISHED
  TCP    127.0.0.1:52553        LAB01:52552            ESTABLISHED
```

Output listing TCP, IPv4 Statistics

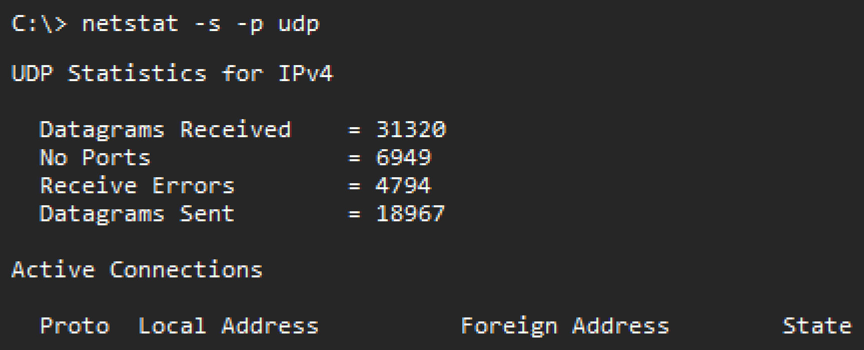
- View TCP Statistics for IPv6:
  - CMD > netstat -s -p tcpv6



```
C:\>netstat -s -p tcpv6

TCP Statistics for IPv6

  Active Opens                        = 455
  Passive Opens                       = 128
  Failed Connection Attempts          = 10
  Reset Connections                   = 26
  Current Connections                 = 0
  Segments Received                   = 324229
  Segments Sent                       = 126512
  Segments Retransmitted              = 588

Active Connections

  Proto  Local Address          Foreign Address        State
```

Output listing TCP, IPv6 Statistics

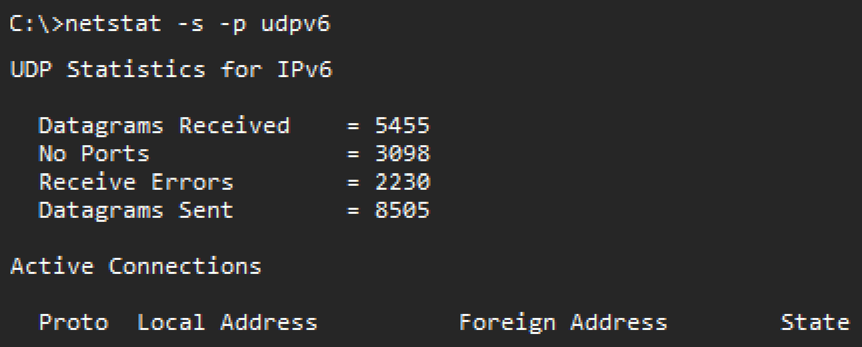
- View UDP Statistics for IPv4:
    - CMD > netstat -s -p udp



```
C:\> netstat -s -p udp

UDP Statistics for IPv4

  Datagrams Received    = 31320
  No Ports              = 6949
  Receive Errors        = 4794
  Datagrams Sent        = 18967

Active Connections

  Proto  Local Address          Foreign Address        State
```

Output listing UDP, IPv4 Statistics

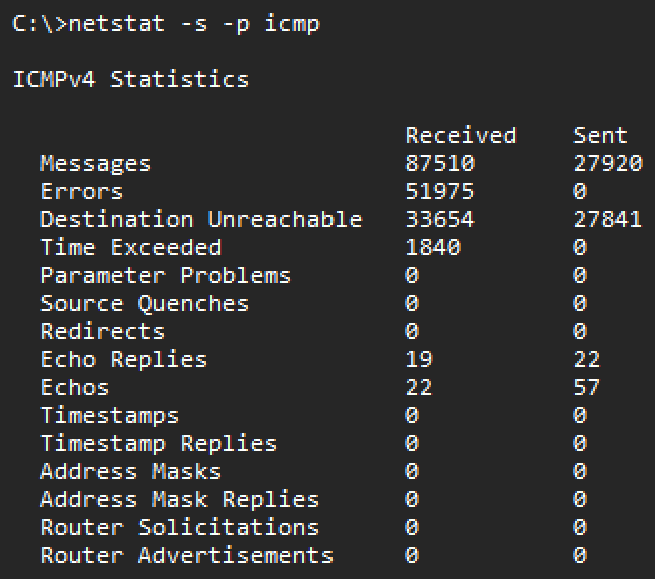
- View UDP Statistics for IPv6:
    - CMD > netstat -s -p udpv6



```
C:\>netstat -s -p udpv6

UDP Statistics for IPv6

  Datagrams Received    = 5455
  No Ports              = 3098
  Receive Errors        = 2230
  Datagrams Sent        = 8505

Active Connections

  Proto  Local Address          Foreign Address        State
```

Output listing UDP, IPv6 Statistics

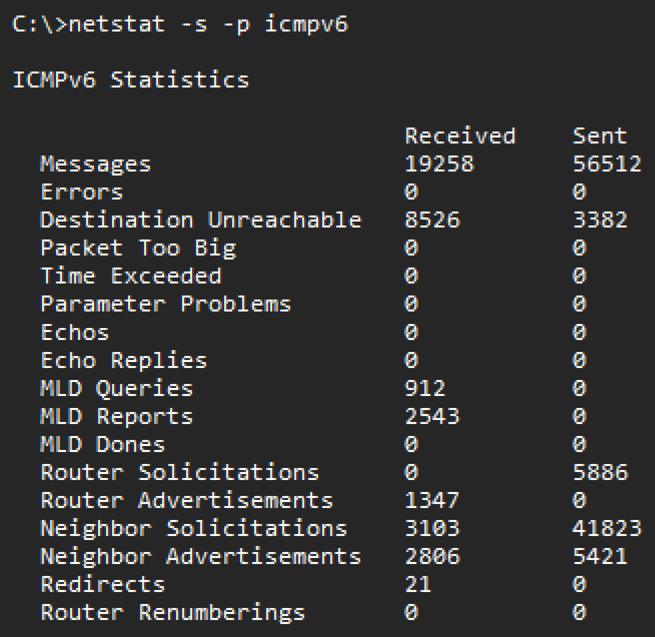
- View ICMP statistics (IPv4):
    - CMD > netstat -s -p icmp



```
C:\>netstat -s -p icmp

ICMPv4 Statistics

                            Received    Sent
  Messages                  87510       27920
  Errors                    51975       0
  Destination Unreachable   33654       27841
  Time Exceeded             1840        0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              19          22
  Echos                     22          57
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0
```

Output listing ICMP statistics for IPv4

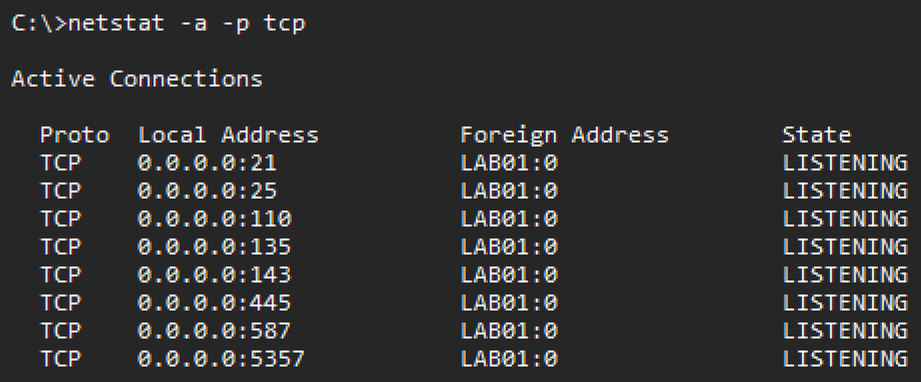
- View ICMP statistics (IPv6):
    - CMD > netstat -s -p icmpv6



```
C:\>netstat -s -p icmpv6

ICMPv6 Statistics

                            Received    Sent
  Messages                  19258       56512
  Errors                    0           0
  Destination Unreachable   8526        3382
  Packet Too Big            0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Echos                     0           0
  Echo Replies              0           0
  MLD Queries               912         0
  MLD Reports               2543        0
  MLD Dones                 0           0
  Router Solicitations      0           5886
  Router Advertisements     1347        0
  Neighbor Solicitations    3103        41823
  Neighbor Advertisements   2806        5421
  Redirects                 21          0
  Router Renumberings       0           0
```

Output listing ICMP statistics for IPv6

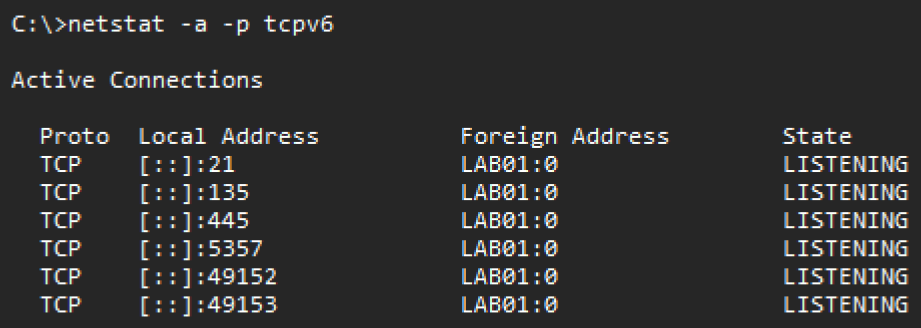
- View all Active TCP Connections for IPv4 (Open Ports):
  - CMD > netstat -a -p tcp



```
C:\>netstat -a -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             LAB01:0                LISTENING
  TCP    0.0.0.0:25             LAB01:0                LISTENING
  TCP    0.0.0.0:110            LAB01:0                LISTENING
  TCP    0.0.0.0:135            LAB01:0                LISTENING
  TCP    0.0.0.0:143            LAB01:0                LISTENING
  TCP    0.0.0.0:445            LAB01:0                LISTENING
  TCP    0.0.0.0:587            LAB01:0                LISTENING
  TCP    0.0.0.0:5357           LAB01:0                LISTENING
```

Output listing open TCP ports (IPv4)

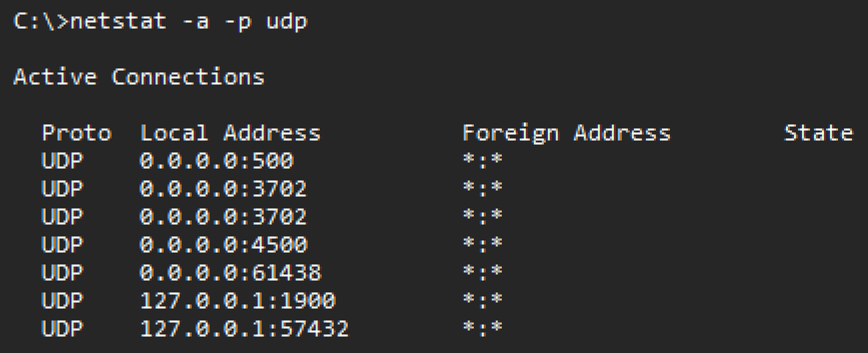
- View all Active TCP Connections for IPv6 (Open Ports):
  - CMD > netstat -a -p tcpv6



```
C:\>netstat -a -p tcpv6

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    [::]:21                LAB01:0                LISTENING
  TCP    [::]:135               LAB01:0                LISTENING
  TCP    [::]:445               LAB01:0                LISTENING
  TCP    [::]:5357              LAB01:0                LISTENING
  TCP    [::]:49152             LAB01:0                LISTENING
  TCP    [::]:49153             LAB01:0                LISTENING
```

Output listing open TCP ports (IPv6)

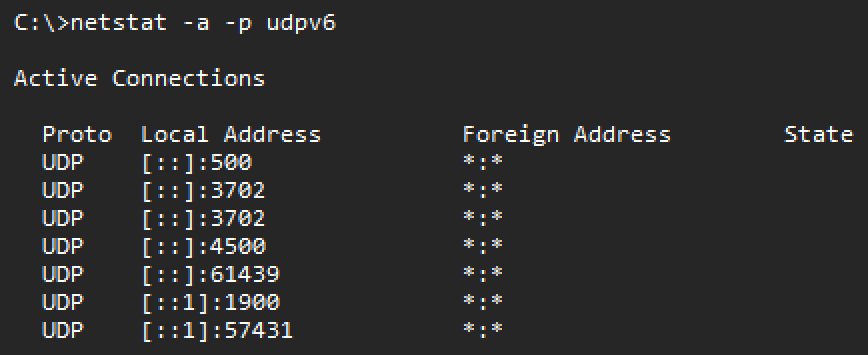
- View all Active UDP Connections for IPv4 (Open Ports):
  - CMD > netstat -a -p udp



```
C:\>netstat -a -p udp

Active Connections

  Proto  Local Address          Foreign Address        State
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:61438          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:57432        *:*
```

Output listing open UDP ports (IPv4)

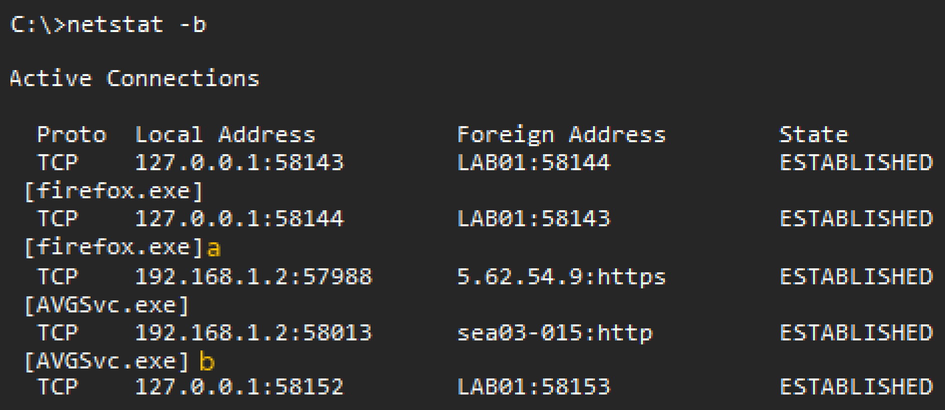
- View all Active UDP Connections for IPv6 (Open Ports):
  - CMD > netstat -a -p udpv6



```
C:\>netstat -a -p udpv6

Active Connections

  Proto  Local Address          Foreign Address        State
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:61439             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:57431            *:*
```

Output listing open UDP ports (IPv6)

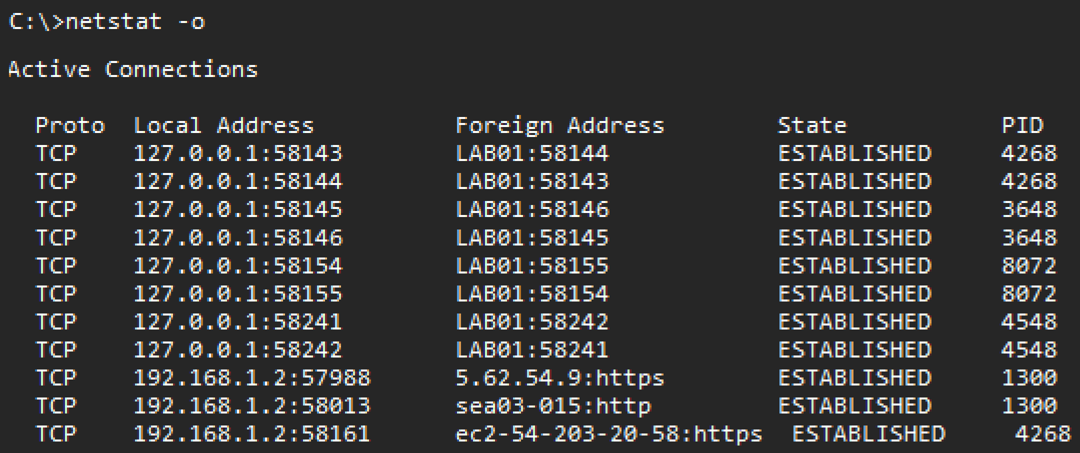
- View statistics (used by a particular executable):
  - CMD > netstat -b



```
C:\>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:58143        LAB01:58144            ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:58144        LAB01:58143            ESTABLISHED
 [firefox.exe]a
  TCP    192.168.1.2:57988      5.62.54.9:https        ESTABLISHED
 [AVGSvc.exe]
  TCP    192.168.1.2:58013      sea03-015:http         ESTABLISHED
 [AVGSvc.exe] b
  TCP    127.0.0.1:58152        LAB01:58153            ESTABLISHED
```

Output listing ports used by programs (executable) a) Mozilla Firefox & b) AVG Anti-virus update

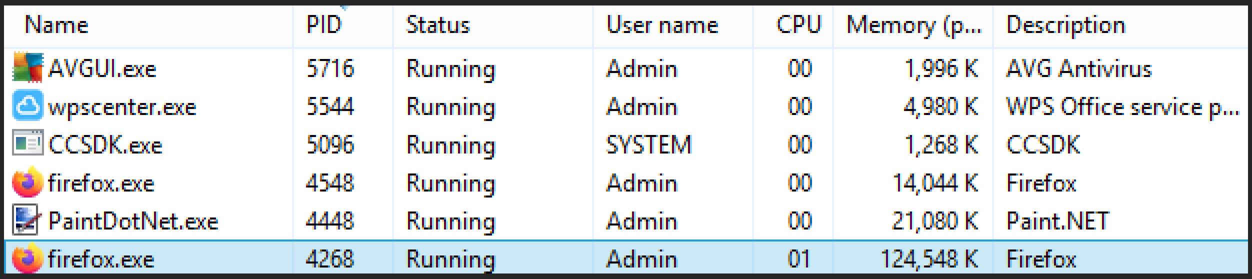
- View statistics (used by a particular executable by process ID):
  - CMD > netstat -o



```
C:\>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:58143        LAB01:58144            ESTABLISHED     4268
  TCP    127.0.0.1:58144        LAB01:58143            ESTABLISHED     4268
  TCP    127.0.0.1:58145        LAB01:58146            ESTABLISHED     3648
  TCP    127.0.0.1:58146        LAB01:58145            ESTABLISHED     3648
  TCP    127.0.0.1:58154        LAB01:58155            ESTABLISHED     8072
  TCP    127.0.0.1:58155        LAB01:58154            ESTABLISHED     8072
  TCP    127.0.0.1:58241        LAB01:58242            ESTABLISHED     4548
  TCP    127.0.0.1:58242        LAB01:58241            ESTABLISHED     4548
  TCP    192.168.1.2:57988      5.62.54.9:https        ESTABLISHED     1300
  TCP    192.168.1.2:58013      sea03-015:http         ESTABLISHED     1300
  TCP    192.168.1.2:58161      ec2-54-203-20-58:https  ESTABLISHED     4268
```

Output listing ports by process ID

- START > RUN > TASKMGR > Details Tab



Name	PID	Status	User name	CPU	Memory (p...	Description
AVGUI.exe	5716	Running	Admin	00	1,996 K	AVG Antivirus
wpscenter.exe	5544	Running	Admin	00	4,980 K	WPS Office service p...
CCSDK.exe	5096	Running	SYSTEM	00	1,268 K	CCSDK
firefox.exe	4548	Running	Admin	00	14,044 K	Firefox
PaintDotNet.exe	4448	Running	Admin	00	21,080 K	Paint.NET
firefox.exe	4268	Running	Admin	01	124,548 K	Firefox

Output listing Process Name, Process ID (Find matching process ID) in Task Manager

- View statistics for all protocols
    - CMD > netstat -e -s

To know if an existing port is used or not:

- CMD > netstat -an | findstr :23000

To view ephemeral port range:

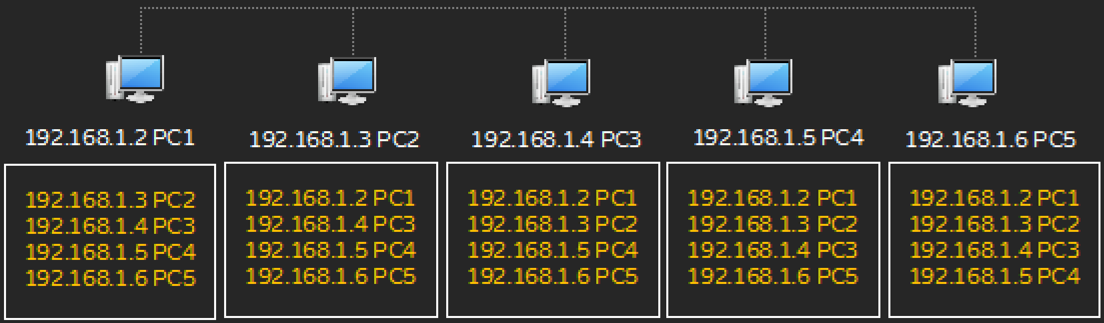
- CMD > netsh int ipv4 show dynamicport tcp
- CMD > netsh int ipv6 show dynamicport tcp

Name Resolution

- Friendly Names are used for identifying hosts in IP networks, instead of IP addresses. Friendly names must be resolved to IP address before communication.
- Name resolution is the process of resolving names to IP address (for example: LAB01 = 192.168.1.2 or www.example.com = 1.2.3.4).
- Multiple methods such as HOSTS, DNS, WINS, DDNS available for resolving names to IP address.

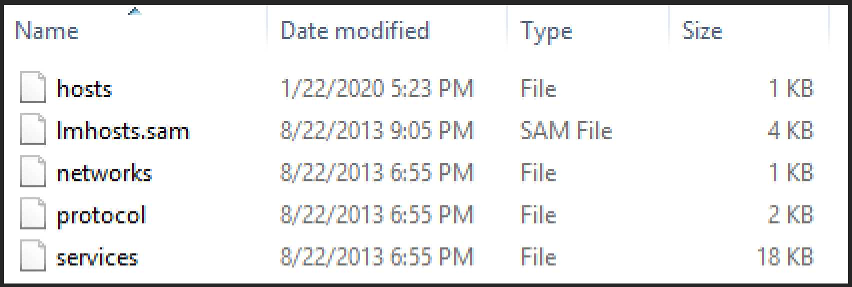
HOSTS

- Before DNS, name resolution was handled manually using a plain text file named HOSTS.
- HOSTS file has entries on each client about other clients name & IP address (Hence not suitable for medium or large networks as it is difficult to update all computers when there is a change).
- HOSTS file mechanism is still used for scenarios such as blocking unwanted websites, URLs, etc.



HOSTS File with proper entries must exist on all computers, similar to a personal phone book

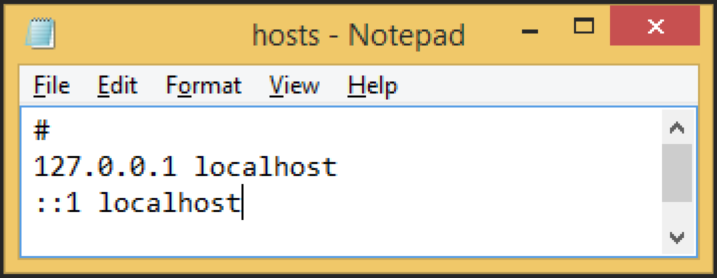
- View HOSTS file (Microsoft Windows)
  - Go to C:\Windows\System32\drivers\etc



Name	Date modified	Type	Size
hosts	1/22/2020 5:23 PM	File	1 KB
lmhosts.sam	8/22/2013 9:05 PM	SAM File	4 KB
networks	8/22/2013 6:55 PM	File	1 KB
protocol	8/22/2013 6:55 PM	File	2 KB
services	8/22/2013 6:55 PM	File	18 KB

Folder listing HOSTS & Other files; observe there is no file extension for "HOSTS"

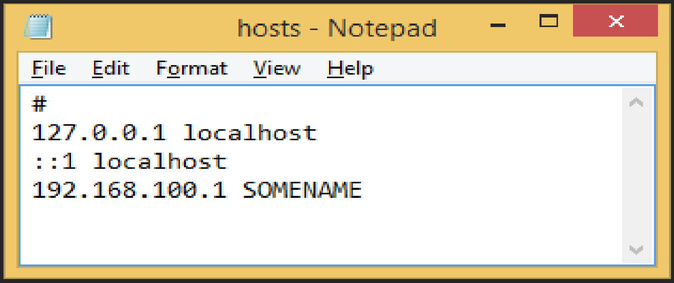
- Open HOSTS in a text editor



```
#
127.0.0.1 localhost
::1 localhost
```

Hosts file open in a text editor, observe existing entries

- To add Entries to a HOSTS file
  - BACKUP existing HOSTS file (Keep a copy elsewhere).
  - Open HOSTS file using a text editor.
  - Add 192.168.100.1 SOMENAME (example).

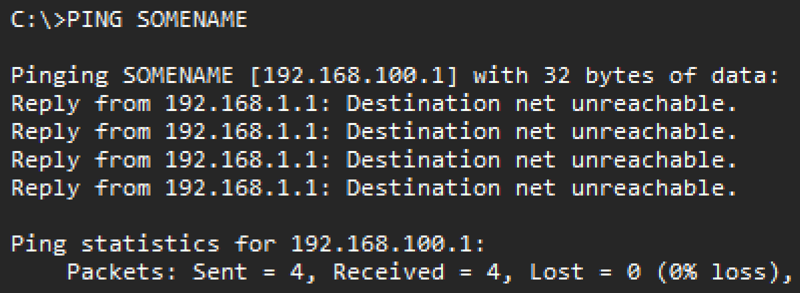


```
#
127.0.0.1 localhost
::1 localhost
192.168.100.1 SOMENAME
```

Sample input in a hosts file

Note: You may not be able to save the file to the same location due to security restrictions. However, you can copy the file to another location, add the necessary entries, and then overwrite the original file in C:\Windows\System32\drivers\etc. Be sure to take extra care to ensure that no extension, such as .txt, is automatically added when saving the file. The file must be named HOSTS, not hosts.txt.

- To test:
  - CMD > PING SOMENAME



```
C:\>PING SOMENAME

Pinging SOMENAME [192.168.100.1] with 32 bytes of data:
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

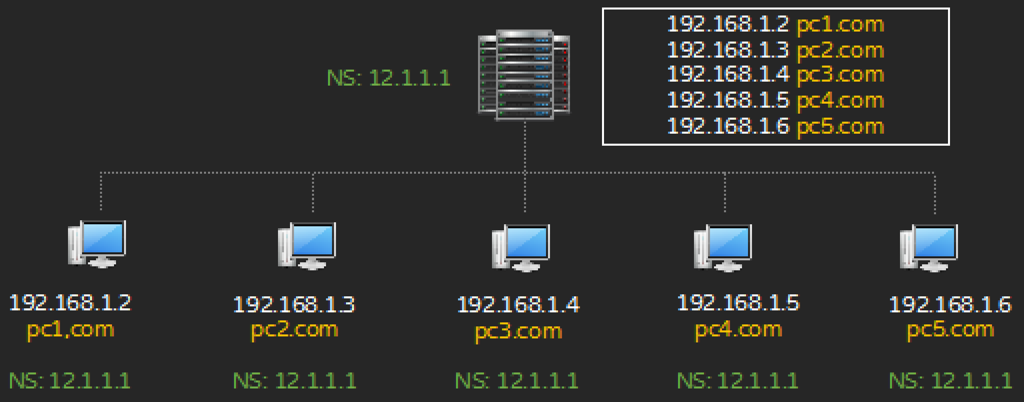
Observe computer name resolved to an IP and message indicating 192.168.100.x network not reachable

Tip: Hosts file can be used for pointing to unfriendly or difficult computer names on a LAN (for example, CORP044594 can be mapped to a friendly name JOESCOMPUTER in HOSTS file).

Note: Try other examples like 127.0.0.1 = SOMEOTHERNAME and so on.

DNS

- Domain Name System - Resolves domain names to IP address – allows users to access websites using human readable names (like www.example.com) instead of IP address.
- Hierarchical distributed naming system, scalable & efficient.
- Reduces administrative efforts, records are saved on a server instead of records on each computer.
- Client/Server Technology – client computers query DNS servers to resolve names to IP.



DNS entries are stored in a centralized database, similar to a telephone directory

DNS ZONES

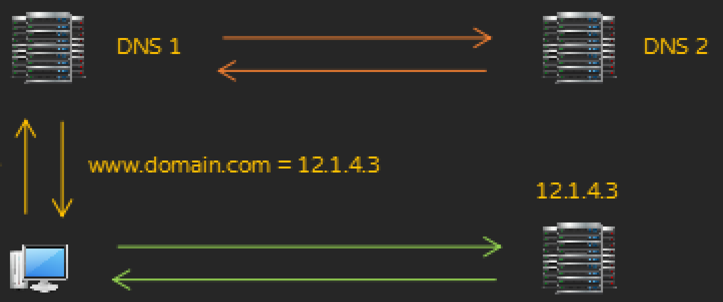
- Zone contains mapping of IP addresses to Domain names, used for DNS queries.
- Zone contains records in a well structured file (kind of text file) on DNS Servers referred to as “Zone” files.
- Zone files contains records such as:
  - NS Record: Name Server records, IP address of name servers for a domain.
  - SOA Record: Start Of Authority Record, the authoritative name server for a domain.
  - A Record: Mapping of IPv4 address to Domain Names (used for resolving domain names to IP addresses).
  - PTR Record: Used for reverse lookup (Resolving IP Address to Domain Names).
  - CNAME Record: Canonical Name record, mapping standard names to a domain name such as www, mail, ftp, etc (www.example.com).
  - AAAA Record: Mapping of IPv6 address.
  - MX Record: Mapping of Mail Servers for a domain.

DNS Servers

Typically there are at least two DNS servers:

- Primary DNS Server: First server that holds the records.
- Secondary DNS Server: Syncs from Primary DNS time-to-time, can serve as a backup for a Primary DNS Server.
- DNS records are synchronized within defined time, so either Primary or Secondary DNS server can respond to a client query as quick as possible and also serve as a backup if one DNS server fails or taken out for maintenance.

DNS Query Process



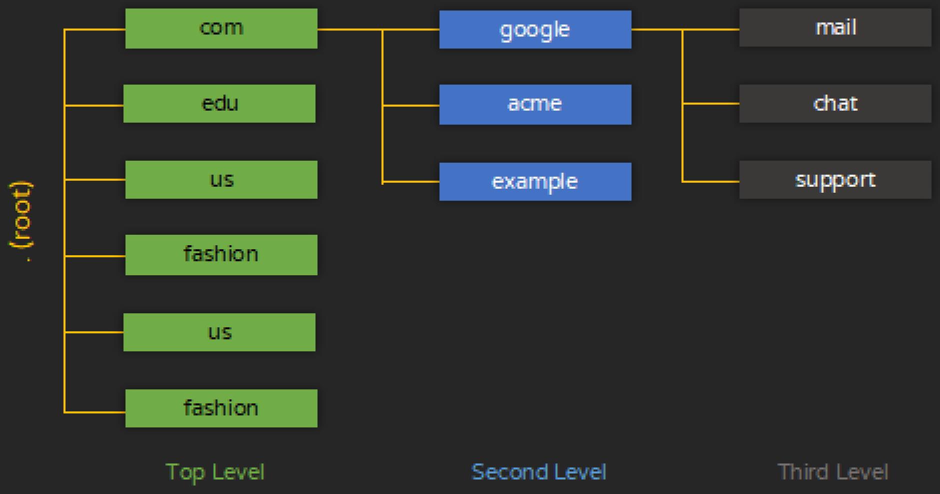
DNS Name Query Process example

1. Client sends DNS request to ISP’s DNS Server.
2. DNS Server replies with the corresponding IP address, if DNS 1 has the answer.
3. If DNS Server 1 doesn’t have the answer, then DNS Server 1 gets the answer from DNS server 2.
4. DNS Server 1 stores record in its Cache.
5. DNS Server 1 replies to Client.
6. Client receives and stores in local cache for subsequent actions (helps in reducing turn around time).

- Authoritative Name Servers: These servers have complete information about a specific domain and can provide the answer directly to a DNS client. (For example, DNS server 1 can respond directly if it's the authoritative server for the domain.)
- Non-Authoritative Name Servers: These servers query authoritative servers to provide answers to DNS clients. They may also respond with answers from their own cache if the information was retrieved from previous queries. (For example, DNS server 1 can get a reply from DNS server 2 if DNS server 2 is the authoritative server for the domain.)

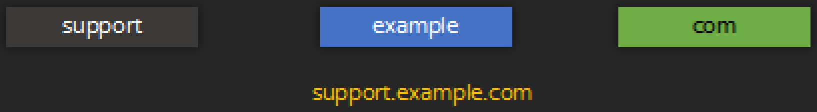
Domain Names

- Unique names, maximum 63 characters per label.
- Mapped to one or more IP addresses.
- Domain name records are stored on DNS servers.
- Domain names follow a hierarchical, multi-level structure.
- Domain names are leased (not owned) for periods of 1 year, 2 years, 3 years, or up to 10 years, and can be renewed thereafter.



Structure

- Domain names follow a tree structure starting with the root (represented as a dot . at the top). This is followed by – TLD, Second Level & Sub-domains.
- Top Level Domains are the highest, controlled by the IANA.
- Second Level Domains are leased through Domain Name Service Providers for a fee.
- Third Level Domains are created by Administrators (for free) - also referred to as “Sub domains”.



Fully Qualified Domain Name (FQDN) for above: support.example.com

Note: There are more than 1000+ TLD’s to choose from, and new TLD’s are being added. Customers may choose different TLD’s based on their business. For example a domain with .APP extension (TLD) may be selected if a customer plans to launch an Android or IOS App, a customer may select a domain name with .fashion extension if they are into garment business and so on. This is also useful in scenarios where a .COM or .NET extension is not available.

Reference(s):

- http://www.iana.org/domains/root/db/

Sub-Domains

Sub-domains are used for creating sections under a domain, for specific purposes.

For example:

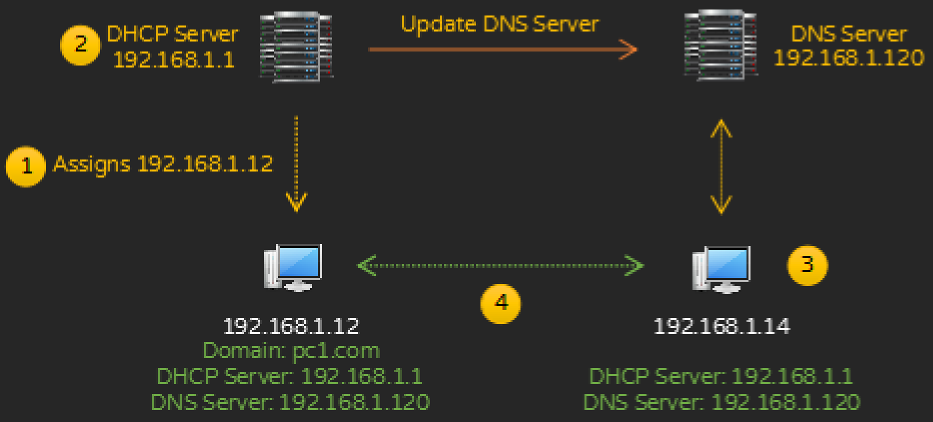
- mail.domainname.com for web mail access
- employee.domainname.com for employee access
- vendors.domainname.com for vendor portals
- dev.domainname.com for testing software
- api.domainname.com for service seperation

16777216 (2^{24})sub-domains can be created per domain at no additional cost, as it is controlled by the domain owner.

DDNS

- DDNS facilitates using dynamic IP address with domain names.
- DDNS (Dynamic DNS), allows automatic update of DNS records on DHCP environments.
- DDNS reduces administrative efforts, since IP assignments & name services are automated.

Note: DNS requires records to be created/updated manually (Static Entries) by an administrator; In DDNS environments, records are automatically updated by DHCP Server (Dynamic Entries). DNS is suitable only for static entries.



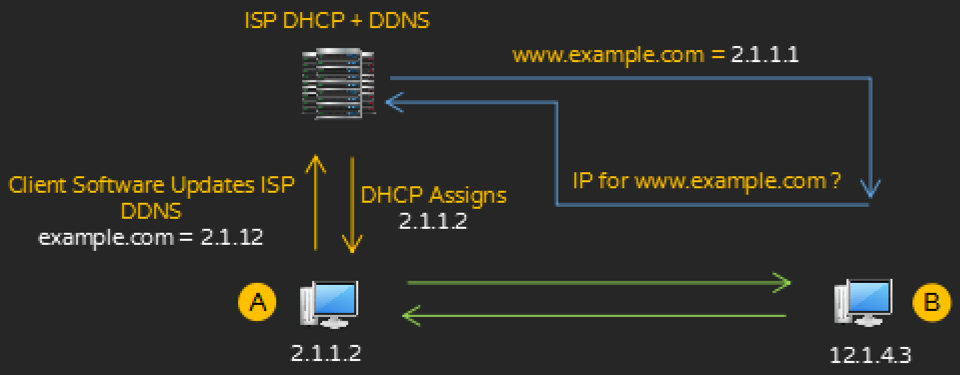
DDNS Process

Example:

1. DHCP Server assigns IP 192.168.1.12 to DHCP Client.
2. DHCP Server updates DNS Server 192.168.1.120 (pc1.com = 192.168.1.12).
3. Client (3) sends name resolution request for pc1.com to DNS Server 192.168.1.120.
4. DNS Server replies to Client with pc1.com’s IP address.
5. Client can communicate directly with 192.168.1.12.
6. If or when IP is changed for pc1.com, then DHCP Server updates DNS Server with new IP.

Internet Service Providers often issue dynamic IP addresses to client devices, due to limited number of IP addresses (IP address assigned to a computer may be assigned to another computer at random, during DHCP renewals or when reconnecting).

This makes it difficult for technical usage such as hosting a website which require a static IP address. Through DDNS, it is possible to host websites using dynamic IP address. DDNS is offered as a free or paid service by many service providers; such service providers offer client software which automatically updates IP address whenever there is a change.



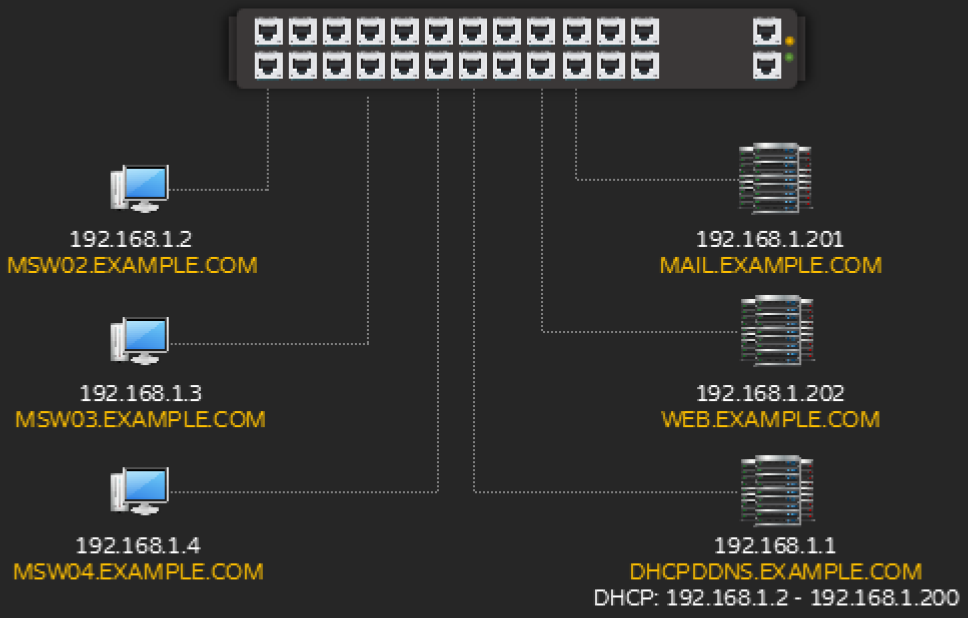
DDNS Example

Example:

1. ISP assigns a dynamic IP address to a computer A.
2. Client software installed on computer A updates DDNS server with the new IP address.
3. Client B queries the ISP's DDNS server to resolve the domain name associated with Computer A to an IP address.
4. The DDNS server replies to Client B with Computer A's current IP address.
5. Computer B communicates with Computer A using the resolved IP address.
6. ISP assigns a new dynamic IP address to the computer A.
7. Client software on Computer A updates DDNS server with the new IP address.
8. Computer B queries ISP's DDNS server.
9. The DDNS server responds with the updated IP address for Computer A.
10. Computer B communicates with Computer A through updated IP address.

Note: There is no guarantee a client will receive the same IP address during DHCP renewals, yet still can be accessible as DHCP/DDNS will point to the right computer/server.

DNS/DDNS is often used in enterprise networks, generally not visible to public. Many organizations use DNS structure for internal Information Technology requirements; for example client computers may be named like CORPDESK01.COMPANYNAME.LOCAL and servers may be named like SVR01.COMPANYNAME.LOCAL for internal identification purposes; client computers are usually assigned IP addresses through DHCP servers and servers may be assigned static IP addresses.



An enterprise network with multiple clients and servers

For example:

- Desktop clients are assigned IP addresses from DHCP Server 192.168.1.1.
- DHCP Server is set to allocate IP from range 192.168.1.2 to 192.168.1.200.
- Mail & Web Servers are assigned static IP addresses.
- DDNS service is enabled on DHCP Server.
- DHCP Server automatically updates DDNS.

Note: If IP addresses of MSW02/O3/04 changes, then it is automatically updated in DDNS

1. To communicate with WEB.EXAMPLE.COM, MSW04 sends a query to 192.168.1.1.
2. 192.168.1.1 replies to 192.168.1.4 with WEB.EXAMPLE.COM’s IP address.
3. 192.168.1.4 communicates with 192.168.1.202.

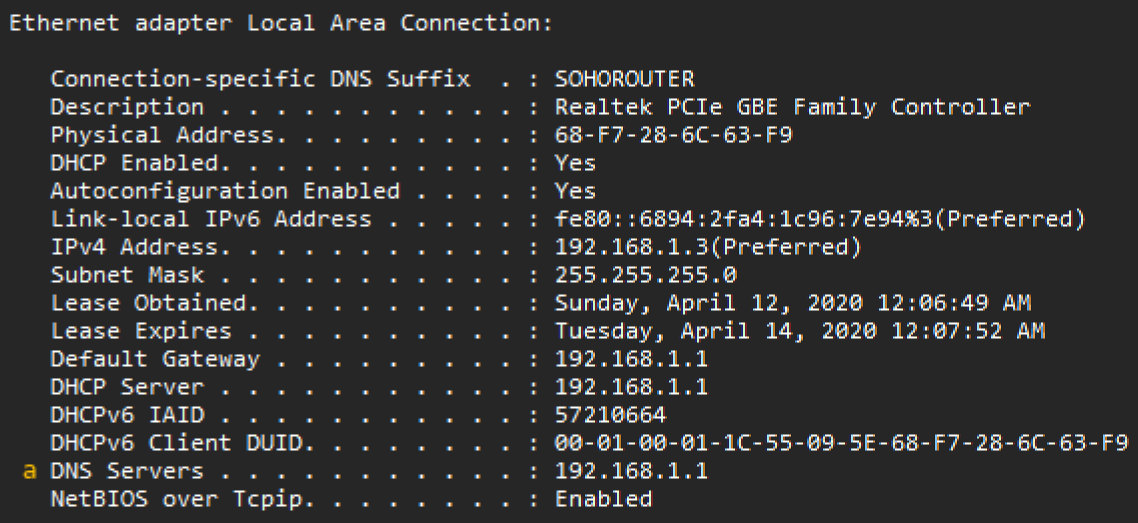
Similarly:

1. To communicate with MSW02.EXAMPLE.COM, MS04 sends a query to 192.168.1.1.
2. 192.168.1.1 replies to 192.168.1.2 with MSW02.EXAMPLE.COM’s IP address.
3. 192.168.1.4 communicates with 192.168.1.2.

Note: If there are on the same physical network, then IP addresses are resolved to MAC address.

Many companies use a naming convention based on the location of a client/server computer; for example: BL01F2DC05 (Building 01, 2nd Floor, Desktop Computer 05). This helps administrators locate computers easily, when physical attention is required.

- View DNS Server’s IP
    - CMD > ipconfig /all



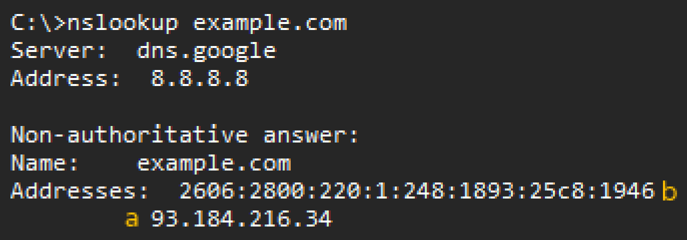
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : SOHOROUTER
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, April 12, 2020 12:06:49 AM
   Lease Expires . . . . . . . . . . : Tuesday, April 14, 2020 12:07:52 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
 a DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Output listing a) IP of DNS Server (in this case it’s the Routers IP address)

Note: DNS Server’s IP addresses are pushed along with IP address from a DHCP server to a client in most scenarios; DNS servers can also be set on each client manually as per administrator’s preference.

NSLOOKUP is a command line utility for querying DNS servers.

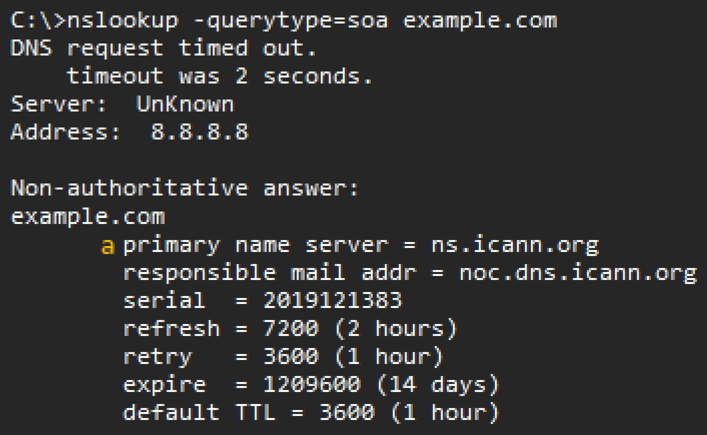
- View A (IPv4) & AAAA (IPv6) Record (IP Address) of a domain:
    - CMD > nslookup domainname



```
C:\>nslookup example.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    example.com
Addresses:  2606:2800:220:1:248:1893:25c8:1946 b
        a 93.184.216.34
```

Output listing resolved a) IPv4 & b) IPv6 addresses (if both are available)

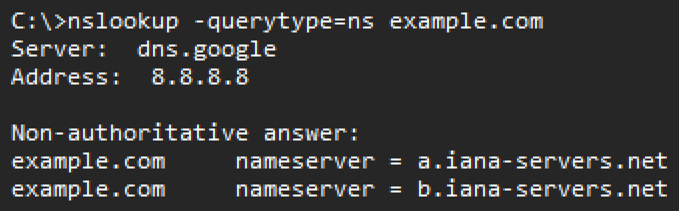
- View Authoritative DNS Server of a domain:
    - CMD > nslookup -querytype=soa domainname



```
C:\>nslookup -querytype=soa example.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  8.8.8.8

Non-authoritative answer:
example.com
      a primary name server = ns.icann.org
        responsible mail addr = noc.dns.icann.org
        serial  = 2019121383
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
```

Output a) listing primary name server (Authoritative) of a domain

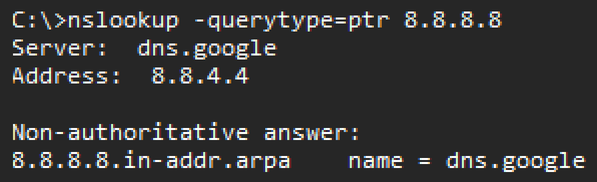
- View Name servers of a domain:
  - CMD > nslookup -querytype=ns domainname



```
C:\>nslookup -querytype=ns example.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
example.com     nameserver = a.iana-servers.net
example.com     nameserver = b.iana-servers.net
```

Output listing all name servers for a domain

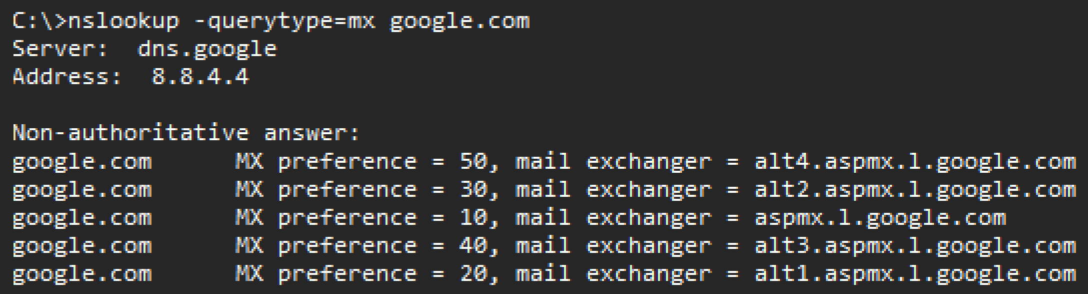
- View Domain Name from IP (Reverse Lookup):
  - CMD > nslookup -querytype=ptr IPADDRESS



```
C:\>nslookup -querytype=ptr 8.8.8.8
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = dns.google
```

Output listing domain name based on IP address

- View Mail Exchange record of a domain:
  - CMD > nslookup -querytype=mx domainname



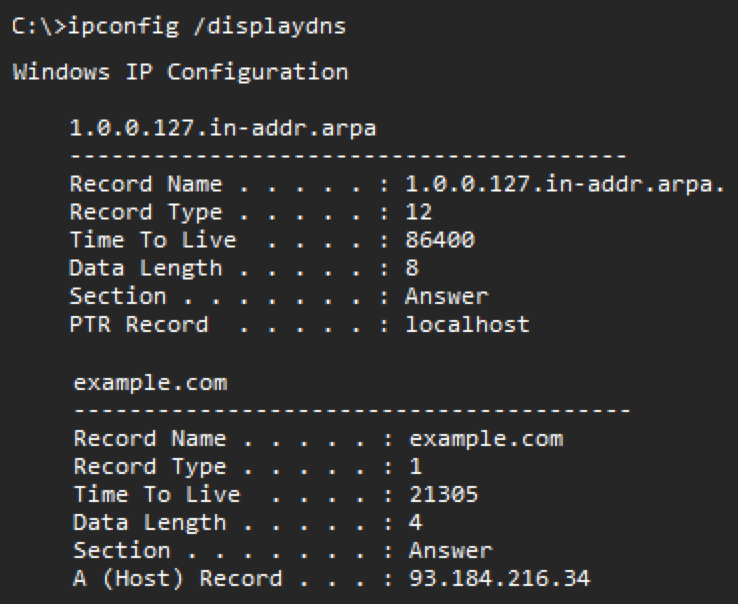
```
C:\>nslookup -querytype=mx google.com
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
```

Output listing mail server records for a given domain

Note: Settings such as port numbers for POP3, SMTP & IMAP can be viewed only through control panel of a domain.

Modern operating systems store cached copies of DNS queries (if visiting a website viewed earlier, client computers refer cache first instead of querying the DNS again, to save time & reduce network traffic):

- View DNS Cache (cached DNS queries):
    - CMD > ipconfig /displaydns

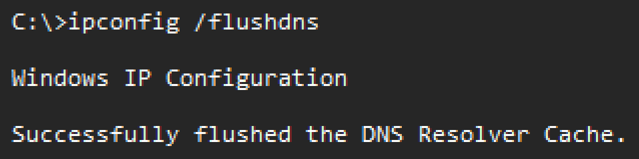


```
C:\>ipconfig /displaydns

Windows IP Configuration

    1.0.0.127.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 1.0.0.127.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 86400
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : localhost

    example.com
    ----------------------------------------
    Record Name . . . . . : example.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 21305
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 93.184.216.34
```

Output listing all resolved domain names & IP addresses available in local cache

Tip: Try viewing few websites using a web browser and observe entries in cache.

- Clear DNS Cache (removes all resolved domain names & IP addresses from DNS cache):
    - CMD > ipconfig /flushdns



```
C:\>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Input to clear DNS queries from local cache

Tip: Clear DNS cache once in a while, particularly if there are problems in resolving domain names (website not found) or internet related issues.

Note: Adding records to a DNS server requires a server operating system and it is currently not included in this guide.

LMHOSTS & WINS

- Similar to the HOSTS file, LMHOSTS (LAN Manager Hosts) is used for name resolution on Microsoft Windows systems, specifically for NetBIOS names (used in older Windows networking).
- Available only on Microsoft Windows Operating Systems.
- LMHOSTS file is located in the same folder as HOSTS file.

WINS

- Similar to DNS, Windows Internet Name Service is used for name resolution.
- Client/Server Technology.
- Available only on Microsoft Windows Operating Systems.
- WINS is depreciated.

Note: LMHOSTS/WINS are depreciated, hence not covered here.

Quiz 06

1. Features of UDP.

A. Connection-less & Unreliable   B. No sequencing
C. No acknowledgment or re-transmission   D. All of the above

2. Features of TCP.

A. Reliable & Connection-oriented   B. Sequencing
C. Flow Control and re-transmission   D. All of the above

3. Number of ports per IP address:

A. 16000   B. 65530   C. 65536   D. Unlimited

4. Well-known port numbers range:

A. 0-1024   B. 0-1023   C. 1024-49151   D. 12001-65535

5. Registered port numbers range:

A. 0-1024   B. 0-1023   C. 1024-49151   D. 12001-65535

6. Default port number for HTTP:

A. 8080   B. 80   C. 12000   D. 21

7. Default port number for FTP:

A. 8080   B. 80   C. 12000   D. 21

8. Default port number for POP3:

A. 20   B. 53   C. 110   D. 25

9. Default port number for SMTP:

A. 20   B. 53   C. 110   D. 25

10. Default port number for DNS:

A. 20   B. 53   C. 110   D. 25

11. Default port number for TELNET:

A. 23   B. 55   C. 443   D. 25

12. Default port number for HTTPS:

A. 23   B. 55   C. 443   D. 25

13. Command line utility for viewing network statistics:

A. ICMP   B. NETSTAT   C. NETVIEW   D. NET

14. Methods for name resolution:

A. HOSTS file B. LMHOSTS file C. DNS D. All of the above

15. Centralized name resolution methods:

A. DNS B. WINS C. DDNS D. All of the above

16. _____ naming resolution is used on networks utilizing dynamic IP addresses.

A. DNS B. WINS C. DDNS D. HOSTS

17. Location of HOSTS file in Microsoft Windows:

A. C:\Windows\System\Drivers\etc B. C:\Windows\System32\Drivers\etc
C. C:\Windows\System32\HOSTNAMES\ D. C:\Windows\etc

18. DNS utilizes a _____ naming system.

A. Symmetrical B. Hierarchical C. Asymmetrical D. Variable

19. Domain names are managed by:

A. IETF B. IEEE C. ICANN D. ISO

20. Acronym - ICANN.

A. Internet Corporation for Automated Names and Numbers
B. Intranet Corporation for Automated Names and Numbers
C. Internet Corporation for Assigned Names and Numbers
D. Intranet Corporation for Assigned Names and Numbers

21. Command line utility for querying DNS servers:

A. PING B. TRACERT C. NSLOOKUP D. NAMEDNS

22. Syntax for viewing DNS resolver cache:

A. NSLOOKUP /DNS B. IPCONFIG /DISPLAYDNS
C. IPCONFIG /FLUSHDNS D. NSLOOKUP /CACHE

23. Syntax for clearing DNS Cache:

A. NSLOOKUP /DNS B. IPCONFIG /DISPLAYDNS
C. IPCONFIG /FLUSHDNS D. NSLOOKUP /CACHE

24. ___ is used for secured transmissions.

A. SSL B. TLS C. DNS D. All of the above.

Wide Area Networks

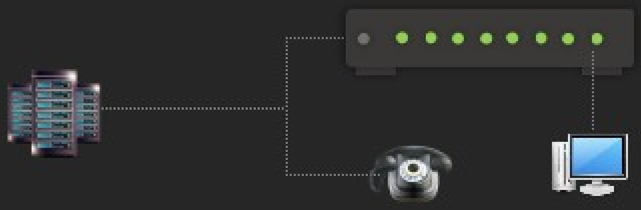
A Wide Area Network (WAN) spans large geographical areas, connecting multiple Local Area Networks (LANs) or providing access to the Internet. Establishing connectivity over long distances require specific technical infrastructure.

A. Dial-up Networking, DSL, Cable Internet, Wi-Max are some of the popular choices across home users, small & medium businesses for Internet access.
B. ISDN, Leased Lines are considered for medium to large office networks & service providers.

Wide Area Networks are used for establishing connectivity between LAN(s) across different locations and/or for providing access to the Internet.

Equipments used in WAN vary depending on requirements, costs & feasibility.

Dial-Up Networking



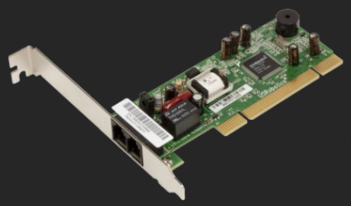
Internet connectivity using a Dial-up modem

- Popular for Internet Access and remote office network setups till early 2000's.
- Customers gain access to the Internet by dialing a phone number provided by the ISP.
- Users connect to remote networks by dialing a number provided by the office.
- Typical speeds around 56 Kbps.
- Either phone or modem can be used at one time, not both at the same time.
- Infrastructure
  - RAS (Remote Access Servers): Server Software, For accepting incoming connections.
  - DUN (Dial Up Networking): Client Software, for connecting to RAS.
- Uses PPP (Point-to-Point Protocol) or SLIP (Serial Line Internet Protocol).
- Internet connectivity is usually shared through 3rd party software during that time.
- Mostly replaced by Broadband technologies like DSL, Cable, etc. (in some countries Dial Up technology is still used).

Note: SLIP requires IP before connectivity, unlike PPP. PPP supersedes SLIP and PPP supports use of other protocols such as NETBEUI, IPX/SPX & DHCP environments.

MODEM (Modulator Demodulator)

- Simple device for connecting to remote networks using telephone networks.
- Available as Internal modems (for personal computers) & external models
- Converts Digital-to-Analog & Analog-to-Digital signals.



Internal Dial-Up MODEM

External Dial-Up MODEM

USB Dial-Up MODEM

- Internal Modems are inserted in PCI / PCIe slots.
- External Modems are connected through Serial Ports & USB ports.

Note: Do NOT confuse "Dial Up Modems" with DSL/Cable Modems.

ISDN

- ISDN (Integrated Services Digital Network) set of standards for digital transmission over PSTN.
- Used by companies for High speed, reliable & stable Internet connectivity (video conference, high speed internet access, etc.).
- ISDN requires specific hardware such as ISDN Modems & Routers which are quite expensive.
- ISDN hardware enables both digital voice and data services over the same line, making ISDN an efficient solution for businesses that need both.
- ISDN is usually offered as:
  - Basic Rate Interface: 2 B Channels (64 Kbps) + 1 D Channel (16 Kbps) =128 Kbps total
  - Primary Rate Interface: 23 B Channels (64 Kbps) + 1 D Channel (64 Kbps) = 1.5 Mbps total

Note: PRI/BRI implementations & plans vary country to country.

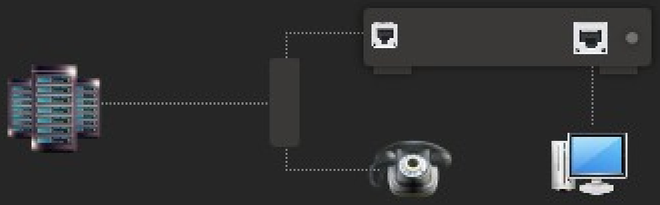
Leased Line

- "Leased Lines" refers to dedicated direct connections between ISP & Consumer, ensuring connectivity all the time.
- Usually expensive and require special hardware for network connectivity.

Reference(s):

https://en.wikipedia.org/wiki/Integrated_Services_Digital_Network
https://en.wikipedia.org/wiki/Leased_line

DSL



Internet connectivity using a DSL modem, DSL filter used for separating voice & data

- Digital Subscriber Line, widely popular for high speed Internet Access.
- Uses different frequencies for data & voice (hence the term "broadband"), allowing telephone & Internet usage at the same time.
- DSLAM used at service provider. DSL filter at customer's premises to split voice and data lines.
- Uses PPPoE (Point-to-Point Protocol Over Ethernet).

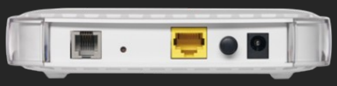
Note: DSL networks are "always connected", unlike in Dial-up networks where connectivity is available until user disconnects.

DSL implementations vary depending on country & provider, through technologies like:

- ADSL (Asymmetric DSL)
  - Download & Upload speeds are different.
  - Example: 10 Mbps download / 256 Kbps upload.
- SDSL (Symmetric DSL)
  - Downloads & Uploads are at same speeds.
  - Example: 10 Mbps download / 10 Mbps upload.

DSL MODEM

- Popular, simple & easy to use device, typically used to share Internet connectivity.
- DSL modems usually have one RJ-11 (WAN) for connecting to the ISP and, one or more RJ-45 (LAN) ports for LAN connectivity.
- May have additional features like Wi-Fi, Printer Sharing, USB ports, etc. depending on the model.



DSL MODEM

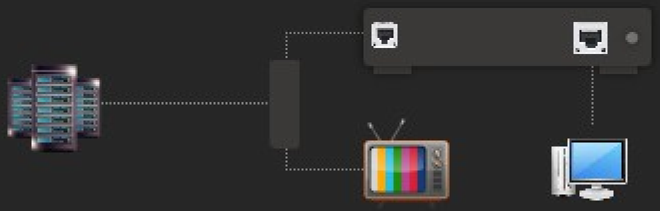
DSL ROUTER – DSL MODEM + 1 WAN Port / 4 LAN Ports + WI-FI

Reference(s):
https://en.wikipedia.org/wiki/DSL

Standards

Technology	Speed	
ADSL (G.lite)	1536/512 kbit/s	192/64 kB/s
HDSL ITU G.991.1 a.k.a. DS1	1544 kbit/s	193 kB/s
MSDSL	2000 kbit/s	250 kB/s
SDSL	2320 kbit/s	290 kB/s
SHDSL ITU G.991.2	5690 kbit/s	711 kB/s
ADSL (G.dmt) ITU G.992.1	8192/1024 kbit/s	1024/128 kB/s
ADSL2 ITU G.992.3	12288/1440 kbit/s	1536/180 kB/s
ADSL2+ ITU G.992.5	24576/3584 kbit/s	3072/448 kB/s
VDSL ITU G.993.1	52 Mbit/16Mbit/s	7 MB/s
VDSL2 ITU G.993.2	100 Mbit/s	12.5 MB/s
Uni-DSL	200 Mbit/s	25 MB/s
VDSL2 ITU G.993.2	300 Mbit/s	37.5 MB/s

Cable Internet



Internet connectivity using a Cable modem

- Uses cable television infrastructure for Internet access (broadband).
- A cable modem is used for managing connections.
- Usually has one CO-AXIAL connector (WAN) & one RJ-45 (LAN) Port.
- Co-Axial for connecting to ISP and RJ-45 port for connecting to LAN port (usually a computer).
- Follows DOCSIS (Data Over Cable Service Interface Specification) standards.

Cable MODEM

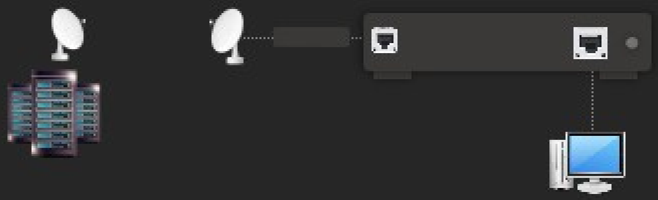
Reference(s):

https://en.wikipedia.org/wiki/Cable_Internet

Standards

Technology	Speed	
DOCSIS 1.0	38/9 Mbit/s	4.75/1.125 MB/s
DOCSIS 2.0	38/27 Mbit/s	4.75/3.375 MB/s
DOCSIS 3.0	1216/216 Mbit/s	152/27 MB/s
DOCSIS 3.1	10/2 Gbit/s	1.25/0.25 GB/s
DOCSIS 3.1 Full Duplex	10/10 Gbit/s	1.25/1.25 GB/s

WiMAX



Internet connectivity using WiMAX setup

- Worldwide interoperability for Microwave Access.
- Wireless Internet Access, alternate to DSL or Cable.
- “Last Mile” solution (where cable network access is NOT possible at all).
- Follows IEEE 802.16 Standard.
- Range up to 50 KM.
- Speed up to 70Mbit/s (depending on implementation & service provider).

WiMax Dish Antenna

WiMax Parabollic Antenna

Reference(s):

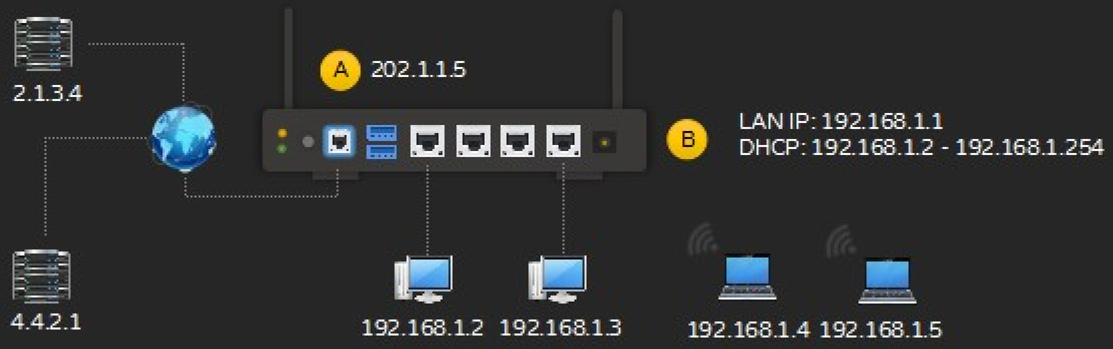
https://en.wikipedia.org/wiki/WiMAX

NAT (Concept)

- Network Address Translation (NAT) - Process of remapping IP addresses.
- Popular example is when an Internet connection is shared (Private to Public & Public to Private IP are remapped in IP address header).
- Implemented through Software or Hardware.
- Widely implemented in SOHO Routers, Internet Sharing & Metering Software, etc. where there are multiple clients with private IP addresses and one public IP address provided by the ISP.

NAT Device has:

A. WAN Interface: For connecting to outside world through DSL, Cable, Dial-Up, etc. (Public IP).
B. LAN Interface: For providing connectivity to devices such as desktops, laptops, etc. (Private IP).



NAT - A. One Public IP & B. Multiple Private IPs

Typically only one Public IP address is assigned by an ISP for every Internet connection; public IP address provided by the ISP is assigned to the WAN port of a Router. Private IP addresses are assigned by the Router to clients connected to it (through wired or Wi-Fi).

For example:

ISP assigns public IP 202.1.1.5.
Router’s LAN IP is set as 192.168.1.1.
Router’s DHCP range is set as 192.168.1.2 to 192.168.1.254.
Router assigns IP addresses to it’s clients from the DHCP pool.

1. 192.168.1.2 sends a request to 2.1.3.4
2. LAN interface on the Router assigned with IP 192.168.1.1 receives the request
3. NAT software on the Router replaces 192.168.1.2 with 202.1.1.5 and sends the request to 2.1.3.4
4. 2.1.3.4 replies to 202.1.1.5
5. NAT software replaces 202.2.1.5 with 192.168.1.1 based on its NAT table
6. Reply sent to 192.168.1.2 from 192.168.1.1

Types of NAT

Static NAT

- One-to-One Mapping
- One private IP address to a specific public IP address
- Often used when a specific service (web server or a email server) needs to be accessed from external public network

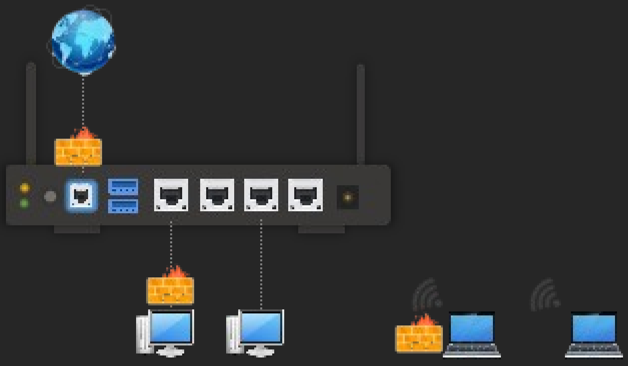
Dynamic NAT

- Private IP addresses are mapped to a pool of public IP addresses
- Used when the organization has more private IP addresses than public IP addresses available

PAT (Port Address Translation)

- Most common form of NAT, used in home and small office networks
- Allows multiple devices on a local network to share one public IP address by differentiating traffic using unique ports

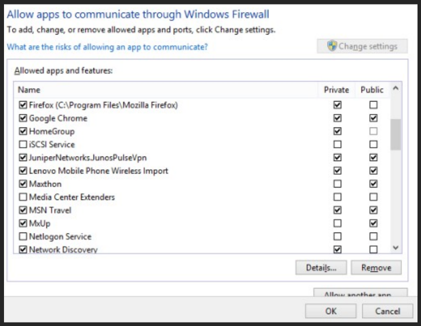
Firewall



Firewall in a router & Software Firewall on computers

- Protects computers & networks (Network Level).
- Monitors & controls incoming & outgoing network traffic.
- Works based on predefined rules, analyzes packets and allows/rejects.
- Essential to keep out unwanted traffic or users outside of a network or computer.
- Hardware or Software based.
- Some Operating Systems, Anti-Virus & NAT software include firewall as a feature.
- Types
  - Personal Firewall
    - Designed for controlling network traffic on a single computer.
    - Personal firewalls are usually configured automatically, require technical expertise for finer control.
  - Enterprise Firewall
    - Designed for controlling traffic across network of computers.
    - Enterprise firewalls require specific technical expertise based on the model.

Note: Firewall is NOT an Anti-Virus Software; Firewall protects only network traffic.



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

Name	Private	Public
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	□
☑ Google Chrome	☑	☑
☑ HomeGroup	☑	□
□ iSCSI Service	□	□
☑ JuniperNetworks.JunosPulseVpn	☑	☑
☑ Lenovo Mobile Phone Wireless Import	☑	☑
☑ Maxthon	□	☑
□ Media Center Extenders	□	□
☑ MSN Travel	☑	☑
☑ MxUp	□	☑
□ Netlogon Service	□	□
☑ Network Discovery	☑	□

Software Firewall

Hardware Firewall

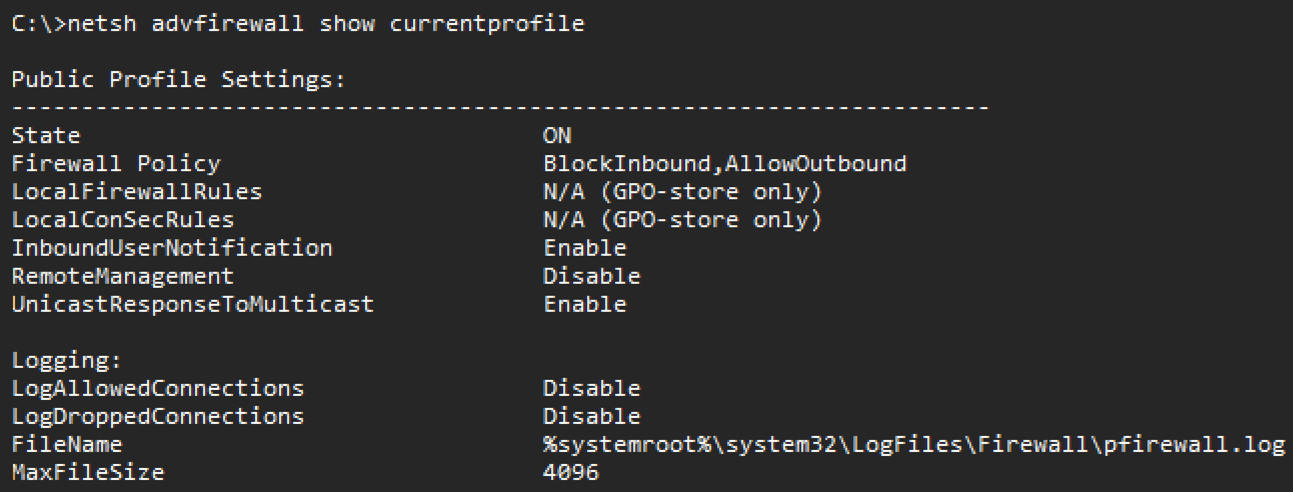
Note: It is recommended to keep one personal firewall active, if there are multiple software firewalls installed on a computer to avoid firewall conflicts.

Microsoft Windows Firewall is a software component that includes most firewall functions.

Manage Windows Firewall Settings

Tip: Microsoft Windows applies different firewall policies according to the network type; domain (for enterprise environments), public (hotspots, restaurants, etc.) & private (office or home network). Users may switch to different profiles as required by just selecting the type of network (in turn appropriate firewall profile is applied); profiles may be modified according to user's preference, for example allow specific applications only on an office network and block all other applications thereby increasing security measures.

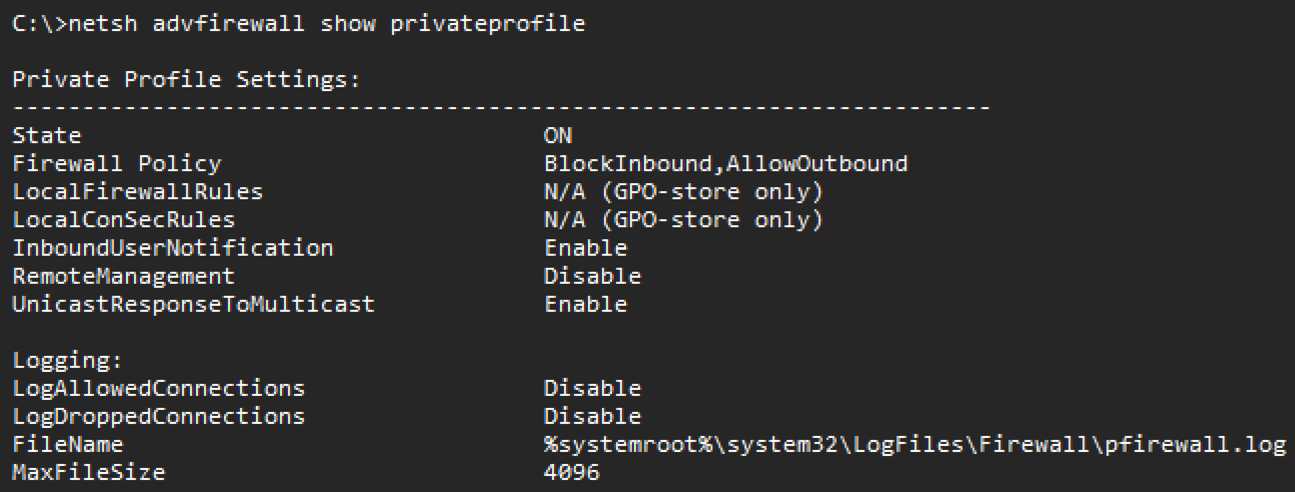
- View status of current profile:
    - CMD > netsh advfirewall show currentprofile



```
C:\>netsh advfirewall show currentprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

Output listing currently active profile (based on currently logged on user account)

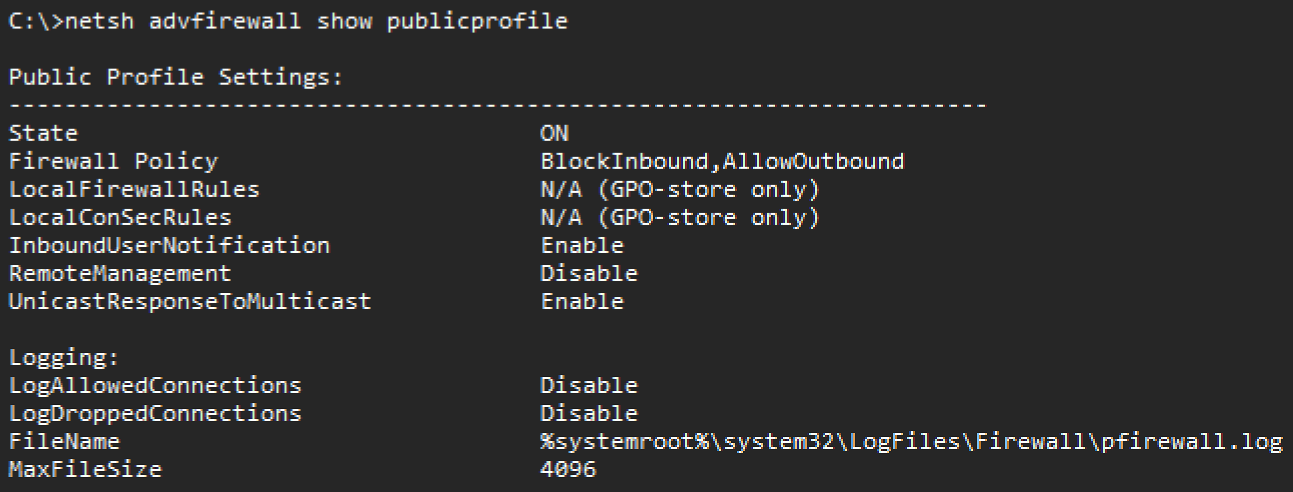
- View status of Private Network:
    - CMD > netsh advfirewall show privateprofile



```
C:\>netsh advfirewall show privateprofile

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

Output listing settings applicable for a private (LAN) network

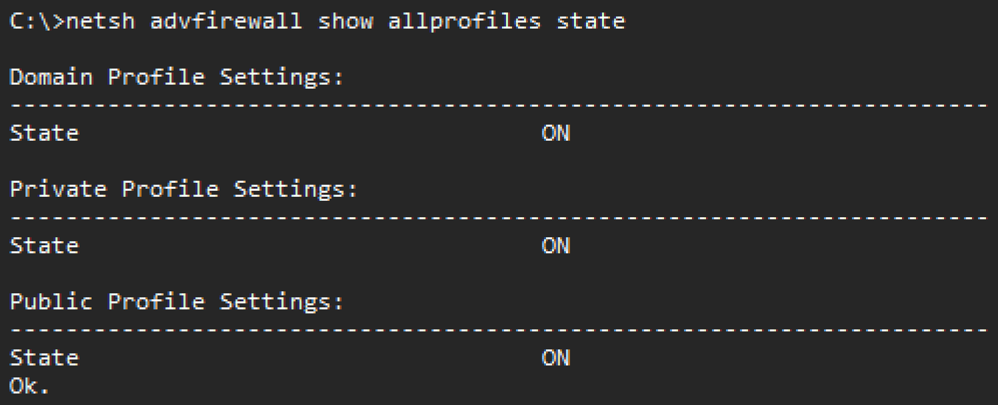
- View status of Public Network:
    - CMD > netsh advfirewall show publicprofile



```
C:\>netsh advfirewall show publicprofile

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

Output listing settings applicable for a public (Internet) network

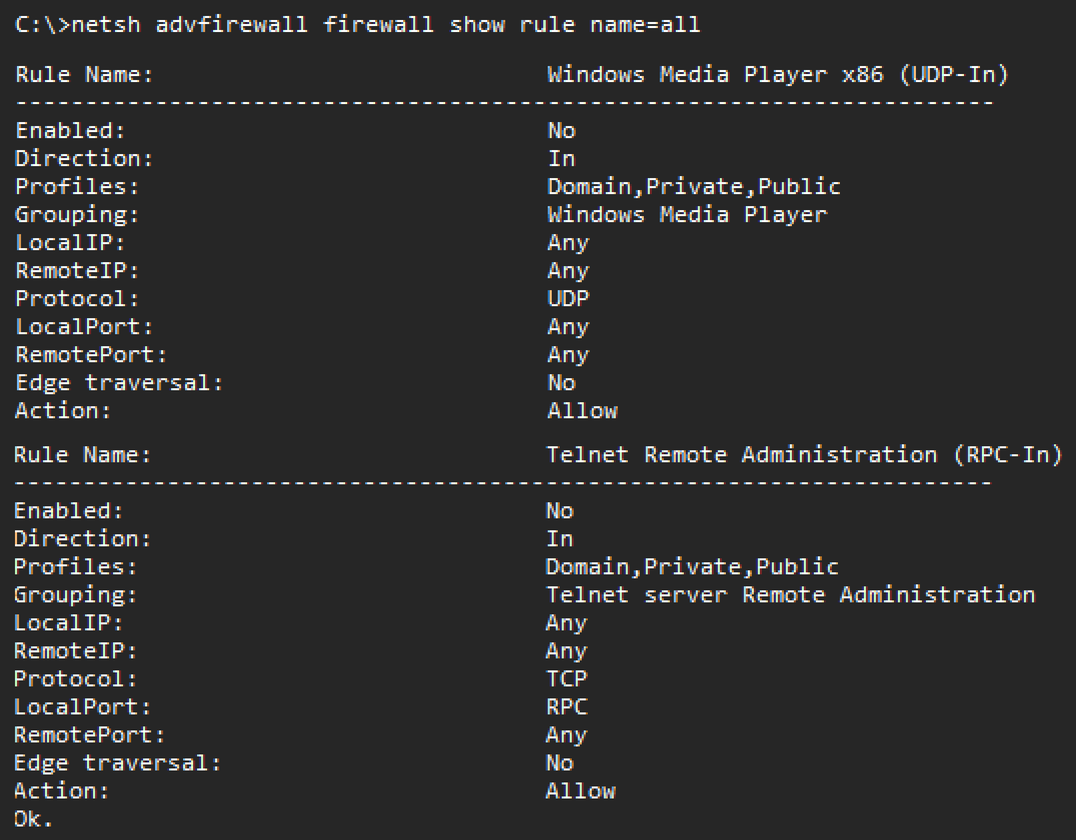
- View status of Windows Firewall for all connections
    - CMD > netsh advfirewall show allprofiles state



```
C:\>netsh advfirewall show allprofiles state

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON

Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Ok.
```

Output displaying status of Windows Firewall

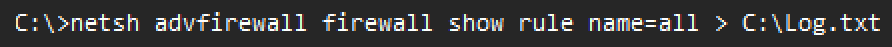
- View list of Applications & Services and, their status in Windows Firewall Profiles
  - CMD > netsh advfirewall firewall show rule name=all



```
C:\>netsh advfirewall firewall show rule name=all

Rule Name:                            Windows Media Player x86 (UDP-In)
----------------------------------------------------------------------
Enabled:                              No
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Windows Media Player
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             UDP
LocalPort:                            Any
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow

Rule Name:                            Telnet Remote Administration (RPC-In)
----------------------------------------------------------------------
Enabled:                              No
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             Telnet server Remote Administration
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            RPC
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow
Ok.
```

Output listing application & service status in Windows Firewall

  - Store all details in a Text file:
    - CMD > netsh advfirewall firewall show rule name=all > C:\Log.txt

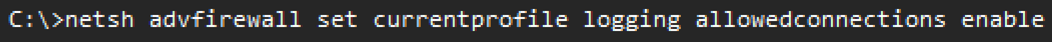


```
C:\>netsh advfirewall firewall show rule name=all > C:\Log.txt
```

Store output in text file

  - View Log.txt in a text editor.

- Enable logging in Windows Firewall for allowed software
  - CMD > netsh advfirewall set currentprofile logging allowedconnections enable

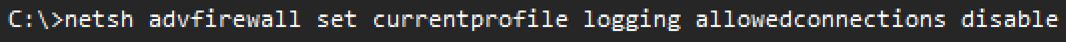


```
C:\>netsh advfirewall set currentprofile logging allowedconnections enable
```

Input to enable logging for allowed connections

  - Open Log File in a text editor to view: C:\Windows\System32\LogFiles\Firewall\pfirewall.log

- DISABLE logging in Windows Firewall
  - CMD > netsh advfirewall set currentprofile logging allowedconnections disable



```
C:\>netsh advfirewall set currentprofile logging allowedconnections disable
```

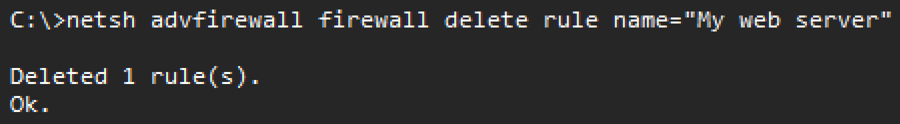
Input to disable logging for allowed connections, if enabled earlier

- Add a program to Windows Firewall using Port Number
  - CMD > netsh advfirewall firewall add rule name=”RULENAME” dir=in action=allow protocol=tcp localport=portnumber

```
C:\netsh advfirewall firewall add rule name=”My web server” dir=in action=allow
                         protocol=tcp localport=8080
```

Sample input to add an exception using Port number

- Remove a program from Windows Firewall
  - CMD > netsh advfirewall firewall delete rule name=”RULENAME”



```
C:\>netsh advfirewall firewall delete rule name="My web server"

Deleted 1 rule(s).
Ok.
```

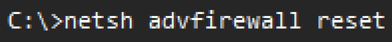
Input for deleting a rule, output with confirmation

- Add an exception by using an executable
  - CMD > netsh advfirewall firewall add rule name=”RULENAME” dir=in action=allow program=”path\program.exe” enable=yes

```
C:\netsh advfirewall firewall add rule name=”Allow TCPVIEW” dir=in action=allow
                  program=”c:\Tools\TCPView.exe” enable=yes
```

Input to add an executable to Windows Firewall

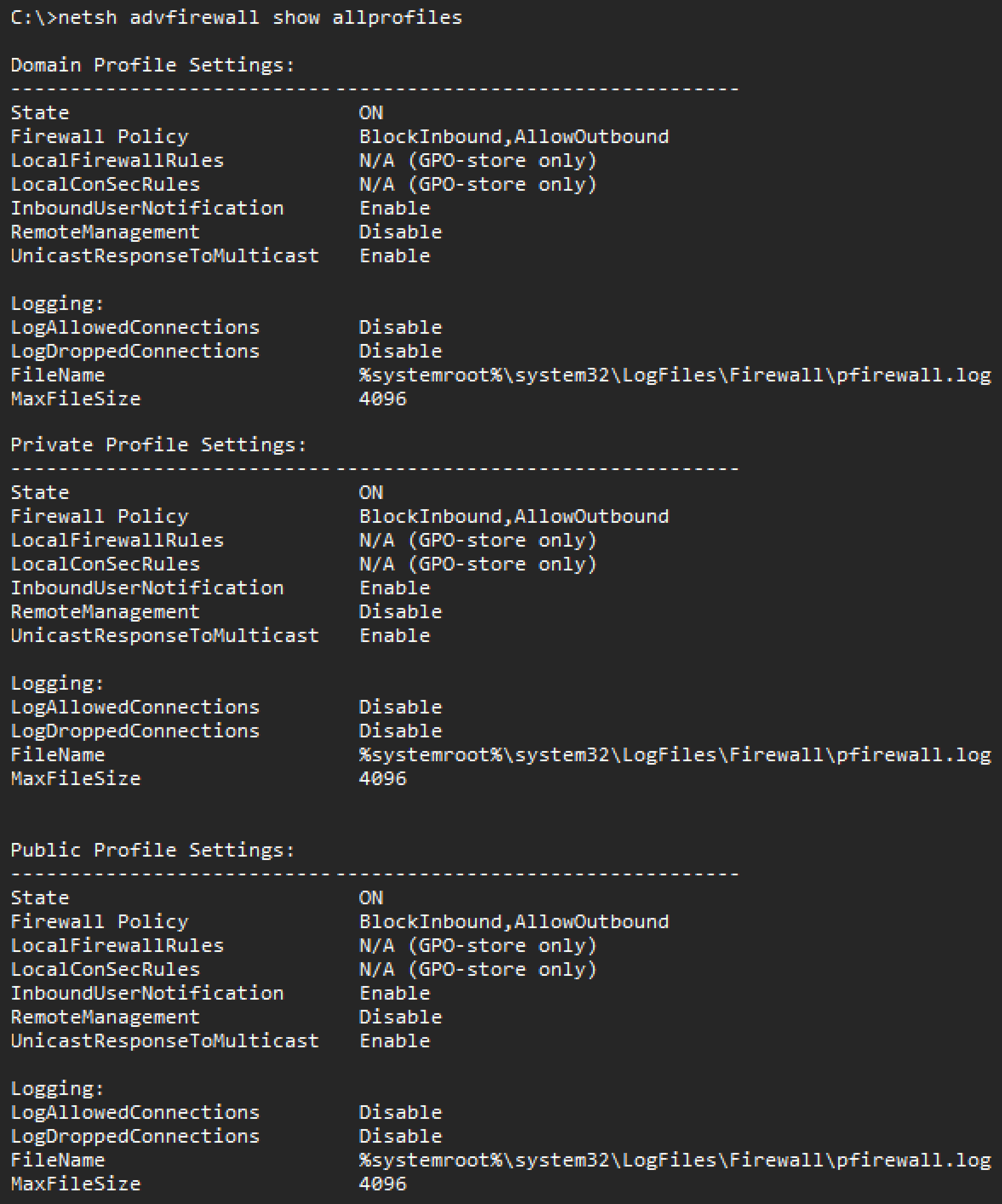
- Reset Windows Firewall to default settings
  - CMD > netsh advfirewall reset



```
C:\>netsh advfirewall reset
```

Input to reset Windows Firewall

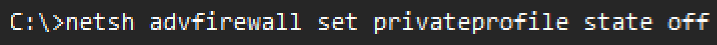
- View complete details:
    - CMD > netsh advfirewall show allprofiles



```
C:\>netsh advfirewall show allprofiles

Domain Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Public Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096
```

Firewall status for all connections

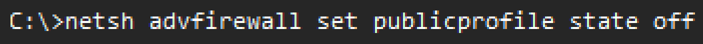
- Turn Off Firewall for Private Network:
  - CMD > netsh advfirewall set privateprofile state off



```
C:\>netsh advfirewall set privateprofile state off
```

Input to disable firewall for private profile

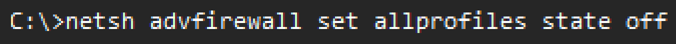
- Turn Off Firewall for Public Network:
  - ◆ CMD > netsh advfirewall set publicprofile state off



```
C:\>netsh advfirewall set publicprofile state off
```

Input to disable firewall for public profile

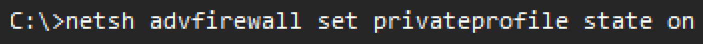
- Turn Off Firewall Both Networks:
  - ◆ CMD > netsh advfirewall set allprofiles state off



```
C:\>netsh advfirewall set allprofiles state off
```

Input to disable firewall for both private & public profiles

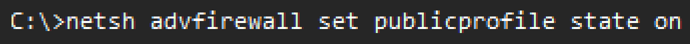
- Turn On Firewall for Private Network:
  - ◆ CMD > netsh advfirewall set privateprofile state on



```
C:\>netsh advfirewall set privateprofile state on
```

Input to enable firewall for private profile

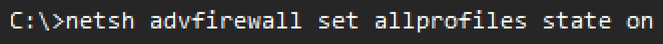
- Turn On Firewall for Public Network:
  - ◆ CMD > netsh advfirewall set publicprofile state on



```
C:\>netsh advfirewall set publicprofile state on
```

Input to enable firewall for public profile

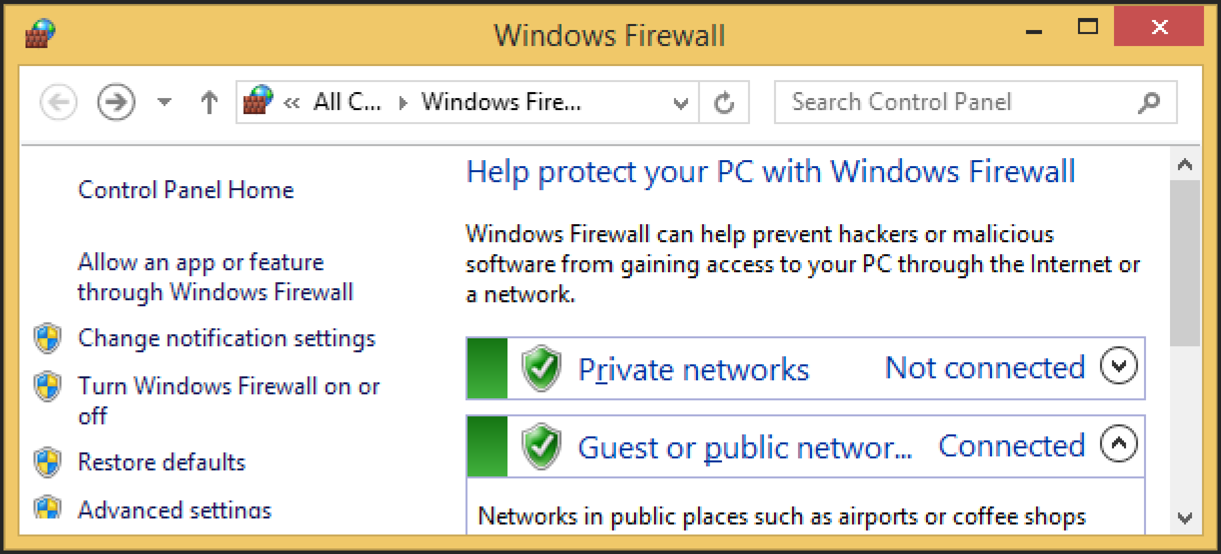
- Turn On Firewall for Both Networks:
  - ◆ CMD > netsh advfirewall set allprofiles state on



```
C:\>netsh advfirewall set allprofiles state on
```

Input to enable firewall for both private & public profiles

- View Firewall Settings (GUI)
  - START > RUN > FIREWALL.CPL


Windows Firewall
« All C... ▸ Windows Fire...
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

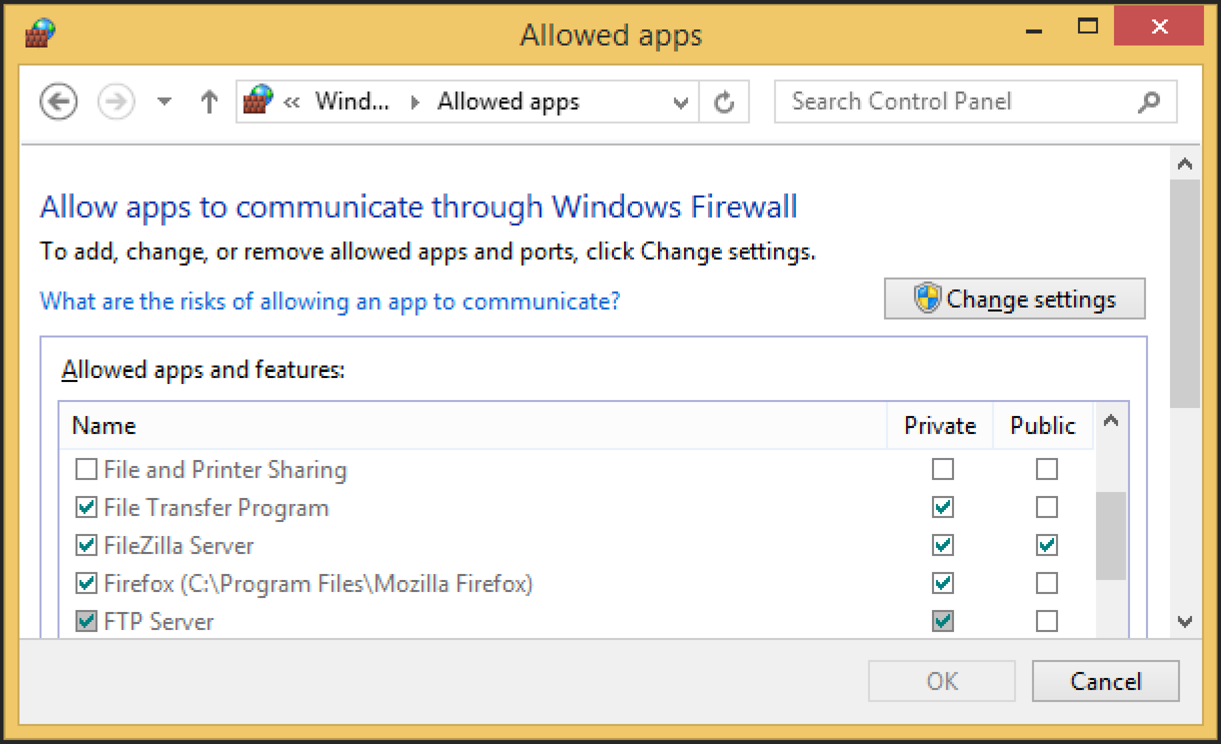
Private networks — Not connected

Guest or public networ... — Connected

Networks in public places such as airports or coffee shops

Windows Firewall

- Add/remove programs or services to Windows Firewall
  - Select "Allow an app or feature through Windows Firewall" from left menu



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

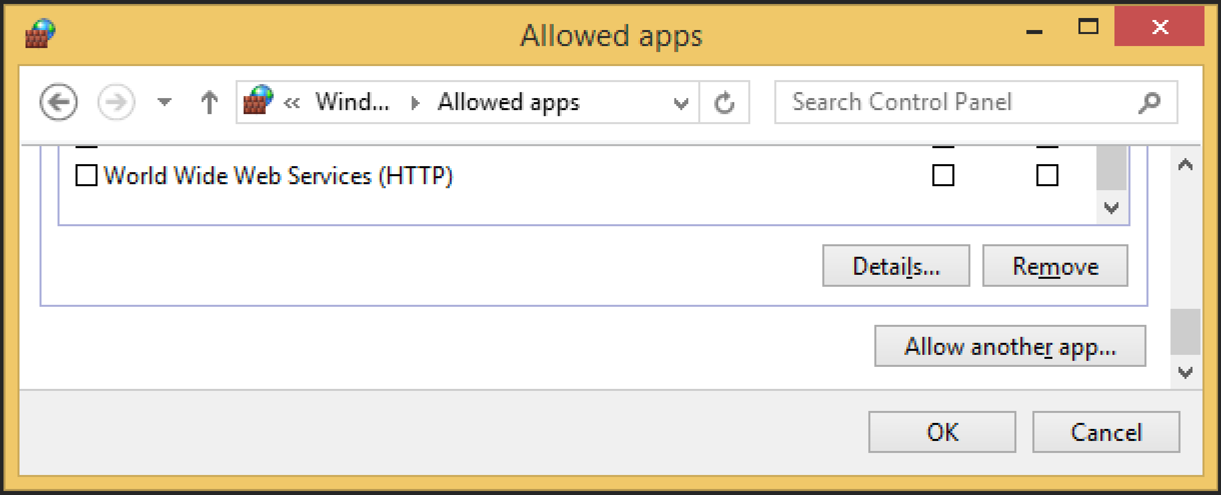
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
□ File and Printer Sharing	□	□
☑ File Transfer Program	☑	□
☑ FileZilla Server	☑	☑
☑ Firefox (C:\Program Files\Mozilla Firefox)	☑	□
☑ FTP Server	☑	□

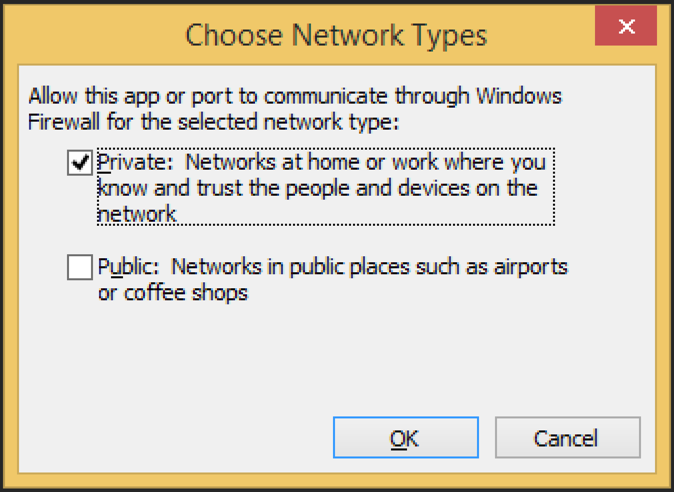
Application & Service List in Windows Firewall

- To add an application, Select "Change settings"
  - If the application / service is already in this list, then check under "Private", "Public" or Both (depending on requirements)
  - If the application / service is NOT listed, then select "Allow Another app…"



Add a program to exception list in Windows Firewall

- Select "Network types…", check "Private", "Public" or both as required



Choose Network Types

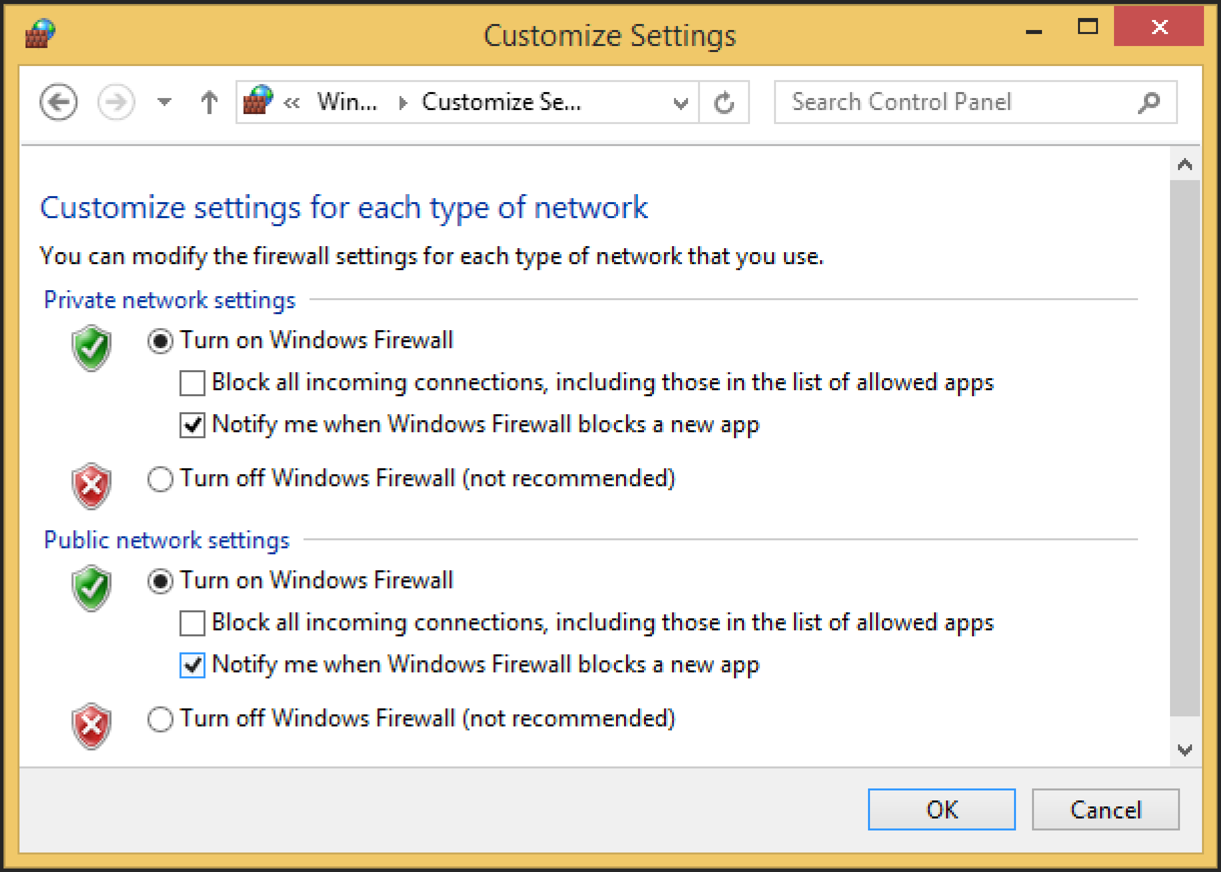
Allow this app or port to communicate through Windows Firewall for the selected network type:

☑ Private: Networks at home or work where you know and trust the people and devices on the network

☐ Public: Networks in public places such as airports or coffee shops

- Select "Browse…", select the program
- Select "Add" & Select "OK"

- To change firewall settings
  - To Disable Firewall, Select “Turn Windows Firewall on or off”



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall

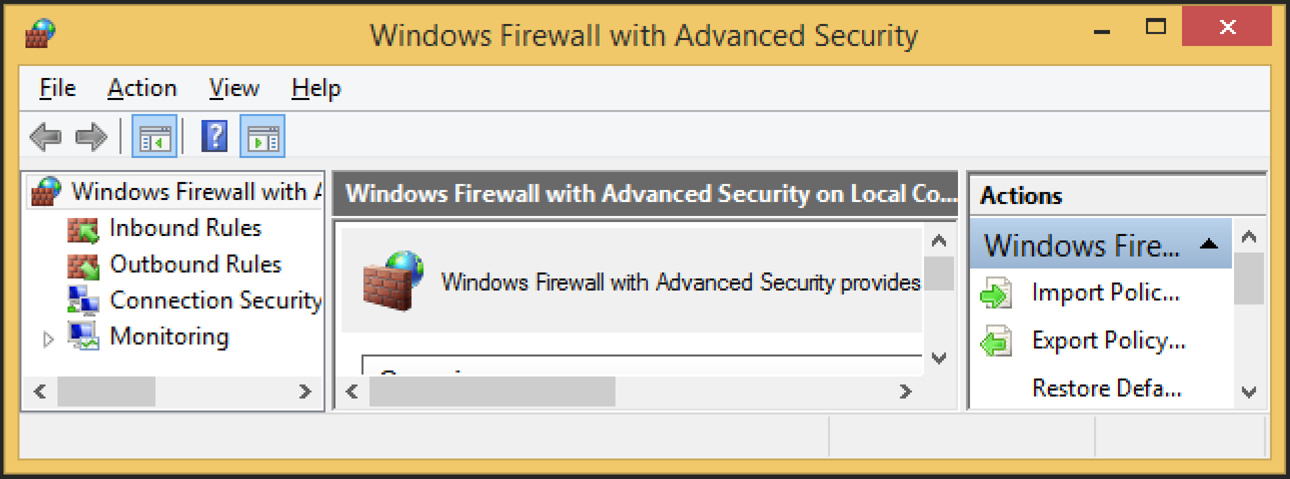
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

- Disable Firewall for Private Networks
  - Select “Turn Off Windows Firewall (not recommended)”
- Disable Firewall for Public Networks
  - Select “Turn Off Windows Firewall (not recommended)”
- Enable Firewall, Select “Turn on Windows Firewall” under respective networks

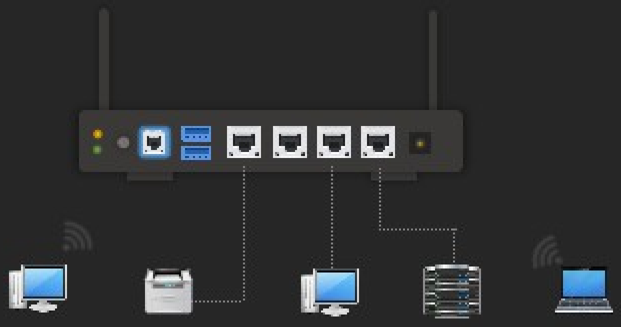
- For finer control (requires technical expertise), select “Advanced Settings” from Windows Firewall



Windows Firewall with Advanced Security provides

Note: Since this topic is advanced, this is not covered further.

SOHO Router



SOHO Router, wired & wireless devices

- Small Office Home Office or Residential/Home Router, a.k.a Residential or Home Router.
- Simple “Network address translation (NAT)” device with facilities such as an Unmanaged Network Switch + Access Point + DSL Modem + SIM Ports + USB Ports…
- Simple & easy to Use, requires minimal technical experience.
- Usually administered through a web interface.
- Widely used in Home & Small Office Networks mostly for sharing Internet Connectivity.

Wireless Router

4G Router

Tip(s):

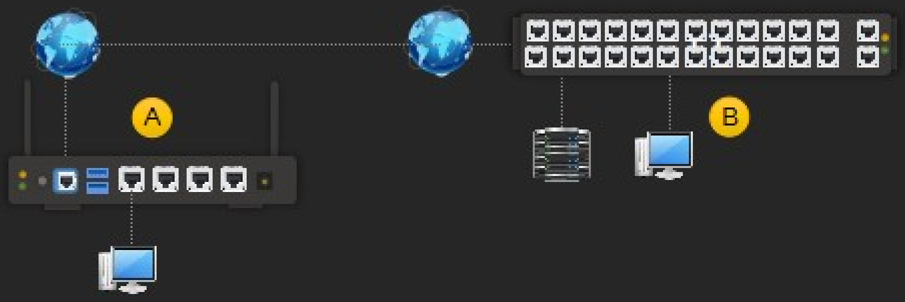
- Wired networks can be extended by using a Network switch or a SOHO Router (as long as SOHO Router has sufficient network connectivity ports).
- Wireless networks can be extended using a range extender (some models of access points & Wi-Fi Routers may have the option to work as a range extender).

SOHO Routers Worksheet			
Vendor			
Model			
Connectivity (DSL / Cable / 4G / All)			
# Of WAN Ports			
No. of Ports (UTP/STP)			
No. of Ports (Optical)			
USB Ports			
USB Version (1.x/2.x/3.x)			
Firewall (Available / Not Available)			
Parental Control			
Beamforming			
Can be used as Wireless Extender? (Yes / No)			
VLAN			
Frequency			
2.4 GHz			
5 GHz			
Dual Band			
Tri Band			
Wireless Security Support			
WEP, 64-bit			
WEP, 128-bit			
WPA			
WPA2			
WPS			
Antennas			
1x1 SISO			
2x2 MIMO			
3x3 MIMO			
4x4 MIMO			
Detachable (Yes/No)			
Standard Compliance			
IEEE 802.3			
IEEE 802.3u			
IEEE 802.3ab			
IEEE 802.3x			
IEEE 802.3z			
IEEE 802.1q			

IEEE 802.1p			
IEEE 802.11b			
IEEE 802.11g			
IEEE 802.11a			
IEEE 802.11n			
IEEE 802.11ac			
IEEE 802.11ax			

VPN

- Virtual Private Network enables the creation of a private network over a public network, ensuring confidentiality, integrity, and privacy of data as it travels across the network.
- A special virtual "Tunnel" created between end-points (like different branch offices across the world).
- Typically used for connecting to office networks from remote locations, over Internet.
- Require VPN Software or Hardware at both ends (VPN Server & VPN Client).
- Uses Protocols like PPTP & L2TP.
- VPN's can be created over technologies such as Dial-ups, DSL, leased lines, etc.



Example: Allows users to connect to a B) office networks from A) home network through the Internet

Quiz 07

1. Which of the following WAN technology is the slowest?

A. ISDN B. Dial-Up C. DSL D. Cable

2. Which of the following connectivity utilizes a 56K modem?

A. ISDN B. PSTN C. DSL D. Both B & C

3. Protocols used in dial-up networking:

A. PPP B. SLIP C. PPPoE D. PPPoA

4. Advantages of PPP over SLIP.

A. Support for Dynamic IP address
B. Support for protocols other than TCP/IP
C. Support for services such as Windows Firewall
D. Support for Layer 1

5. Acronym - ISDN.

A. Internet Services for Digital Network
B. Intranet Services for Digital Network
C. Integrated Services for Digital Network
D. Integrated Services for DSL Network

6. Acronym - DSLAM.

A. Direct subscriber line access multiplexer
B. Direct subscriber line access multiplier
C. Digital subscriber line access multiplexer
D. Digital subscriber line access multiplier

7. Device used for splitting voice and data at a customer's premises in a DSL connection:

A. SOHO Router B. Wi-Fi Router C. DSL Modem D. DSL Splitter

8. DSL uses _____ protocols.

A. PPP B. SLIP C. PPPoE D. Ethernet

9. Acronym - PPPoE.

A. Packet-to-Packet Protocol Over Ethernet B. Point-to-Point Packet Over Ethernet
C. Point-to-Point Protocol Over Ethernet D. Point-to-Packet Protocol Over Ethernet

10. Acronym - PPPoA.

A. Packet-to-Packet Protocol Over ATA B. Point-to-Point Packet Over ATM
C. Point-to-Point Protocol Over ATM D. Point-to-Packet Protocol Over ATA

11. _____ refers to private network over the Internet.

A. WLAN B. DSL C. WiMAX D. VPN

12. Acronym - VPN.

A. Virtual Public Network B. Virtual Private Network
C. Vertical Private Network D. Vertical Public Network

13. Protocols used in VPN:

A. PPP B. PPTP C. L2TP D. SLIP

14. Acronym - PPTP.

A. Private to Public Tunneling Protocol B. Point to Point Teredo Protocol
C. Point to Point Tunneling Protocol D. Private to Public Tunneling Protocol

15. Acronym - L2TP.

A. Level 2 Teredo Protocol B. Level 2 Tunneling Protocol
C. Layer 2 Teredo Protocol D. Layer 2 Tunneling Protocol

16. Encryption used in L2TP:

A. AED B. IP C. IPSec D. 3DES

17. _____ controls incoming & outgoing traffic.

A. DSL B. Anti-Virus Software C. Firewall D. WAP

18. Acronym - NAT.

A. Network Application Translation B. Network Address Translation
C. Nano Address Translation D. Network Application Technology

Connect two computers using a patch cable

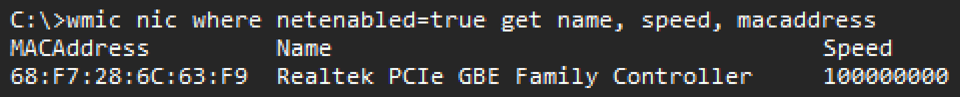
Note: Use a Wired Network Adapter to complete this exercise; disable Wireless network adapter (if any) to avoid confusion.

✓ Step 1: Connect Patch cable to both Ethernet Ports

Try using a straight-through cable; use a cross-over cable if straight-through does Not work. Observe LED indicators on the NIC.

Note: If you get a popup “Do you want to turn on network discovery and file sharing for all public networks?”, Select “No, make the network I am connected to a private network…”.

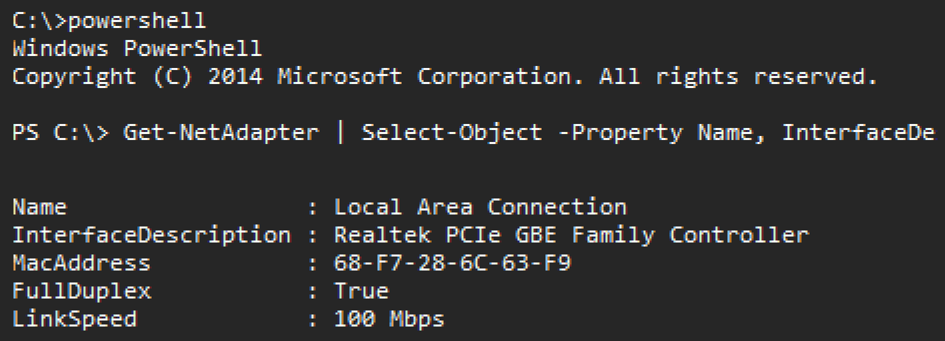
- Confirm if they are connected:
  - CMD > wmic nic where netenabled=true get name, speed, macaddress



```
C:\>wmic nic where netenabled=true get name, speed, macaddress
MACAddress         Name                                    Speed
68:F7:28:6C:63:F9  Realtek PCIe GBE Family Controller      100000000
```

Check for speed value, indicating connectivity

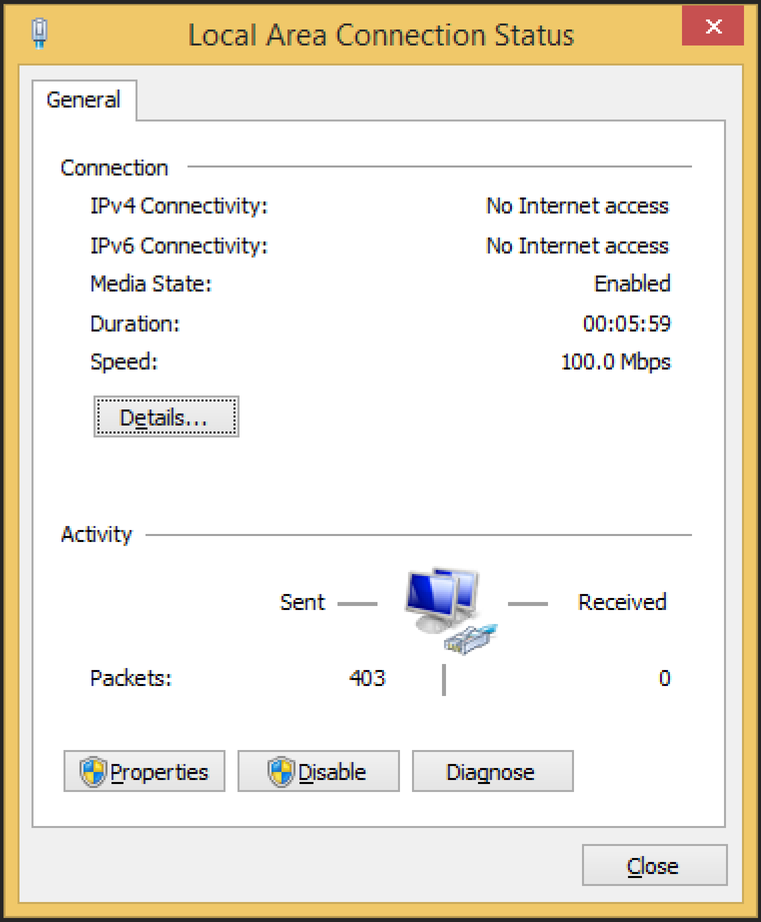
  - CMD > Powershell > Get-NetAdapter | Select-Object -Property Name, InterfaceDescription, MacAddress, FullDuplex, LinkSpeed



```
C:\>powershell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\> Get-NetAdapter | Select-Object -Property Name, InterfaceDe


Name                 : Local Area Connection
InterfaceDescription : Realtek PCIe GBE Family Controller
MacAddress           : 68-F7-28-6C-63-F9
FullDuplex           : True
LinkSpeed            : 100 Mbps
```

Check for Duplex & Speed status, similar to above

- START > RUN > NCPA.CPL, Right-click “Local Area Connection”, select “Status”



Local Area Connection Status

General

Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:05:59

Speed: 100.0 Mbps

Packets: 403 | 0

Local Area Connection, Connectivity Status & Speed

✓ Step 2: Configure IP

- View IP Configuration:
  - CMD > “ipconfig” on both computers to know the IP addresses

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3
   Autoconfiguration IPv4 Address. . : 169.254.126.148
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

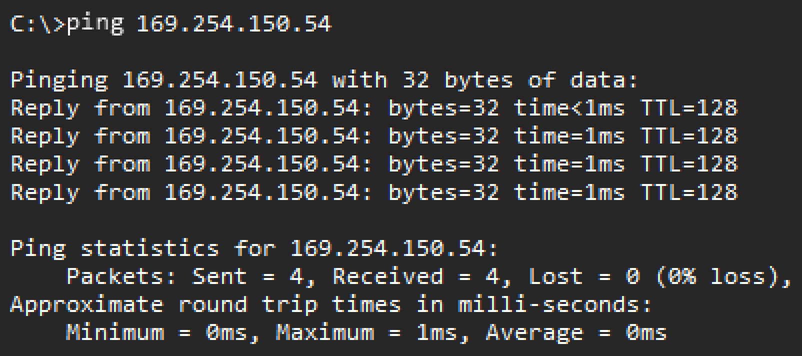
Scroll to view details of wired connection: APIPA IPv4 (Computer 1)

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3
   Autoconfiguration IPv4 Address. . : 169.254.150.54
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

Scroll to view details of wired connection: APIPA IPv4 (Computer 2)

In current scenario both computers are connected directly; since there are no DHCP servers available, both computers have self-assigned IP addresses (APIPA).

- Test connectivity using PING utility (Disable Firewall on both computers temporarily)
    - CMD > “ping 169.254.150.24” (Each other computer’s IP address) or
    - CMD > “ping -4 COMPUTERNAME” (Each other computer’s computer name)

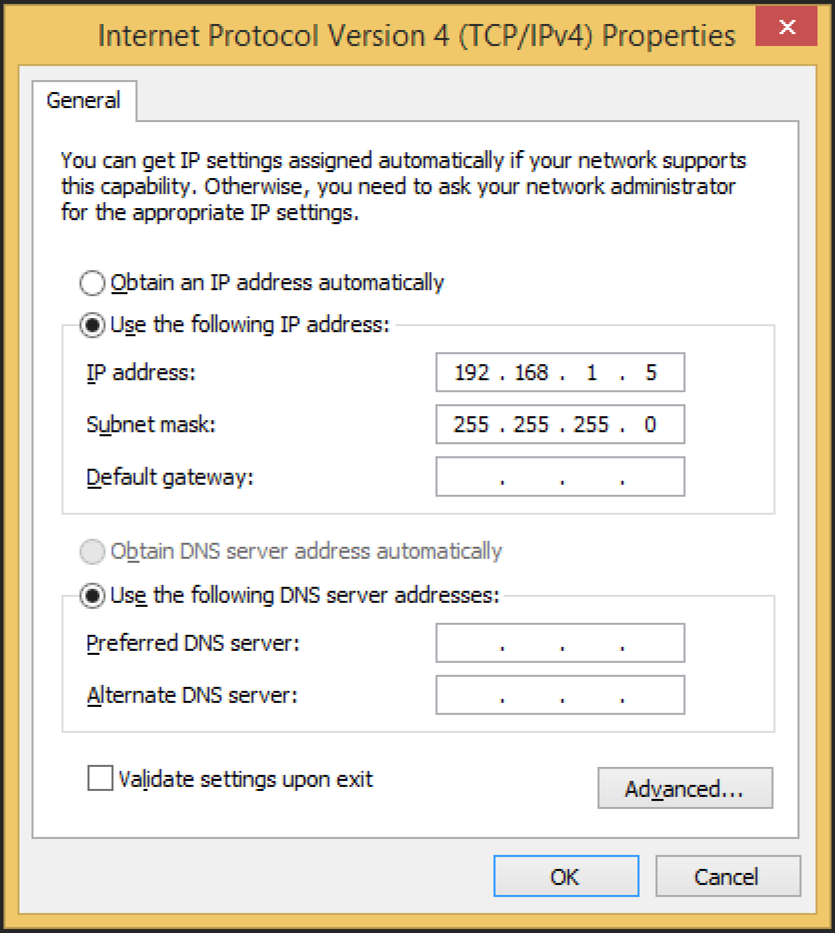


```
C:\>ping 169.254.150.54

Pinging 169.254.150.54 with 32 bytes of data:
Reply from 169.254.150.54: bytes=32 time<1ms TTL=128
Reply from 169.254.150.54: bytes=32 time=1ms TTL=128
Reply from 169.254.150.54: bytes=32 time=1ms TTL=128
Reply from 169.254.150.54: bytes=32 time=1ms TTL=128

Ping statistics for 169.254.150.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Observe results, successful communication

Assigning an IP address is optional, as both computers are already communicating with other; follow the instructions below to assign static IP addresses:

- Assign Static IP Address, Microsoft Windows (Computer 1)
  - START > RUN > NCPA.CPL
  - Right-click “Local Area Connection”, select “Properties”
    - Select “Internet Protocol Version 4 (TCP/IPv4)” from the list and Click “Properties”
    - Select “Use the following IP address:”
      - Enter “192.168.1.5” in “IP address:”
      - Enter “255.255.255.0” in “Subnet mask:”
    - Select “OK”
    - Select “Close”



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 5

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

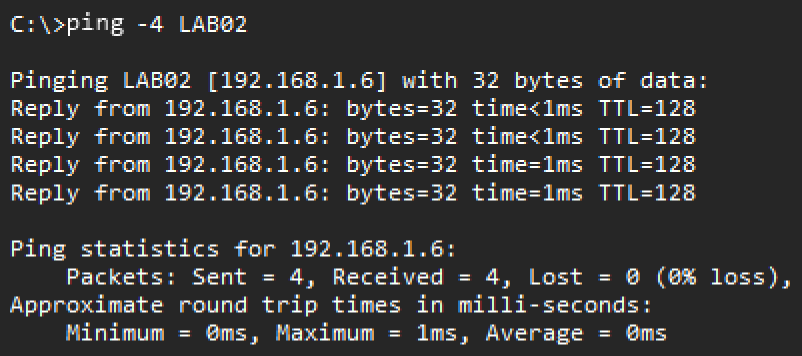
□ Validate settings upon exit

IPv4 Properties

- Assign Static IP Address, Microsoft Windows (Computer 2)
  - START > RUN > NCPA.CPL
  - Right-click “Local Area Connection”, select “Properties”
    - Select “Internet Protocol Version 4 (TCP/IPv4)” and Click “Properties”
    - Select “Use the following IP address:”
      - Enter “192.168.1.6” in “IP address:”
      - Enter “255.255.255.0” in “Subnet mask:”
    - Select “OK”
    - Select “Close”

- Test connectivity using PING utility (Disable Firewall on both computers temporarily if required)

  - CMD > “ping 192.168.1.6” (Each other computer’s IP address) or
  - CMD > “ping -4 COMPUTERNAME” (Each other computer’s computer name)

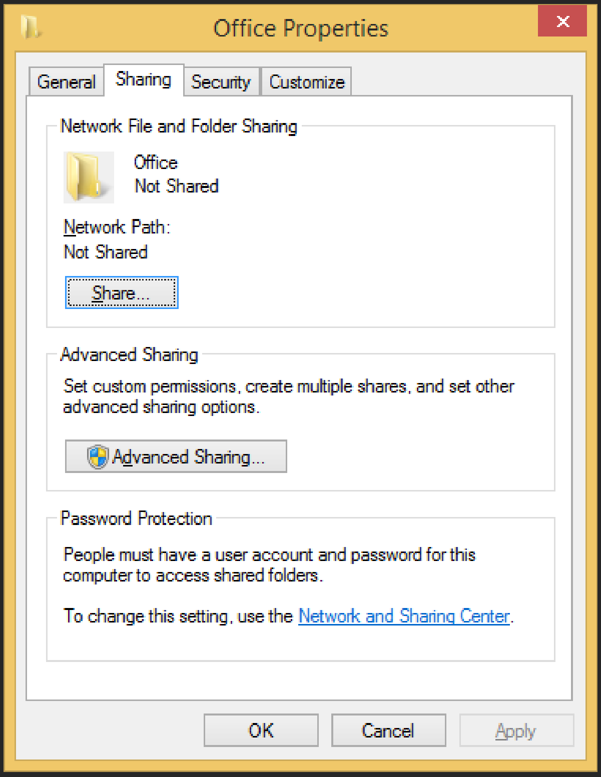


```
C:\>ping -4 LAB02

Pinging LAB02 [192.168.1.6] with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Observe replies from each other computer

✓ Step 3: To Share Folders

- Create a new folder, for example: C:\Office
- Right-Click FOLDERNAME, Select “Properties“
- Select Sharing Tab



Office Properties

Network File and Folder Sharing

Office
Not Shared

Network Path:
Not Shared

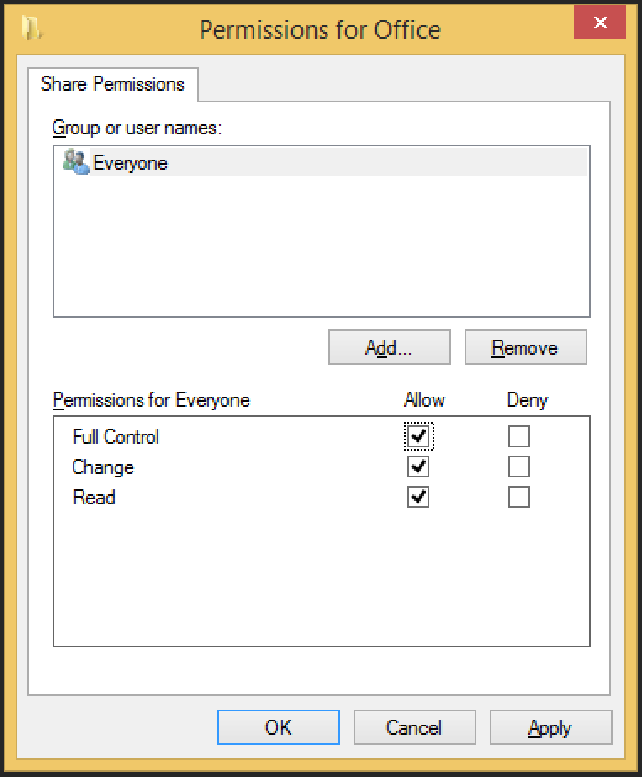
Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.



Permissions for Office

Group or user names:

Everyone

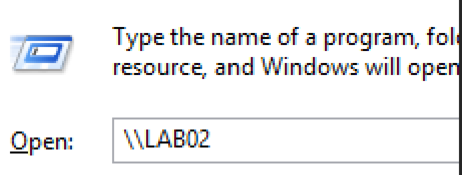
Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

- Select “Advanced Sharing”
- Select “Share this folder”
- Select “Permissions”
- Select “Allow” (Image above) - Full Control
- Select “Apply”, Select “OK” Twice
- Select “Close”

Repeat on the other computer as well.

✓ Step 4: To access the shared folder

- START > RUN > \\COMPUTERNAME

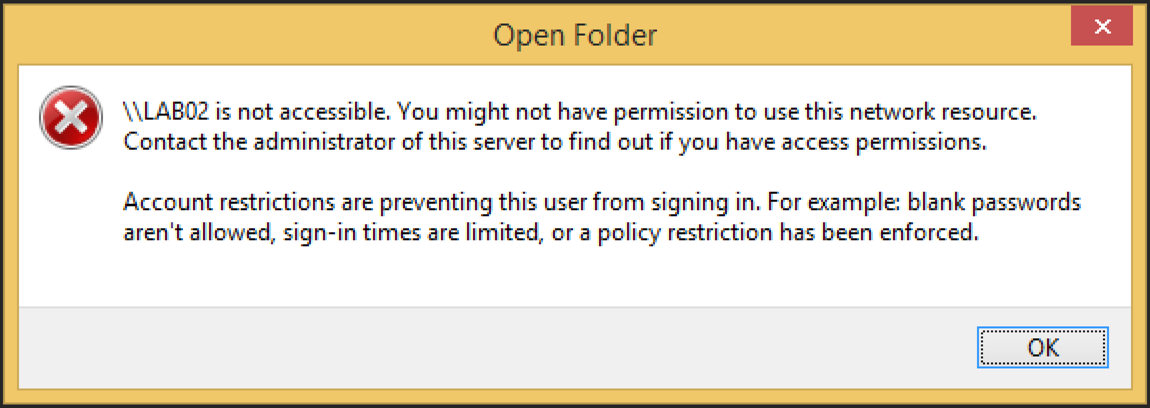


Type the name of a program, fol
resource, and Windows will open

Open: \\LAB02

Input to access another computer by computer name

- Enter Credentials as required

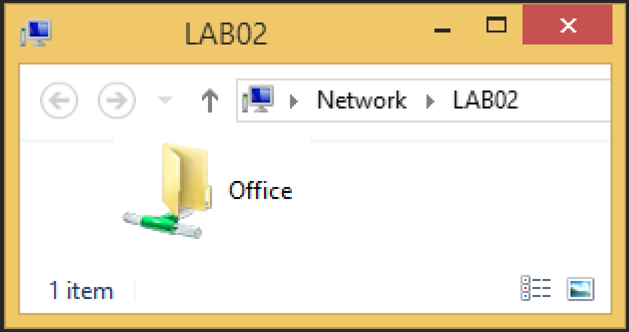


\\LAB02 is not accessible. You might not have permission to use this network resource. Contact the administrator of this server to find out if you have access permissions.

Account restrictions are preventing this user from signing in. For example: blank passwords aren't allowed, sign-in times are limited, or a policy restriction has been enforced.

Restrictions Popup

Note: If above popup is displayed, then set a password for the user account on the computer that is being accessed (Windows requires password for user accounts, when accessed over network).

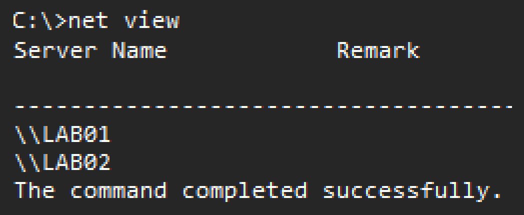


Shared folder on a remote computer

- Files may be copied to the shared folder

Tips: It is NOT recommended to share an entire drive (though it is possible), rather share specific folders with appropriate permissions.

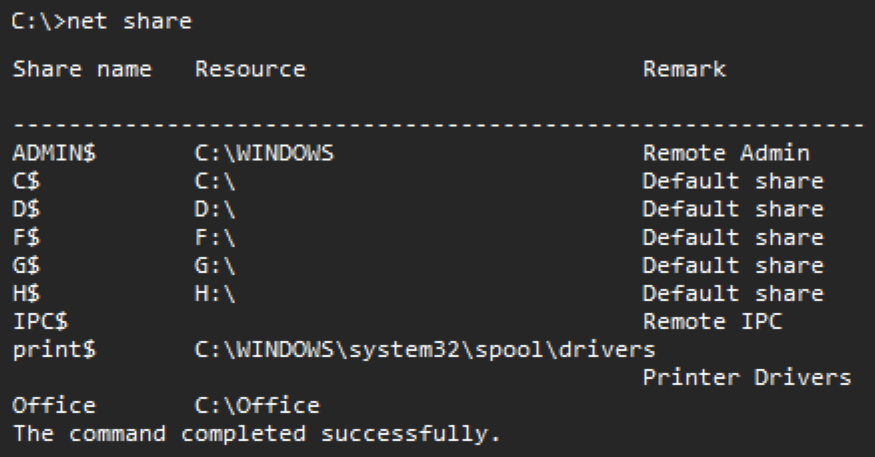
- To View computers on a network:
  - CMD > net view



```
C:\>net view
Server Name            Remark

-------------------------------------
\\LAB01
\\LAB02
The command completed successfully.
```

Output listing computers on a network

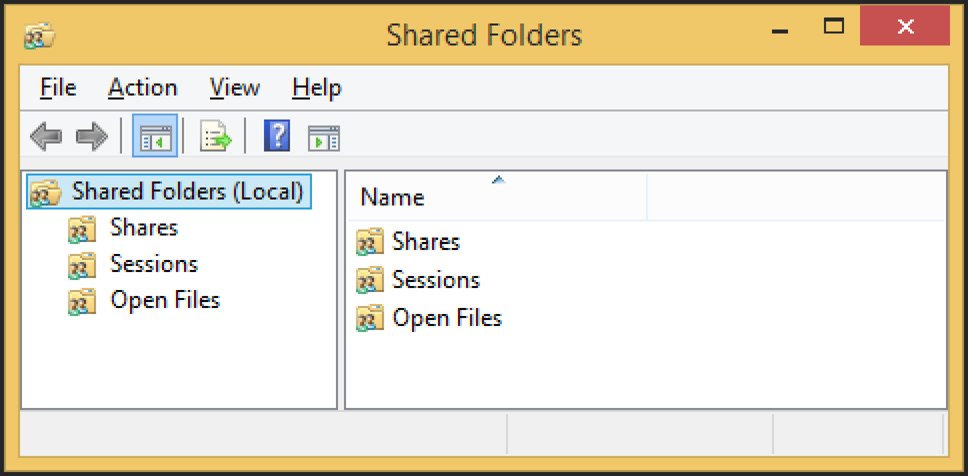
- To View shares available on a local computer:
  - CMD > net share



```
C:\>net share

Share name   Resource                        Remark

-------------------------------------------------------------
ADMIN$       C:\WINDOWS                      Remote Admin
C$           C:\                             Default share
D$           D:\                             Default share
F$           F:\                             Default share
G$           G:\                             Default share
H$           H:\                             Default share
IPC$                                         Remote IPC
print$       C:\WINDOWS\system32\spool\drivers
                                             Printer Drivers
Office       C:\Office
The command completed successfully.
```

Output listing shares on a local computer

  - START > RUN > FSMGMT.MSC



GUI listing shares, sessions & Open files

- To view open files (if connected to a remote share and files are open)
  - CMD > openfiles

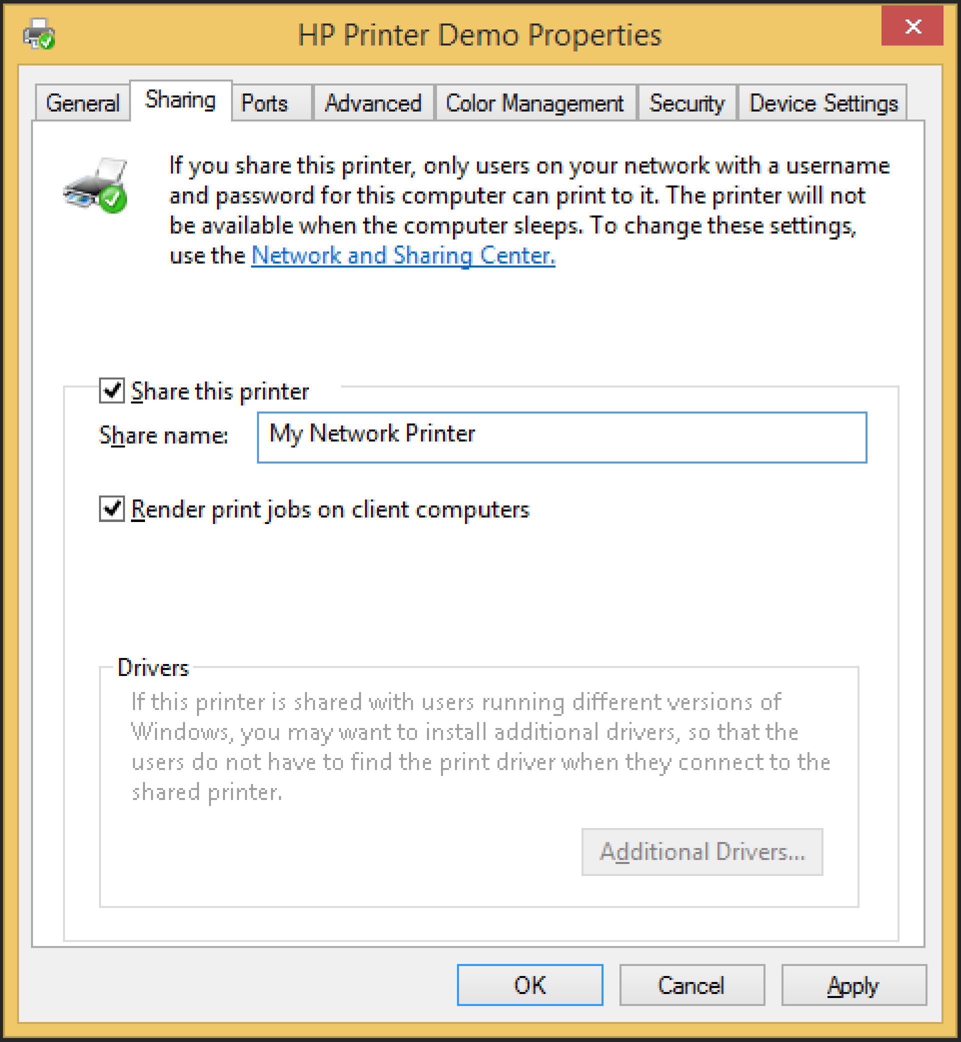
Sharing & Accessing Printers

To install a printer (example):

- START > RUN > CONTROL PRINTERS
- Select “Add a printer”
- Select “The printer that I want isn’t listed”
- Select “Add a local printer or network printer with manual settings”, Select “Next”
- Select “Use an existing port:”, Select “LPT1: Local Port” and Select “Next”
- Select a Manufacturer / Model from the list displayed (for example: HP > HP Color LaserJet 1600 Class Driver)”, Select “Next”
- Specify “HP Printer Demo” under “Printer name:”, Select “Next”
- Select “Do not share this printer”, Select “Next” & Select “Finish”

To share a printer:

- Select any printer, for example “HP Printer Demo”
- Right-click and Select “Printer Properties”, Select “Sharing” tab
- Select “Share this printer” and Specify “My Network Printer” under “Share name:”



HP Printer Demo Properties

If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: My Network Printer

☑ Render print jobs on client computers

Drivers

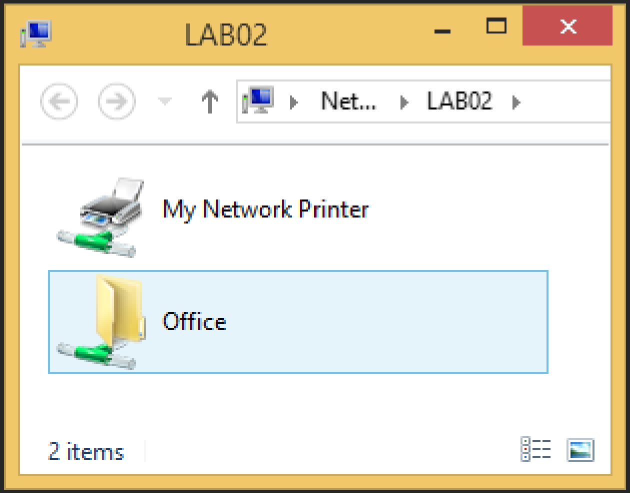
If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Printer Properties

- Select “Apply” and Select “OK”

To access a shared printer:

- START > RUN > \\COMPUTERNAME



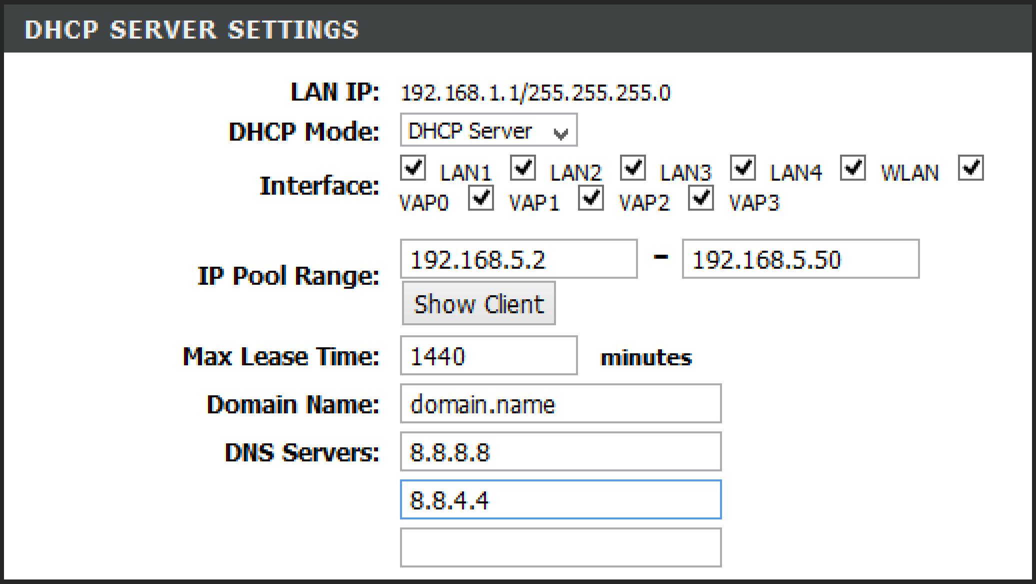
View list of shared resources available in a network

- Double-click on the shared printer, for example: “My Network Printer”

Note: Printer drivers are automatically installed, if the device drivers for selected model is included with the operating system; if not, printer driver media or source will be required to complete the installation of a printer.

Setting up DHCP Server (Using a Home Router)

- Navigate to DHCP Settings or similar (depending on the model)
- Set Range (Use a range different from other routers nearby or from common settings)
  - Start: 192.168.5.2
  - End: 192.168.5.50
  - Lease time: 2 days or so
  - DNS Servers
    - Primary: 8.8.8.8
    - Secondary: 8.8.4.4



DHCP SERVER SETTINGS

LAN IP:	192.168.1.1/255.255.255.0
DHCP Mode:	DHCP Server
Interface:	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2 ☑ VAP3
IP Pool Range:	192.168.5.2 - 192.168.5.50 Show Client
Max Lease Time:	1440 minutes
Domain Name:	domain.name
DNS Servers:	8.8.8.8 8.8.4.4

DHCP Settings on a specific SOHO Router

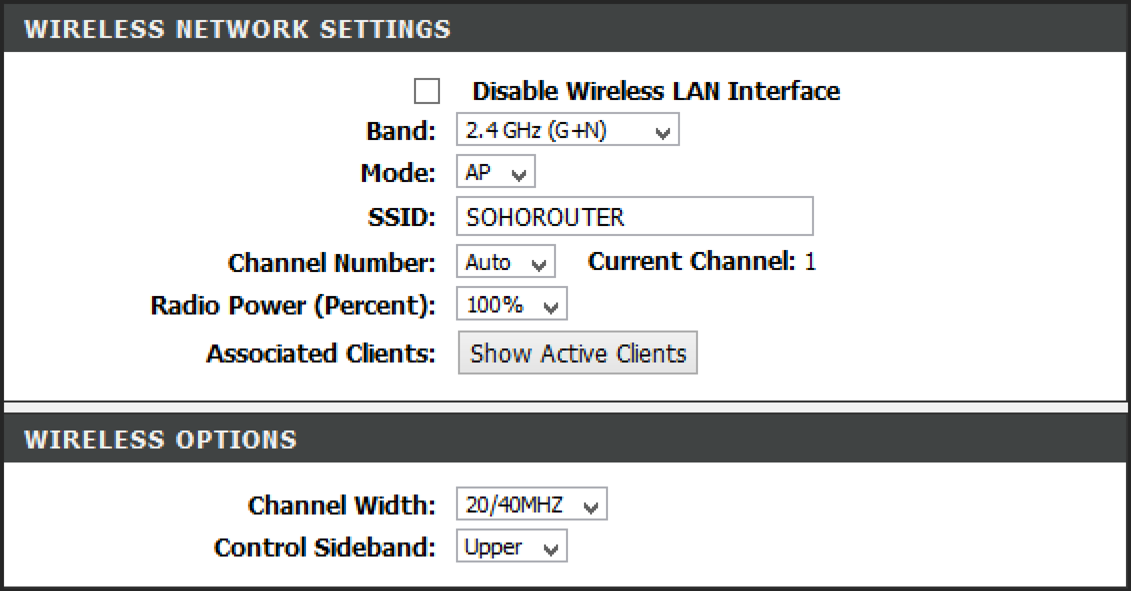
Note: DNS settings can be implemented at Router level or at each device level.

- Use ipconfig /release & ipconfig /renew to apply changes (Client Computers).

- Setup Wireless Network (Infrastructure Mode)

Tip: Most home routers have the IP address set as 192.168.1.1, 192.168.2.1, etc. (192.168.x.x range). Home routers are managed through a web browser, by typing the URL as “192.168.1.1”. Similarly usernames may be as simple as “admin” with password as “password” or no password at in for most models. Refer to product documentation for exact IP address, username and password.

  - Logon & Navigate to WLAN or Wireless Settings or Wi-Fi Settings page (depending on model)



WIRELESS NETWORK SETTINGS

□ Disable Wireless LAN Interface
Band: 2.4 GHz (G+N)
Mode: AP
SSID: SOHOROUTER
Channel Number: Auto Current Channel: 1
Radio Power (Percent): 100%
Associated Clients: Show Active Clients

WIRELESS OPTIONS

Channel Width: 20/40MHZ
Control Sideband: Upper

Wireless Settings on a specific SOHO Router

- If all devices in the network support IEEE 802.11N, then it is recommended to set the “band” as “N” (“G” may be used for backward compatibility if there are IEEE 802.11G clients). Similar for other IEEE 802.11 standards.

Note: On routers supporting other IEEE 802.11 standards such as IEEE 802.11a or IEEE 802.11ac, there may be additional options not included here. Also different SSID can be set for 2.4 GHz & 5 GHz, if the router support multiple frequencies.

- Use ipconfig /release & ipconfig /renew to apply changes (Client Computers).

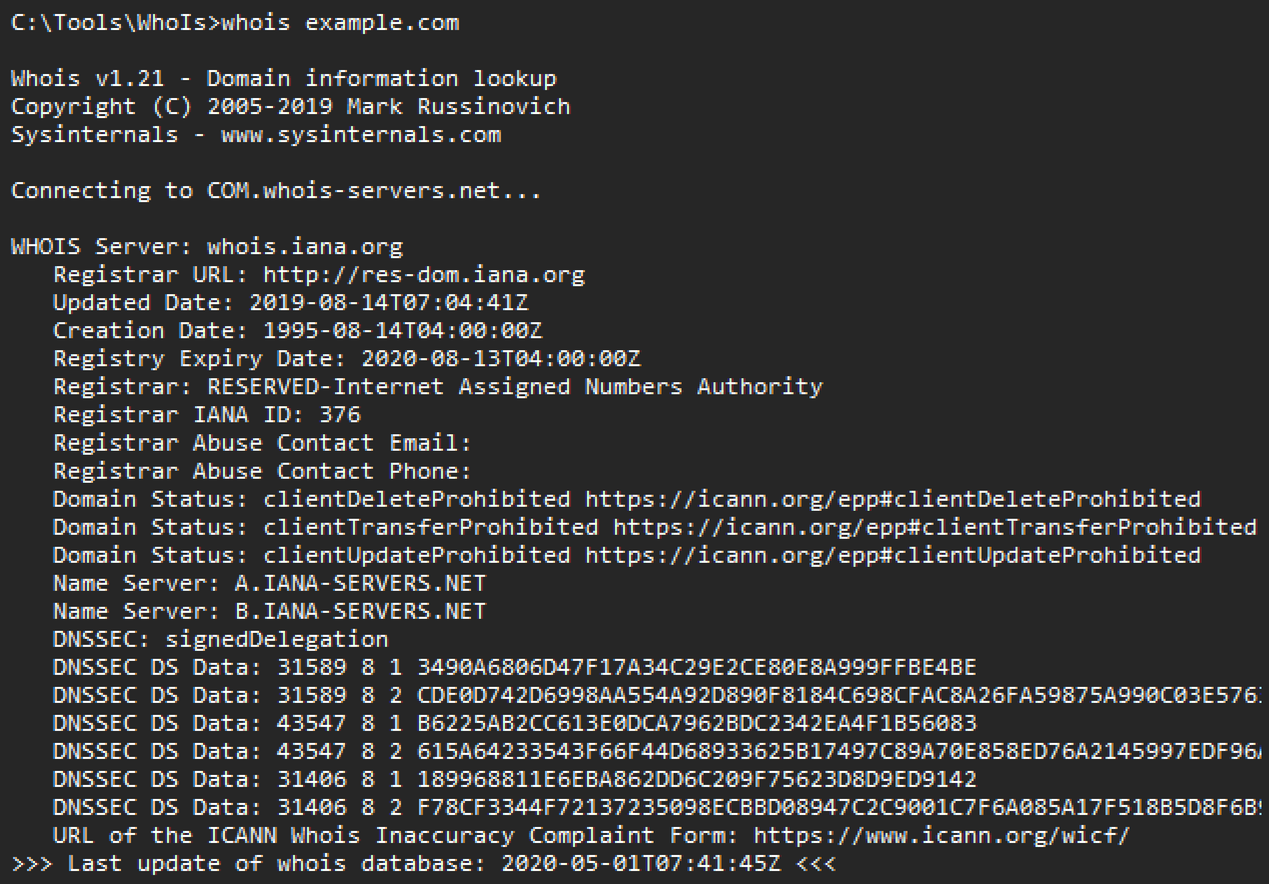
Additional Settings (Depending on model):

- MAC Filtering: Facility to “limit” client devices by specifying MAC addresses (allows devices to connect only if the MAC addresses match, preventing unauthorized computers / devices to be a part of a network).
- Port Forwarding: Allow a particular service on a computer in an internal network, to be accessible from public network. For example, a computer running a web server on the internal network can be made accessible from external network (Internet).
- DMZ (Demilitarized Zone): Allow a specific computer from an internal network to be accessible to the public network (high risk); for example, a computer running multiple services or if it requires almost most ports to be open, can be kept in DMZ.
- Parental Control: Control Internet usage, usually through Whitelists, blacklists, Time limits, etc.
- Guest Access & Virtual WAP: Facility to set limited access for clients/guests.
- MAC Clone: Facility to use a different MAC address instead of integrated MAC Address.

Note: Some home routers may have the facility to keep different SSID’s, for home & guest networks.

WHOIS Tool

- Download from https://docs.microsoft.com/en-us/sysinternals/downloads/whois
- Extract the compressed file to C:\Tools\
- To view details for a domain: CMD > CD C:\Tools\WhoIs > whois domainame



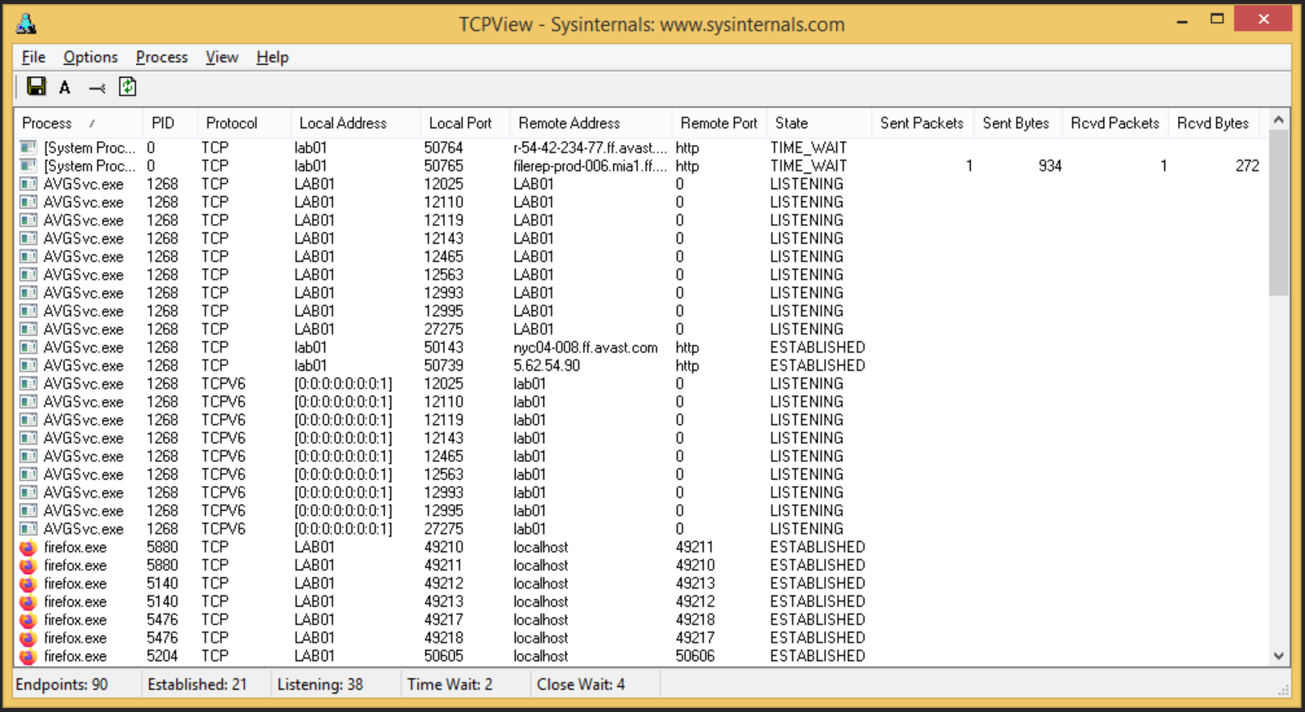
```
C:\Tools\WhoIs>whois example.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2019-08-14T07:04:41Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2020-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 31589 8 1 3490A6806D47F17A34C29E2CE80E8A999FFBE4BE
   DNSSEC DS Data: 31589 8 2 CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03E576
   DNSSEC DS Data: 43547 8 1 B6225AB2CC613E0DCA7962BDC2342EA4F1B56083
   DNSSEC DS Data: 43547 8 2 615A64233543F66F44D68933625B17497C89A70E858ED76A2145997EDF96
   DNSSEC DS Data: 31406 8 1 189968811E6EBA862DD6C209F75623D8D9ED9142
   DNSSEC DS Data: 31406 8 2 F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D8F6B
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-05-01T07:41:45Z <<<
```

Output listing ownership of a domain name

TCPView

TCPView is a 3rd party GUI utility similar to NETSTAT.

- Download https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
- Extract to C:\Tools
- Execute C:\Tools\Tcpview.exe



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	lab01	50764	r-54-42-234-77.ff.avast....	http	TIME_WAIT				
[System Proc...	0	TCP	lab01	50765	filerep-prod-006.mia1.ff....	http	TIME_WAIT	1	934	1	272
AVGSvc.exe	1268	TCP	LAB01	12025	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12110	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12119	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12143	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12465	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12563	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12993	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	12995	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	LAB01	27275	LAB01	0	LISTENING				
AVGSvc.exe	1268	TCP	lab01	50143	nyc04-008.ff.avast.com	http	ESTABLISHED				
AVGSvc.exe	1268	TCP	lab01	50739	5.62.54.90	http	ESTABLISHED				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12025	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12110	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12119	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12143	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12465	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12563	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12993	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	12995	lab01	0	LISTENING				
AVGSvc.exe	1268	TCPV6	[0:0:0:0:0:0:0:1]	27275	lab01	0	LISTENING				
firefox.exe	5880	TCP	LAB01	49210	localhost	49211	ESTABLISHED				
firefox.exe	5880	TCP	LAB01	49211	localhost	49210	ESTABLISHED				
firefox.exe	5140	TCP	LAB01	49212	localhost	49213	ESTABLISHED				
firefox.exe	5140	TCP	LAB01	49213	localhost	49212	ESTABLISHED				
firefox.exe	5476	TCP	LAB01	49217	localhost	49218	ESTABLISHED				
firefox.exe	5476	TCP	LAB01	49218	localhost	49217	ESTABLISHED				
firefox.exe	5204	TCP	LAB01	50605	localhost	50606	ESTABLISHED				

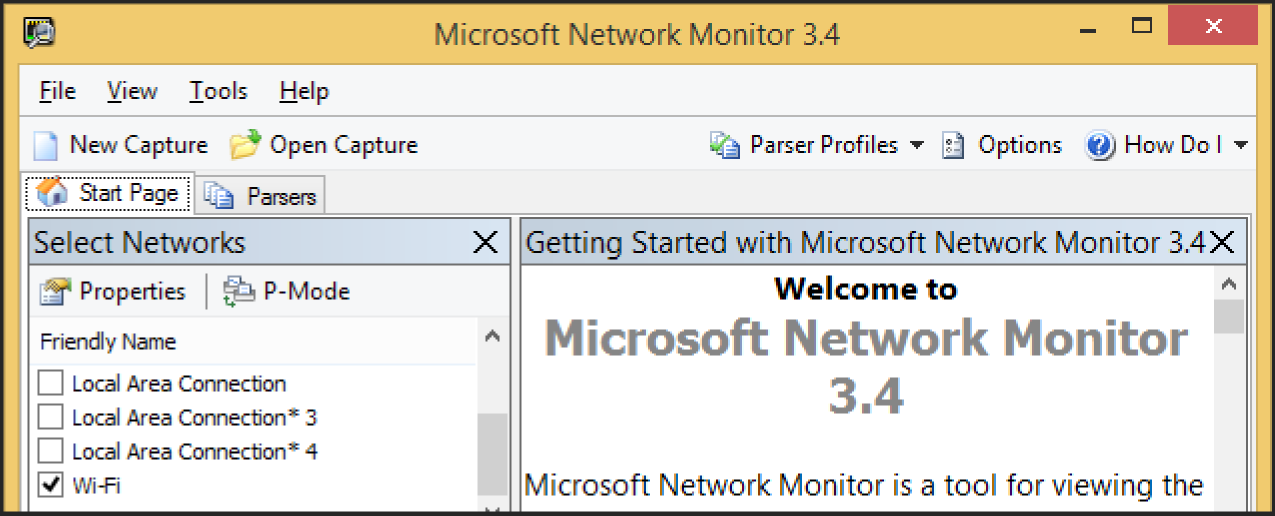
Endpoints: 90 Established: 21 Listening: 38 Time Wait: 2 Close Wait: 4

Sample TCPVIEW Utility Output

Network Monitor

Network Monitor is a free utility, which can be used for learning a lot of things that happen behind the scenes. Though it may appear complicated initially, this tool can help in deeper understanding.

- Download from https://www.microsoft.com/en-in/download/details.aspx?id=4865
- Install and launch Network Monitor
- Select the adapter with an active Internet Connection (Either Wired or Wireless)



Friendly Name

- ☐ Local Area Connection
- ☐ Local Area Connection* 3
- ☐ Local Area Connection* 4
- ☑ Wi-Fi

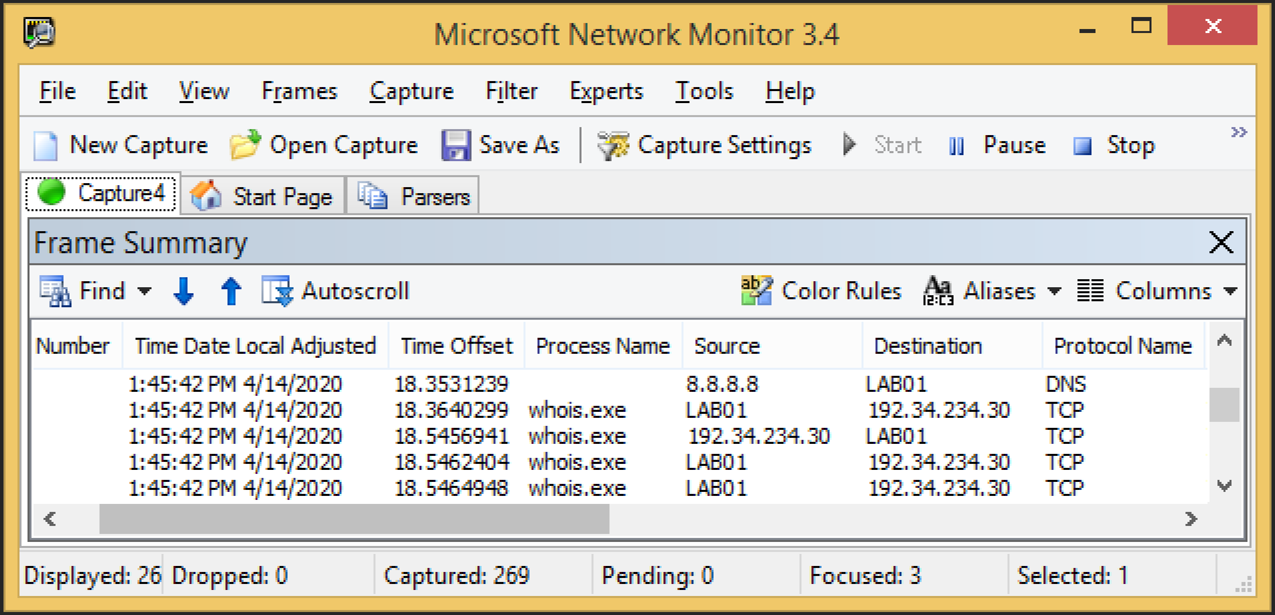
Welcome to

Microsoft Network Monitor 3.4

Microsoft Network Monitor is a tool for viewing the

Sample: Connection Name "Wi-Fi" selected

- Select "New Capture"
- Select "Start"
- Try PING or WHOIS command & Observe results under "Frame Summary"



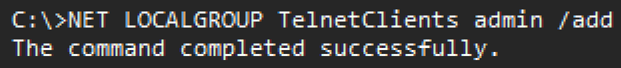
Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name
	1:45:42 PM 4/14/2020	18.3531239		8.8.8.8	LAB01	DNS
	1:45:42 PM 4/14/2020	18.3640299	whois.exe	LAB01	192.34.234.30	TCP
	1:45:42 PM 4/14/2020	18.5456941	whois.exe	192.34.234.30	LAB01	TCP
	1:45:42 PM 4/14/2020	18.5462404	whois.exe	LAB01	192.34.234.30	TCP
	1:45:42 PM 4/14/2020	18.5464948	whois.exe	LAB01	192.34.234.30	TCP

Displayed: 26 Dropped: 0 Captured: 269 Pending: 0 Focused: 3 Selected: 1

Observe Process name, Source & Destination IP address, Protocol Used, etc.

TELNET SERVER (Microsoft Windows)

- Control Panel > Programs & Features
- Select "Turn Windows Features on or off"
- Scroll and select "Telnet Server", Select "OK"
- START > RUN > Services.msc
- Scroll and Select "Telnet", Right-click & Select "Properties"
- Select "Manual" from "Startup type:" dropdown, Select "Apply"
- Select "Start" & Select "OK"
- CMD > NET LOCALGROUP TelnetClients USERNAME /add

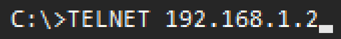


```
C:\>NET LOCALGROUP TelnetClients admin /add
The command completed successfully.
```

Output listing command results; user accounts must be enabled for Telnet Access

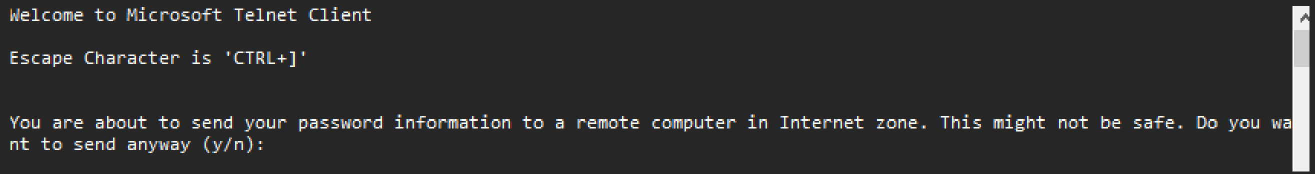
TELNET CLIENT (Microsoft Windows)

- Control Panel > Programs & Features
- Select "Turn Windows Features on or off"
- Scroll and select "Telnet Client", Select "OK"
- CMD > TELNET IPV4 Address



```
C:\>TELNET 192.168.1.2_
```

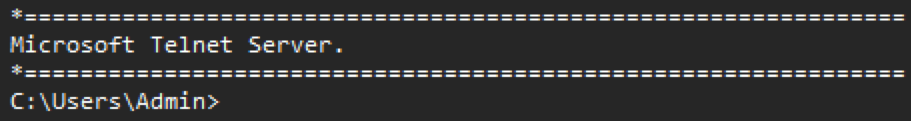
Connect to Telnet Service using an IPv4 address



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'


You are about to send your password information to a remote computer in Internet zone. This might not be safe. Do you wa
nt to send anyway (y/n):
```

Credentials

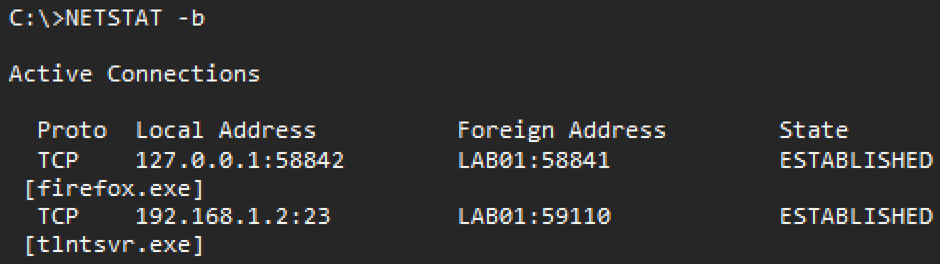
- Specify Credentials as required



```
*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\Admin>
```

Output of a Telnet Connectivity

- Open another CMD > NETSTAT -b



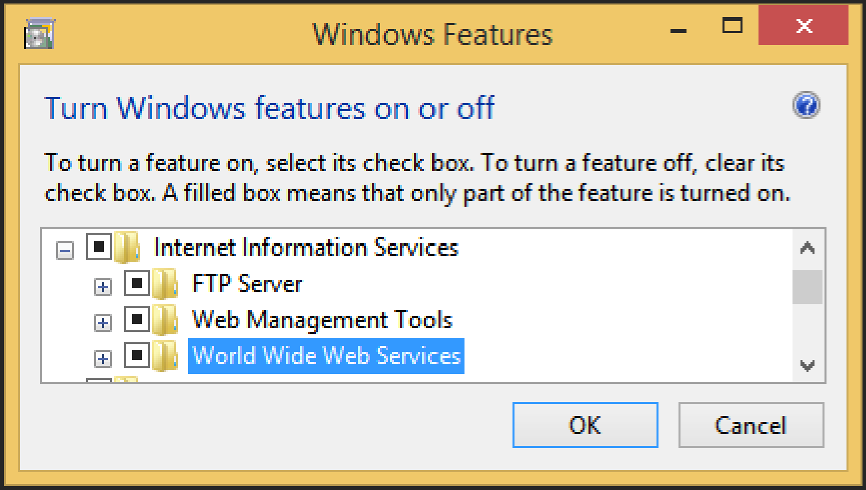
```
C:\>NETSTAT -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:58842        LAB01:58841            ESTABLISHED
 [firefox.exe]
  TCP    192.168.1.2:23         LAB01:59110            ESTABLISHED
 [tlntsvr.exe]
```

Observe Telnet Server Service available on Port 23

Note: Type "help | more" for commands supported under Telnet environment; Type "Exit" to quit.

HTTP + FTP Server - Internet Information Services (Microsoft Windows)

- START > RUN > APPWIZ.CPL
- Select “Turn Windows Features on or off”
- Select “FTP Server”, “Web Management Tools” & “World Wide Web Services” & Select “OK”



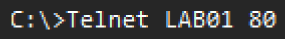
Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

Windows Features - Internet Information Services

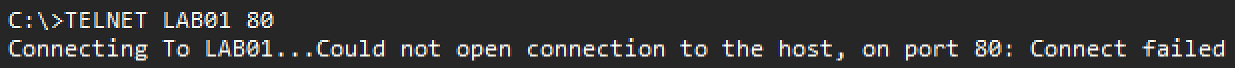
- Test for open port:
  - CMD > Telnet IPv4 PORT (or) Telnet COMPUTERNAME PORT



```
C:\>Telnet LAB01 80
```

Example: HTTP Service running on “LAB01” on Port “80”

  - A blank window with blinking cursor or custom message - confirms an open port at 80 (CTRL+C to stop)
  - Any other result - Port 80 is not open or blocked for response



```
C:\>TELNET LAB01 80
Connecting To LAB01...Could not open connection to the host, on port 80: Connect failed
```

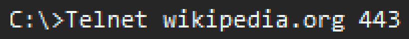
Output when port is not open or blocked

Tip: Use Telnet to check Application Layer issues, such as if a remote service is enabled or having any connectivity issues such as firewall blocking a particular port.

- Check Web Servers
  - CMD > Telnet DOMAINNAME PORT# (Example: Telnet wikipedia.org 80)

Note: If SSL is available on a domain, then use Telnet domainname 443 (assuming default HTTPS port 443)

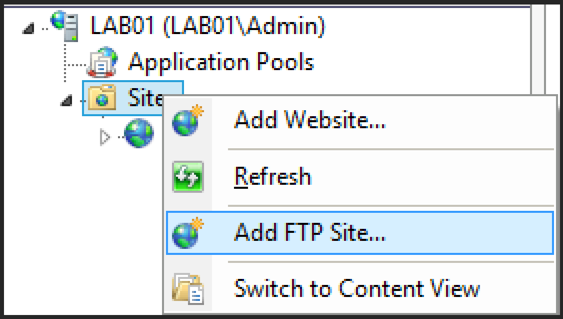
  - CMD > Telnet wikipedia.org 443



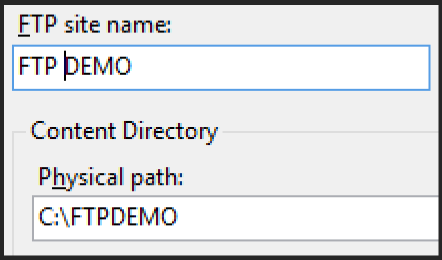
```
C:\>Telnet wikipedia.org 443
```

Example using wikipedia.org on port 443

- To create FTP site (FTP sites are NOT created by default):
  - Control Panel > Administrative Tools > Internet Information Services (IIS) Manager
  - Right-click on Sites > Select "Add FTP Site…"



  - Create a folder, for example: C:\FTPDEMO
  - Specify a name for FTP site, for example: FTP DEMO & Select the folder created earlier

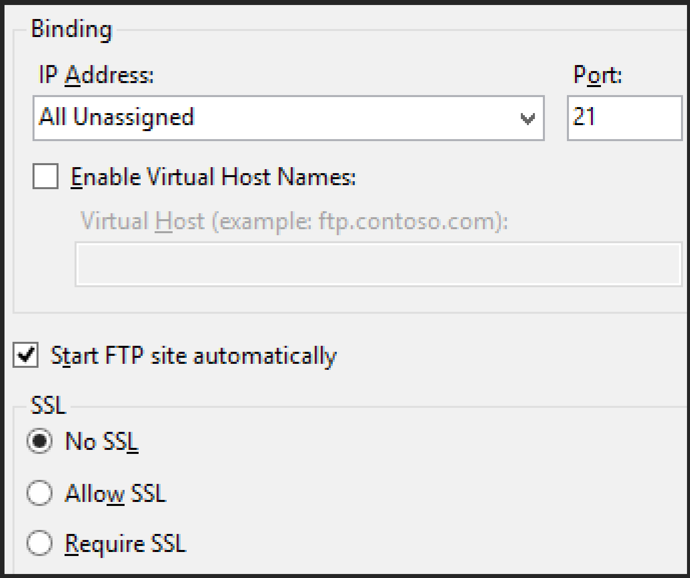


FTP site name: FTP DEMO

Content Directory

Physical path: C:\FTPDEMO

  - Select "Next", Select "No SSL" and Select "Next"



Binding

IP Address: All Unassigned

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

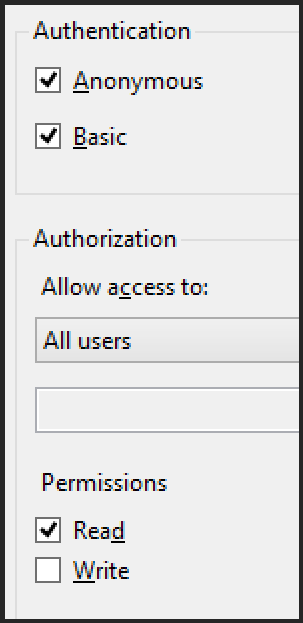
☑ Start FTP site automatically

SSL

● No SSL

○ Allow SSL

○ Require SSL



Authentication

☑ Anonymous

☑ Basic

Authorization

Allow access to: All users

Permissions

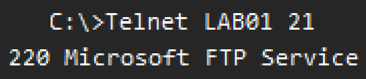
☑ Read

□ Write

  - Select "Anonymous" and "Basic" under Authentication
  - Select "All Users" under Allow access to:
  - Select "Read" under Permissions
  - Select "Finish"

Note: “Anonymous” access may be used where security is not a concern. Popular public ftp sites often provide access using Anonymous accounts.

- To test FTP server:
  - CMD > Telnet COMPUTERNAME PORT#

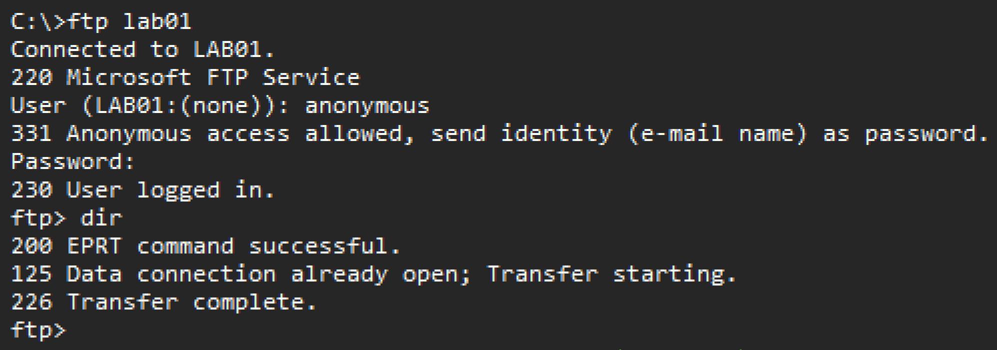


```
C:\>Telnet LAB01 21
220 Microsoft FTP Service
```

Example: FTP Service running on “LAB01” on Port “21”

- If FTP service is set to 8090 on ftp.domainname.extension, then:
  - CMD > Telnet ftp.domainname.extension 8090

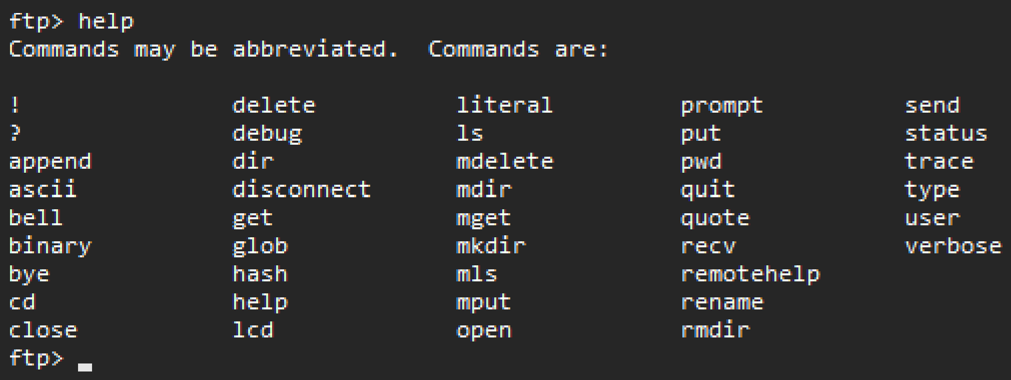
- To access FTP server:
  - CMD > ftp COMPUTERNAME



```
C:\>ftp lab01
Connected to LAB01.
220 Microsoft FTP Service
User (LAB01:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> dir
200 EPRT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

Example: Use “anonymous” as a valid User account (Windows) for credentials to log on

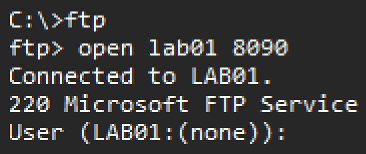
  - To view complete list of supported commands:
    - ftp > help



```
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp> _
```

Output listing available commands

- To access FTP service COMPUTERNAME on port 8090
  - CMD > ftp > open COMPUTERNAME 8090



```
C:\>ftp
ftp> open lab01 8090
Connected to LAB01.
220 Microsoft FTP Service
User (LAB01:(none)):
```

Input to logon using different port number

- To access FTP Service on ftp.domainname.extension on port 8090,
  - CMD > ftp
  - open ftp.domainname.extension 8090

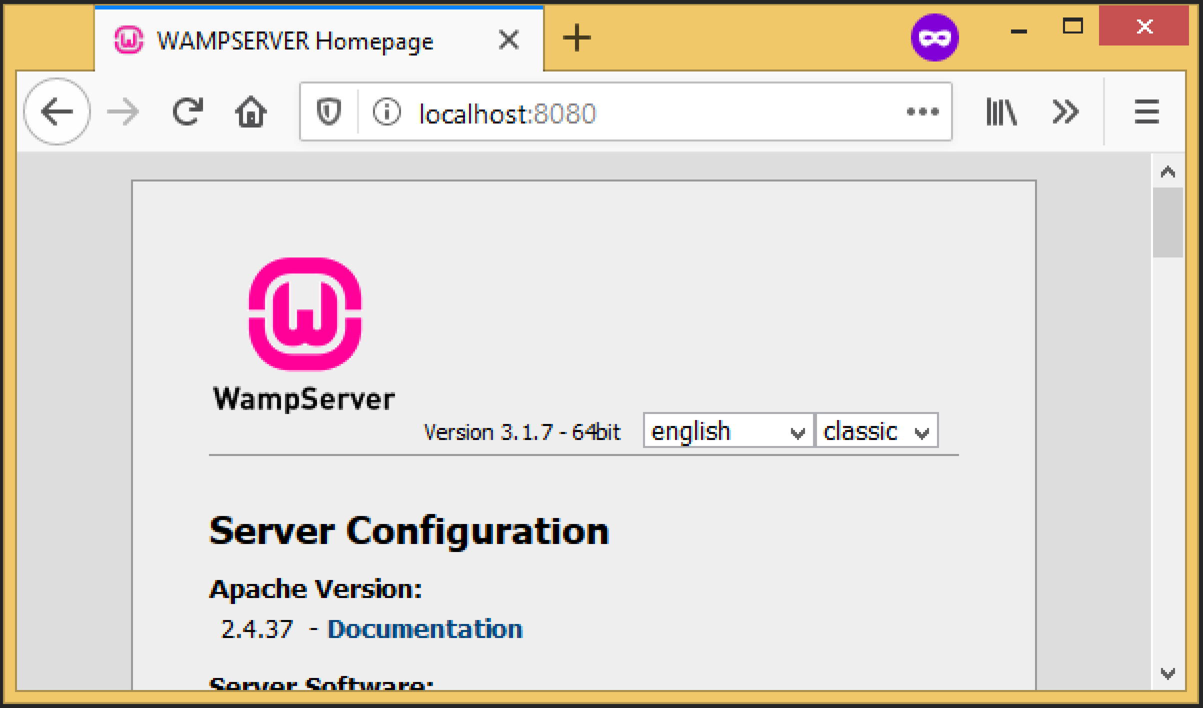
HTTP Server - WAMP (Windows Apache MySQL PHP in one)

- Download from http://www.wampserver.com/en/

Important: Use a different port for WAMP to avoid port conflict with IIS (if installed and working).

- Install and launch the program
- Open Web Browser > http://localhost or http://COMPUTERNAME

Important: If the web server is running on a different port (other than default port 80), then use http://COMPUTERNAME:PORT# (for example: http://LAB01:8080 (Colon format applicable for web browsers).



Server Configuration

Apache Version:

2.4.37 - Documentation

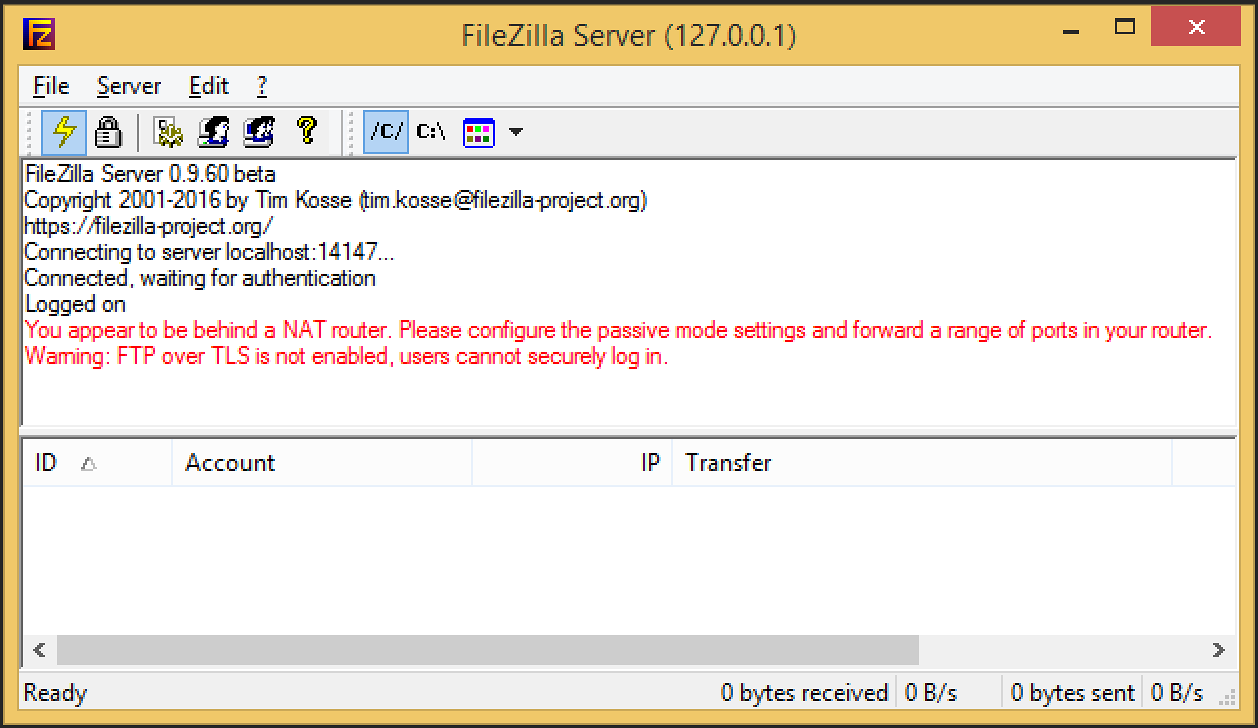
Server Software:

Apache Web Service listening on Port 8080

Note: Use TELNET to check for open ports.

FTP Server - FileZilla

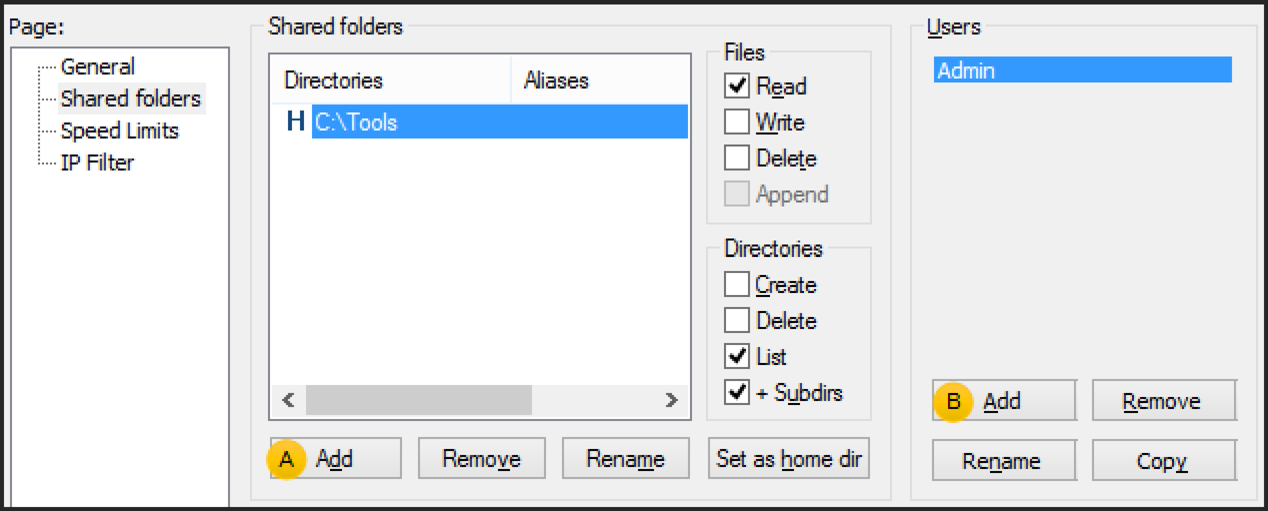
- Download FileZilla Server from https://filezilla-project.org/
- Install and launch the program & Logon.



```
FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
```

Ready | 0 bytes received | 0 B/s | 0 bytes sent | 0 B/s

Administrative interface of Filezilla



Directories: H C:\Tools

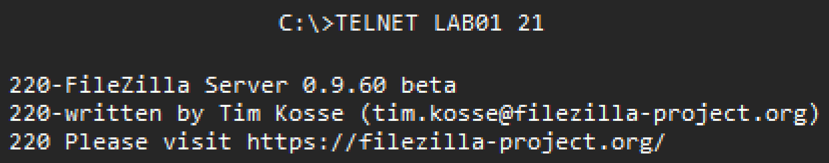
Users: Admin

Files: ☑ Read ☐ Write ☐ Delete ☐ Append

Directories: ☐ Create ☐ Delete ☑ List ☑ + Subdirs

- Setup root directory
  - Select Add > Select a Folder (For example: C:\Tools)
- Create FTP User Account
  - Edit > Users > Add (for example: Admin)

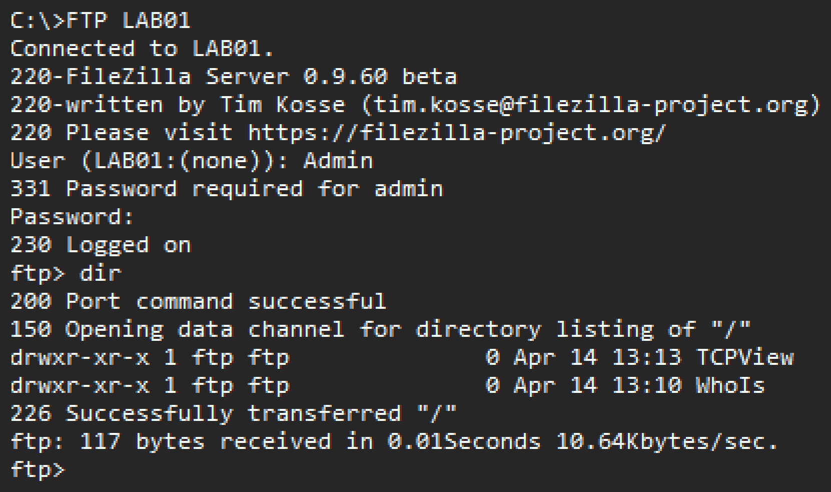
- Test for open ports:
  - CMD > TELNET COMPUTERNAME 21



```
                                C:\>TELNET LAB01 21

220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
```

Example: FTP Service running on “LAB01” on Port “21”

- To Connect to a FTP Server:
  - CMD > FTP COMPUTERNAME
  - Specify Credentials



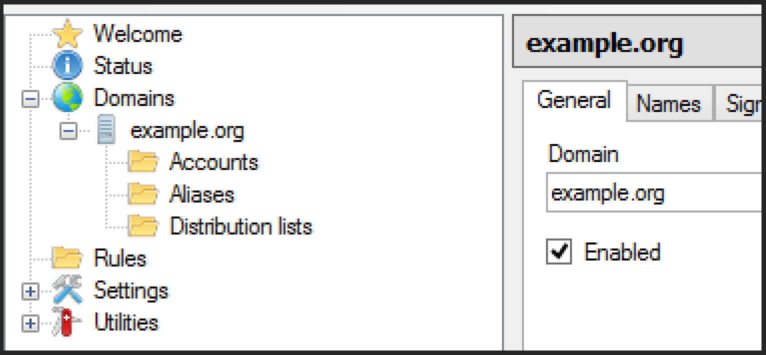
```
C:\>FTP LAB01
Connected to LAB01.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
User (LAB01:(none)): Admin
331 Password required for admin
Password:
230 Logged on
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp              0 Apr 14 13:13 TCPView
drwxr-xr-x 1 ftp ftp              0 Apr 14 13:10 WhoIs
226 Successfully transferred "/"
ftp: 117 bytes received in 0.01Seconds 10.64Kbytes/sec.
ftp>
```

Connected to an FTP Server, Directory Listing using DIR Command

Mail Server - HMAILSERVER

HMAILSERVER is a popular & powerful open source email server, suitable for home & small networks.

- Download from https://www.hmailserver.com
- Install and launch the program
- Select Add domain…
- Specify a domain name, for example: example.org
- Select "Save"

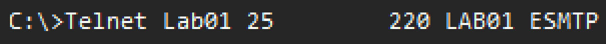


Domain: example.org

☑ Enabled

Popup to connect in administrative mode

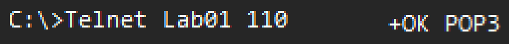
- Test for open ports:
  - SMTP: CMD > Telnet COMPUTERNAME 25



```
C:\>Telnet Lab01 25        220 LAB01 ESMTP
```

Example: SMTP Service running on "LAB01" on Port "25"

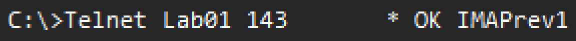
  - POP3: CMD > Telnet COMPUTERNAME 110



```
C:\>Telnet Lab01 110        +OK POP3
```

Example: POP3 Service running on "LAB01" on Port "110"

  - IMAP: CMD > Telnet COMPUTERNAME 143



```
C:\>Telnet Lab01 143        * OK IMAPrev1
```

Example: IMAP Service running on "LAB01" on Port "143"

- Check Mail Servers

  - SMTP: Telnet DOMAINNAME PORT (Example: Telnet mail.domainname.extension 25)
  - POP3: Telnet DOMAINNAME PORT (Example: Telnet mail.domainname.extension 110)
  - IMAP: Telnet DOMAINNAME PORT (Example: Telnet mail.domainname.extension 143)

Note: Output message might vary depending on respective server software; refer service provider website for exact port numbers as it usually varies (default ports may not respond if modified).

- If POP3 service is set to 443 on mail.domainname.extension, then:
  - CMD > Telnet mail.domainname.extension 443

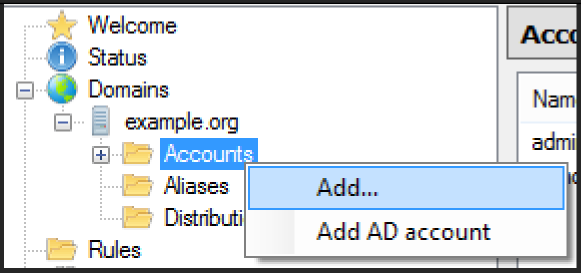
Email Client - Thunderbird

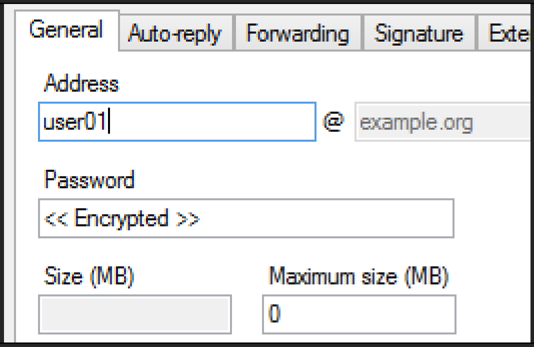
Mozilla Thunderbird is an open source & free email client, suitable for home & office networks.

- Download from https://www.thunderbird.net
- Install Mozilla Thunderbird

Create email accounts in HMAILSERVER

- Launch HMAILSERVER Administrator
- Expand domains, Select a domain
- Right-Click Accounts, Select Add





Address
user01 @ example.org

Password
<< Encrypted >>

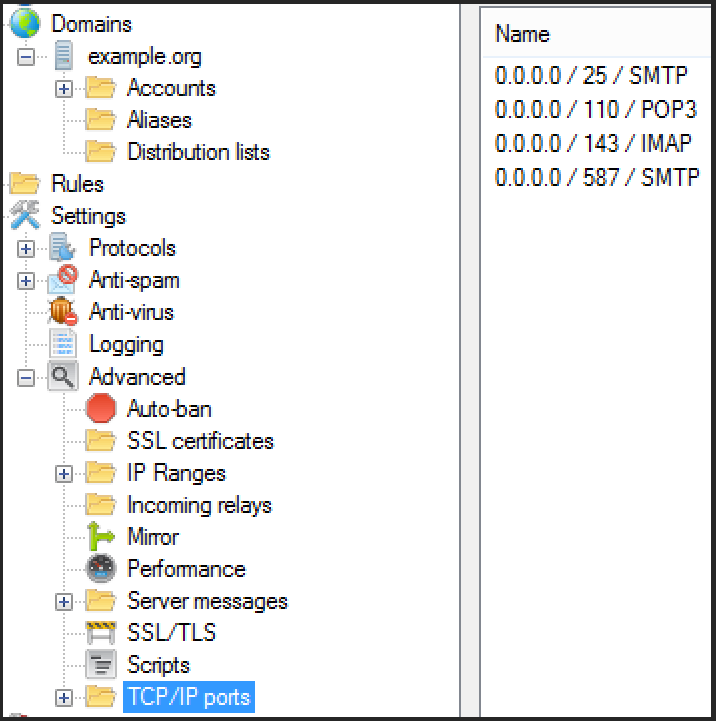
Size (MB)

Maximum size (MB)
0

- Specify an account name (for example, user01), set a password & select “Save”

To view (or modify) port numbers for HMAILSERVER

- Expand Domains, Expand Settings, Select TCP/IP Ports

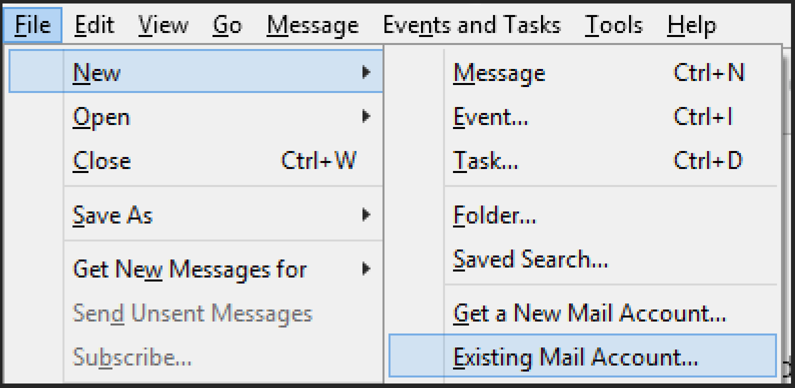


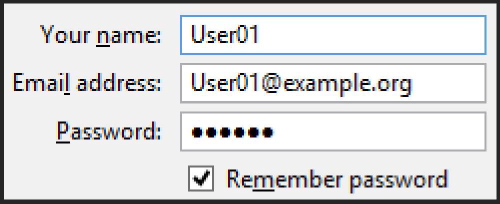
Name
0.0.0.0 / 25 / SMTP
0.0.0.0 / 110 / POP3
0.0.0.0 / 143 / IMAP
0.0.0.0 / 587 / SMTP

HMAILSERVER Settings

Set up email account in Mozilla Thunderbird

- Launch Mozilla Thunderbird
- Select File > New > Existing Mail Account…





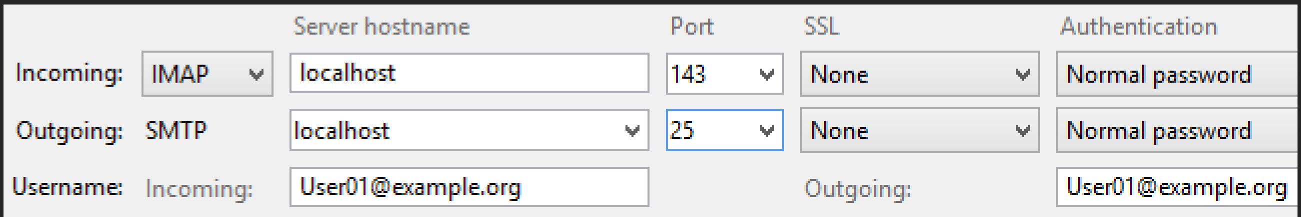
Your name: User01

Email address: User01@example.org

Password: ●●●●●●

☑ Remember password

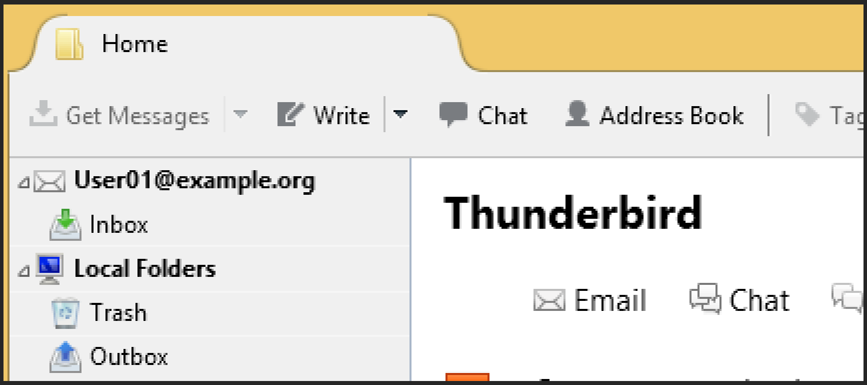
- Enter Name, Email address & password, Select Continue
- Select Manual Config



		Server hostname	Port	SSL	Authentication
Incoming:	IMAP	localhost	143	None	Normal password
Outgoing:	SMTP	localhost	25	None	Normal password
Username:	Incoming:	User01@example.org		Outgoing:	User01@example.org

Mail settings

- Specify settings as per server
- Select "Done"



Note: Repeat the procedure to create & add multiple email accounts; specify computer name or IP address if setting up on LAN. Multiple email accounts can be setup on a single computer if required.

Wi-Fi Analyzers

Wireless Site Survey is a technique used for analyzing, planning & designing wireless networks; parameters such as speed, signal strength, etc. are used to estimate wireless equipment needs and placement of wireless access points.

Though technical expertise is required, there are simple tools available to get a high-level overview of current setup and modify the network setup if required (whether to use different channels, extend network by adding wireless extenders, etc.).

- For Desktops & Laptops
    - Download from https://www.vistumbler.net/
    - Extract to C:\Tools\Vistumbler_v10-6-5_Portable
    - Launch Vistumbler.exe
    - Select Scan APs, Observe output
- For Android
    - Download https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer
    - Install & Launch program, Observe output

General Practices & Tips

“Computer”, “Network” or “Internet” not working is NOT a clear definition of a problem; appropriate probing always helps in isolating a problem and to determine a permanent solution. Devices such as desktops, laptops & smartphone are usually connected to the internal network at very high speeds yet a single Internet connectivity is shared across all the devices. Activities such as downloading large files, system updates, etc. generally use a lot of bandwidth as compared to standard use such as browsing the Internet. Estimate the actual bandwidth required for all devices in a network, check if the selected Internet plan is adequate.

Most small networks are very similar and it is recommended to have a standard approach such as basic network diagram or a checklist to understand the exact environment which helps in isolating problems quickly and effectively.

Basic Setup	
Network Type: Home / Office	
# of Desktops	
# of Laptops	
# of Smartphone	
# of SOHO Routers	
# of Wireless Access Points	
# of Printers / All-In-Ones	
# of NAS	
# of Gaming Console (If Internet connectivity required)	
# of Smart Televisions	
# of Other Devices that require Internet Connectivity (Security Cameras, etc.)	
# of Wired Connections	
# of Wireless Connections	
Internet Connectivity	
# of Internet Connectivity (If multiple connections available)	
Internet Plan	
Internet Speed (Required)	
Internet Speed (Available)	

Basic Data Collection Sample

- Use exact error messages (do NOT try to trim or use parts of error messages) if available, for further research on the Internet or manufacturer or technical websites.
- Do NOT neglect any outages (planned or unplanned) from a service provider, as that is critical to understand a scenario before beginning to troubleshoot - particularly if all devices in a network are affected.

Product Specific Issues:

- Always update to the latest device driver, only from well known source.
- Check and update Firmware on SOHO Routers & Network/Internet related devices.

Most product specific issues may be well known to a manufacturer; it is highly recommended to refer manufacturer’s support website or knowledge-base first before attempting to troubleshoot as it can save time. Referring 3rd party forums/blogs can solve some issues, but identifying the right forum/expert may take time.

OSI Model based Troubleshooting (Basic)

Some common issues:

- Unable to connect to the Internet
- Unable to use a particular network application
- Unable to access another computer on the same network
- Unable to access shared folders or printers

General questions:

- Was it working before?
- Any recent changes made?
- Does it happen to a single computer or all computers?
- Is it application specific?
- If it's slow, how many active wired and/or wireless connections? Is the guest access enabled?

Note: Some software might include one or more 3rd party software to be installed without user's knowledge which may cause specific issues such as automatic redirection in a browser, blocking services or applications, or even technical issues in operating systems; in such cases, use add/remove programs to filter and remove such programs if necessary.

For effective troubleshooting, it is recommended to follow a standard approach such as:

- Physical Layer
  - Wired
    - Check if the SOHO Router / Network switch is turned on
    - Check if the SOHO Router has Internet connectivity
      - Solutions
        - Check Internet Status by logging on to the Router or status indicator
        - Check for any loose connections or DSL filter issues (Replace filter)
        - Restart the Router
    - Check if network cable is secure (no loose pins or damaged RJ-45 Jacks) at both ends
      - Solutions
        - Use alternate patch cable
  - Wireless
    - Check if signal strength is good or below average
    - Check placement of Wi-Fi Routers or Access Points or hotspots
    - Check if there are other devices causing interference to the signal
    - Solutions (Analyze using Wi-Fi Analyzers)
      - Turn Off interfering devices
      - Adjust SOHO Router or Access Point location (Placement of antennas)
      - Use a less crowded channel
      - Use 5 GHz (if available) if there are many 2.4 GHz based devices
- Data Link Layer
  - Check if the NIC is installed & Working properly
    - Solution
      - Use Device Manager to check NIC status
      - Update Device Drivers (or rollback if an update has caused the problem)
      - Re-install Device Drivers
      - Use a different NIC (or a different slot if it's PCI/PCIe or different port if it's USB adapter)
  - Check for incorrect settings or changes made to the NIC
- Network Layer
  - Check DHCP service is enabled on the SOHO Router
  - Check if the Network Adapters have valid IP addresses
  - Check if the Network Adapter has a valid IP address & Gateway
  - Check if the Network Adapter has valid DNS servers
  - Check if there are any issues communicating to Default Gateway
  - Check if the website is actually working
  - Check if DNS server is reachable & resolving domain names
    - Solutions
      - Use ipconfig /release & ipconfig /renew
      - Use Static IP Address & Gateway (If DHCP is NOT working) - Assign IP in the same same range of SOHO Router
      - Use public DNS Servers for faster name resolution, such as:
        - Google Public DNS - 8.8.8.8 (Primary) & 8.8.4.4 (Secondary)
        - OpenDNS Home - 208.67.222.222 (Primary) & 208.67.220.220 (Secondary)
- Transport, Session Layer, Presentation & Application Layer
    - Check Network Application Specific settings
      - Web Browser
        - Determine if it is very slow or no connectivity at all
        - Close unwanted tabs & Windows
        - Use an alternate browser to check, if available
        - Check another website, not all websites serve content at super speeds
        - Clear Browser Cache
        - Disable Browser Plugins
      - Email Application

- Match Email Settings as per ISP
- Check Webmail access, if email application is not working
- Check POP3 / IMAP / SMTP, Security & Authentication Settings

- 3rd Party Applications
  - Determine application settings as per vendor including port numbers
- Check if Anti-Virus or Firewall is active & blocking any connections
  - Solutions
    - Disable Anti-Virus & Firewall Temporarily and Check
    - Add Executable/Service to exception list of Anti-Virus & Firewall as required
    - Enable Anti-Virus & Firewall

Unable to access another computer (not Internet), File Sharing Service (Microsoft Windows)

- Check if the Network is set to “Private”
- Check if the Network Adapters have valid IP addresses
- Check Computer Name (Spelling)
- Check Network Connectivity between computers by Computer Name
- Check if it’s accessible by IPv4
- Check if NETBIOS over TCP/IP is enabled
- Check for Authentication issues (User accounts & Passwords)
- Check if the remote folder is shared & appropriate permissions are set
- Check Share Name (May not be same as a the folder name)
- Solutions
  - Create a new user account for file & print sharing purposes
  - Use HOSTS file to map IPv4 to computer names
  - Add File & Print Sharing Services to Firewall Exceptions List

Unable to connect to a printer on another computer, Print Sharing Service (Microsoft Windows)

- Check Share Name (May not be same as a the printer name)
- Check Printer Permissions (Sharing)

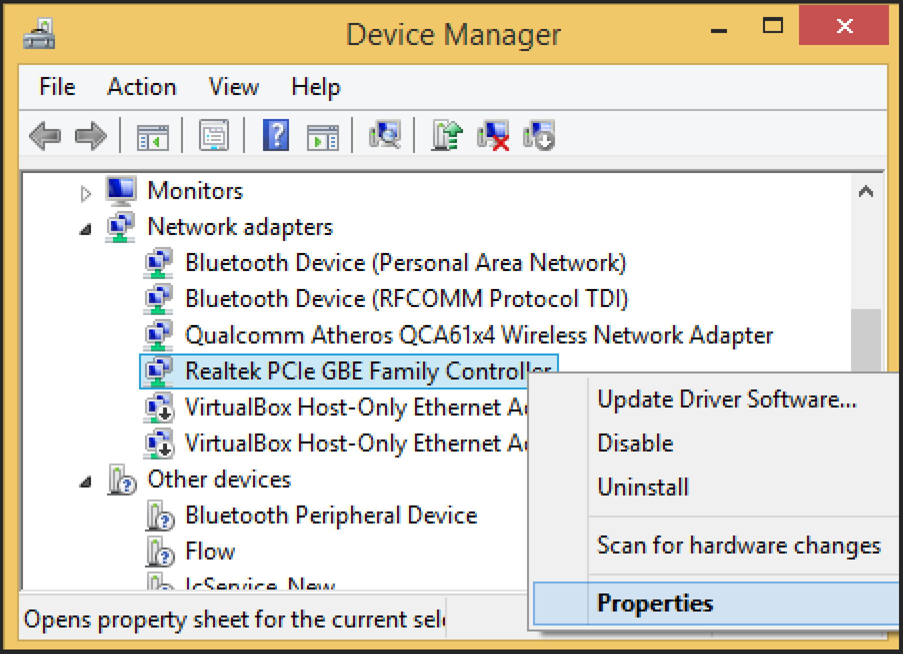
Note: Above is NOT applicable for network printers connected to a network switch; applicable only for printers that are connected directly to a computer with Microsoft Windows.

Using Device Manager

- Management console to manage hardware devices
- Has pre-defined error codes, ease of troubleshooting

“Device Drivers” or “Drivers” refers to software that controls the hardware.

- START > RUN > DEVMGMT.MSC


Device Manager
File
Action
View
Help
Monitors
Network adapters
Bluetooth Device (Personal Area Network)
Bluetooth Device (RFCOMM Protocol TDI)
Qualcomm Atheros QCA61x4 Wireless Network Adapter
Realtek PCIe GBE Family Controller
VirtualBox Host-Only Ethernet A
VirtualBox Host-Only Ethernet A
Other devices
Bluetooth Peripheral Device
Flow
IcService New
Update Driver Software...
Disable
Uninstall
Scan for hardware changes
Properties

Opens property sheet for the current sel

Device manager listing devices

- Select an NIC, Right-Click & Select “Properties”
- Check message under “Device Status”

Reference(s):

- Go to https://support.microsoft.com
- Refer KB 310123

Steps to install an NIC

1. Insert the NIC (PCI/PCIe/USB)
2. Install Device Drivers &
3. Modify Settings (Only if required)
4. Insert cable (Wired NIC)
5. Select SSID (Wireless NIC)

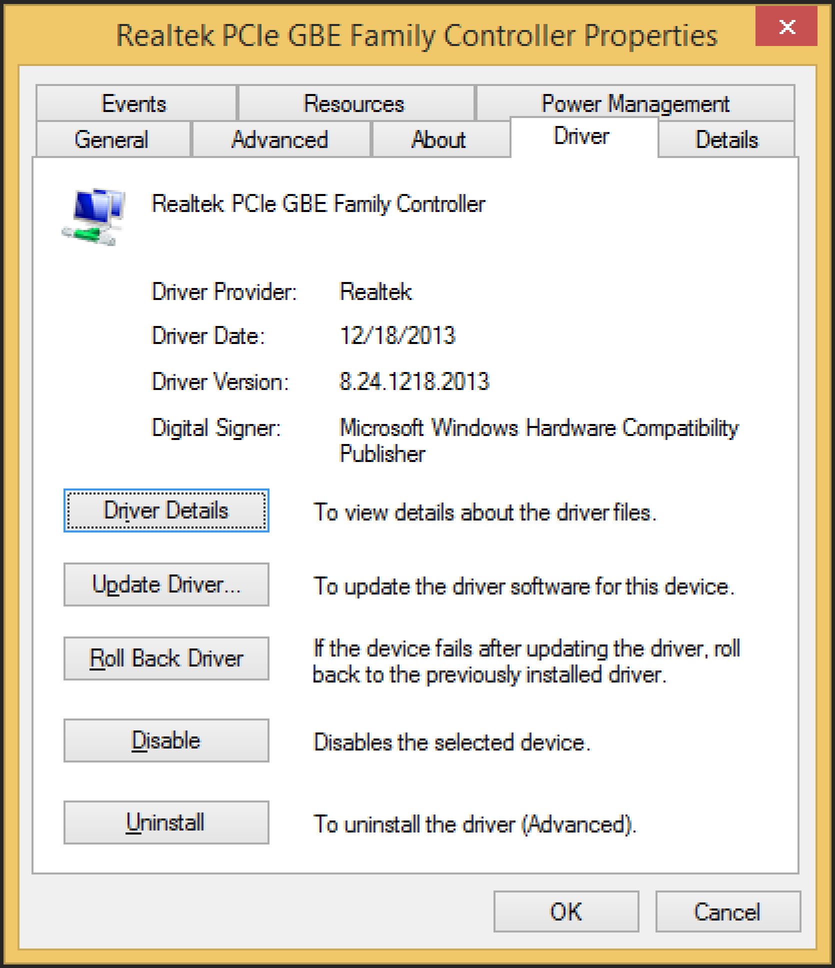
Most recent versions of Microsoft Windows, Linux are designed to detect, install device drivers and configure device automatically (device drivers for many models are included with the operating system package), but this may not work for recently released devices (as device drivers may not be available within the OS package). In such cases, device drivers may be installed from the CD/DVD included with the device package or, device drivers can be downloaded through Windows Update or, device drivers can be downloaded from respective vendor website to complete the installation.

Package types from vendors:

- Ready-to-install packages are usually available from most vendors, that should be downloaded and installed. Recommended for most users, as it requires minimal technical intervention.
- Driver Only Package (usually smaller in size) requires administrator efforts for installations; use Update Driver option in Device Manager (Microsoft Windows) to install device driver.

To view device driver details:

- START > RUN > DEVMGMT.MSC
- Select Driver tab



Realtek PCIe GBE Family Controller Properties

Realtek PCIe GBE Family Controller

Driver Provider: Realtek

Driver Date: 12/18/2013

Driver Version: 8.24.1218.2013

Digital Signer: Microsoft Windows Hardware Compatibility Publisher

Driver Details — To view details about the driver files.

Update Driver... — To update the driver software for this device.

Roll Back Driver — If the device fails after updating the driver, roll back to the previously installed driver.

Disable — Disables the selected device.

Uninstall — To uninstall the driver (Advanced).

Driver tab

Common Issues:

A. Unknown device (Device listed like “PCI Device” with no further details)
   a) Check the Model/Manufacturer of the NIC
   b) Download appropriate drivers (Select exact Operating System / 32 or 64 bit version)
   c) Select Update Driver
   d) Point to the folder where drivers are extracted

B. Yellow Question Mark (devices drivers not installed)

- To install and/or update device drivers
  - Select “Update Driver Software…”
  - Options
    - Select “Search automatically for updated driver software…” - Latest devices drivers will be automatically installed if available.
    - Select “Browse my computer for driver software” - use this if the device driver has been downloaded from vendor’s website (use this method if the device drivers are downloaded and/or available through CD/DVD).

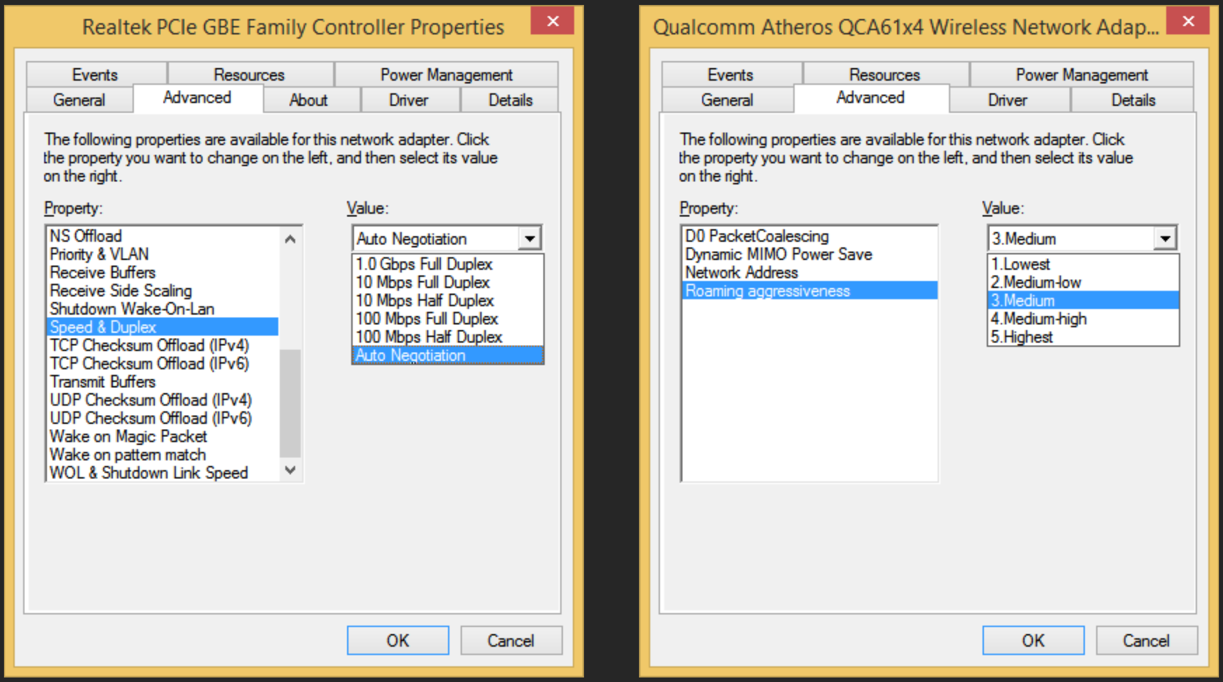
- To Re-install NIC
  - Right-Click on a device
  - Select “Uninstall”
  - Select “Scan for hardware changes” (or restart computer)

Sometimes an updated device driver may cause specific problems; in such scenarios, previous version of a device driver (restore is possible only if the previous device driver was updated, not on a fresh installation) can be restored through the Rollback driver option.

- Select NIC, Right-Click & Select “Properties”
- Select “Driver” Tab
- Select “Roll Back Driver”

Tip: Always check a) Windows Update b) Vendor website for device drivers. Never download drivers from unknown sources as it may cause other problems. Download specific device driver version if required.

- Check NIC Settings
  - START > RUN > DEVMGMT.MSC
  - Select NIC, Right-Click & Select “Properties”
  - Select “Advanced” Tab



Realtek PCIe GBE Family Controller Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- NS Offload
- Priority & VLAN
- Receive Buffers
- Receive Side Scaling
- Shutdown Wake-On-Lan
- Speed & Duplex
- TCP Checksum Offload (IPv4)
- TCP Checksum Offload (IPv6)
- Transmit Buffers
- UDP Checksum Offload (IPv4)
- UDP Checksum Offload (IPv6)
- Wake on Magic Packet
- Wake on pattern match
- WOL & Shutdown Link Speed

Value: Auto Negotiation

- 1.0 Gbps Full Duplex
- 10 Mbps Full Duplex
- 10 Mbps Half Duplex
- 100 Mbps Full Duplex
- 100 Mbps Half Duplex
- Auto Negotiation

Qualcomm Atheros QCA61x4 Wireless Network Adap...

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- D0 PacketCoalescing
- Dynamic MIMO Power Save
- Network Address
- Roaming aggressiveness

Value: 3.Medium

- 1.Lowest
- 2.Medium-low
- 3.Medium
- 4.Medium-high
- 5.Highest

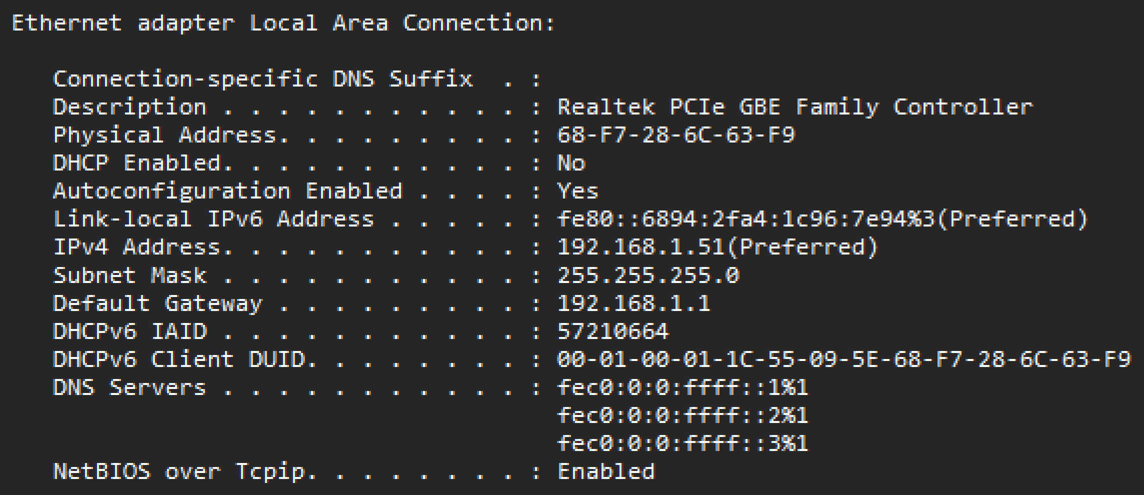
Settings of a wired NIC (Left) and Wireless NIC (Right)

Note: Settings may differ depending on the model, requires technical expertise to modify. It is highly recommended to leave the settings to “AUTO”; this means the settings will be managed by the operating system. If unsure, reinstall the NIC. MODIFY THESE SETTINGS, only if you have a clear understanding.

- Assign Static IP Address & Gateway (If DHCP server has not assigned any IP address or if you prefer to use static IP address):
  - CMD > netsh interface ipv4 set address ”CONNECTIONNAME” static ipv4 subnet mask gateway

```
C:\netsh interface ipv4 set address “Local Area Connection” static 192.168.1.51
                          255.255.255.0 192.168.1.1
```

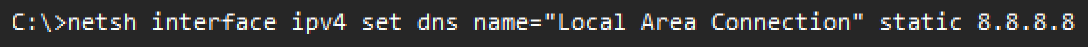
Sample input to setup an IPv4 Address



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.51(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

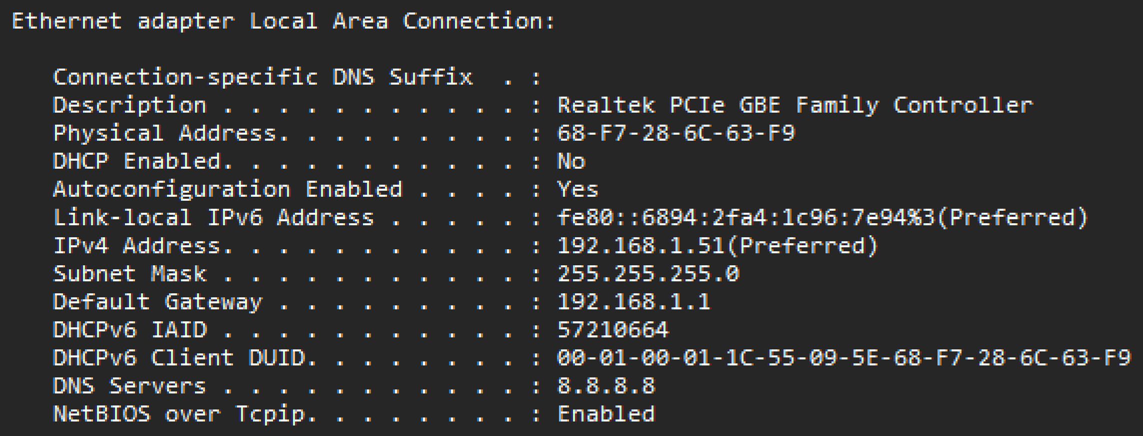
Sample Output displaying DHCP Status as disabled and, assigned static Pv4 address

- Assign static DNS IPv4 address via command line:
  - CMD > netsh interface ipv4 set dns name=”CONNECTIONNAME”static DNSIP1



```
C:\>netsh interface ipv4 set dns name="Local Area Connection" static 8.8.8.8
```

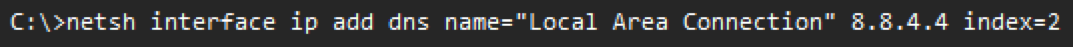
Sample input to use 8.8.8.8 as the primary DNS server



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 68-F7-28-6C-63-F9
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.51(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 57210664
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-55-09-5E-68-F7-28-6C-63-F9
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Output listing DNS Server IPv4 Address

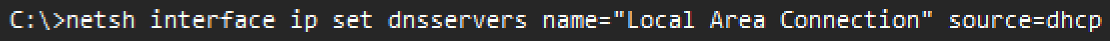
  - CMD > netsh interface ip add dns name=”CONNECTIONNAME” DNSIP2 index=x



```
C:\>netsh interface ip add dns name="Local Area Connection" 8.8.4.4 index=2
```

Sample Input to add secondary DNS

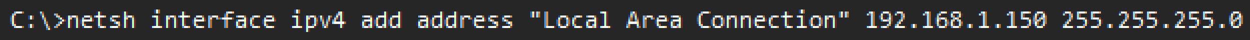
- Use DNS Servers from DHCP settings
  - CMD > netsh interface ip set dnsservers name="CONNECTIONNAME" source=dhcp



```
C:\>netsh interface ip set dnsservers name="Local Area Connection" source=dhcp
```

Input to use DNS servers from DHCP

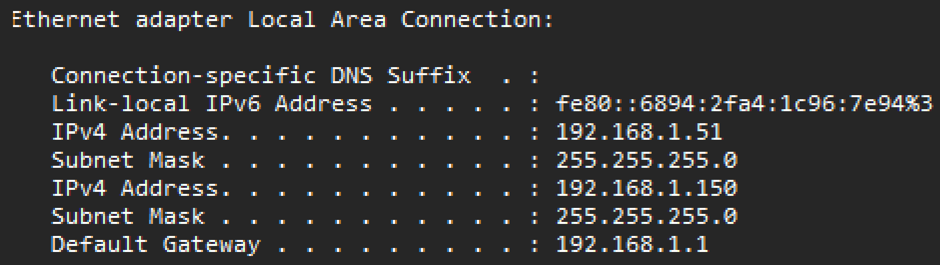
- Add second IPv4 address
  - CMD > netsh interface ipv4 add address "CONNECTIONNAME" IPv4 Subnet Mask Gateway



```
C:\>netsh interface ipv4 add address "Local Area Connection" 192.168.1.150 255.255.255.0
```

Input to add second IPv4 address

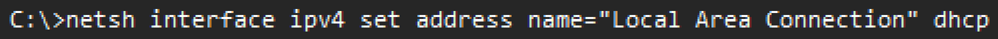
  - CMD > ipconfig



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6894:2fa4:1c96:7e94%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.51
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 192.168.1.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Output listing two IPv4 addresses assigned to a single connection

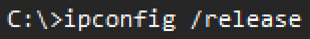
- Enable DHCP Client:
  - CMD > netsh interface ipv4 set address name=”CONNECTIONNAME” dhcp



```
C:\>netsh interface ipv4 set address name="Local Area Connection" dhcp
```

Sample input to enable DHCP client

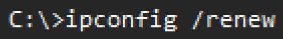
- Force IPv4 address to be released (before requesting for a new IP address)
  - CMD > ipconfig /release



```
C:\>ipconfig /release
```

Input to release existing dynamic IP address (only on DHCP Clients)

- Request for IPv4 address
  - CMD > ipconfig /renew



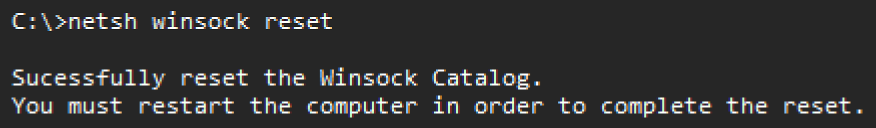
```
C:\>ipconfig /renew
```

Input to request for a IP address (only on DHCP Clients)

Note: DHCP client may be offered the same IP address as before, if that IP is not leased to any other client. DHCP Client can receive the same IP address, if it’s reserved on a DHCP Server.

Tip: Any number of IP addresses can be added to a single network card, though there may be technical limitations imposed through operating system.

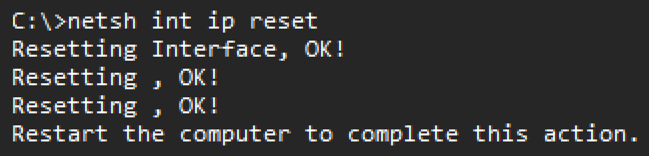
- Advanced Troubleshooting
  - Reset Windows Socket
    - CMD > netsh winsock reset



```
C:\>netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

Input to reset Windows Socket

  - Reset TCP/IP
    - CMD > netsh int ip reset



```
C:\>netsh int ip reset
Resetting Interface, OK!
Resetting , OK!
Resetting , OK!
Restart the computer to complete this action.
```

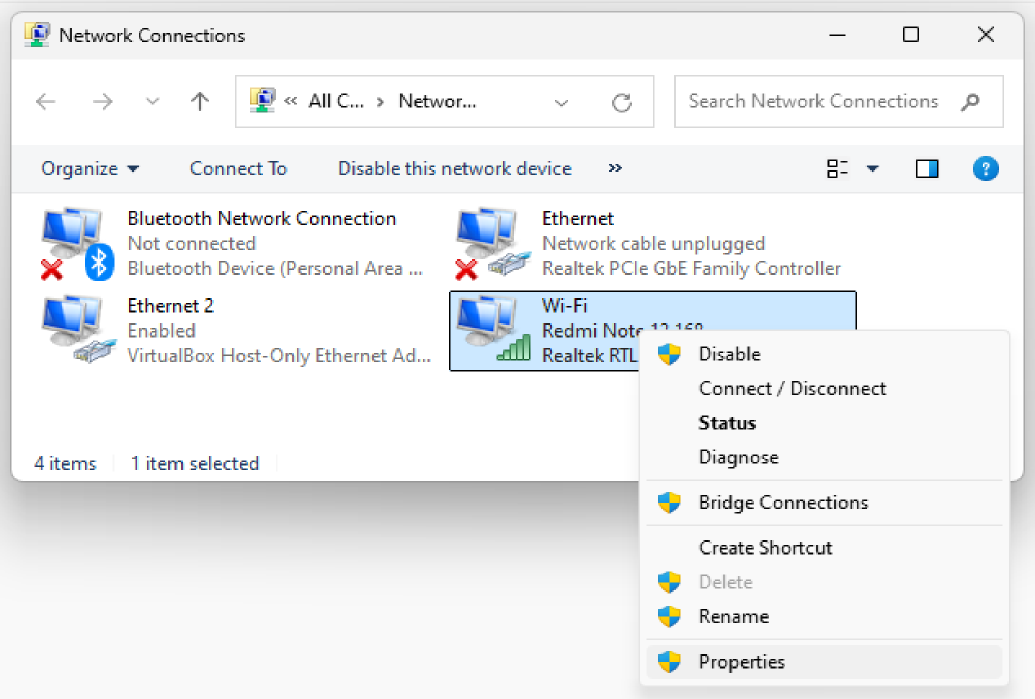
Input to reset TCP/IP

  - Restart computer

- To create a log file for reference:
  - CMD > netsh int ip reset > C:\Log.txt

To assign static IP via GUI:

- START > NCPA.CPL



Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

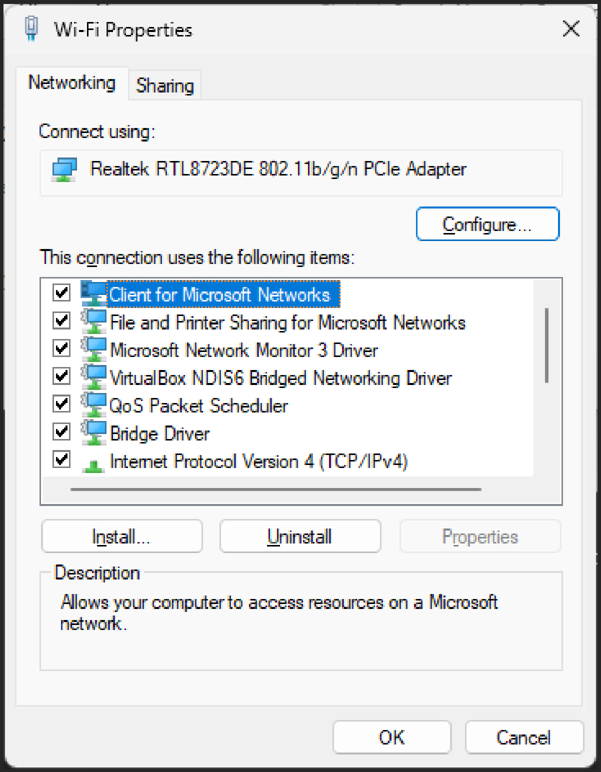
Ethernet
Network cable unplugged
Realtek PCIe GbE Family Controller

Ethernet 2
Enabled
VirtualBox Host-Only Ethernet Ad...

Wi-Fi
Redmi Note 12 169
Realtek RTL

4 items | 1 item selected

- Select an existing connection and select Properties



Connect using:

Realtek RTL8723DE 802.11b/g/n PCIe Adapter

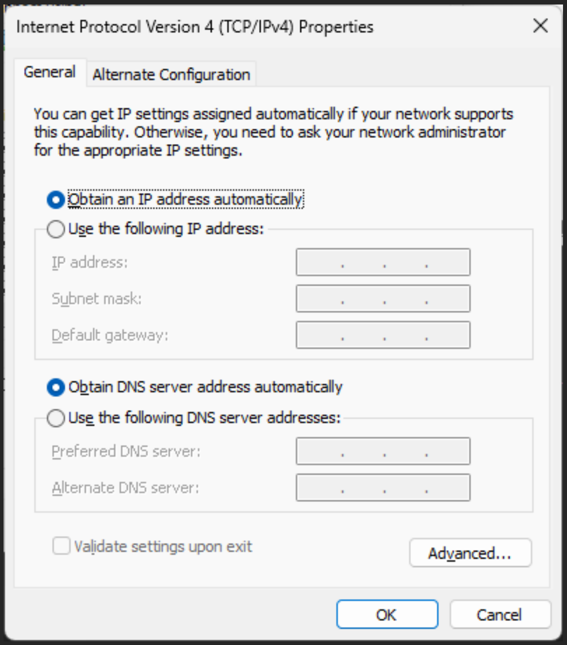
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Microsoft Network Monitor 3 Driver
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ QoS Packet Scheduler
- ☑ Bridge Driver
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Allows your computer to access resources on a Microsoft network.

- Select Internet Protocol Version 4 (TCP/IPv4), select Properties



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

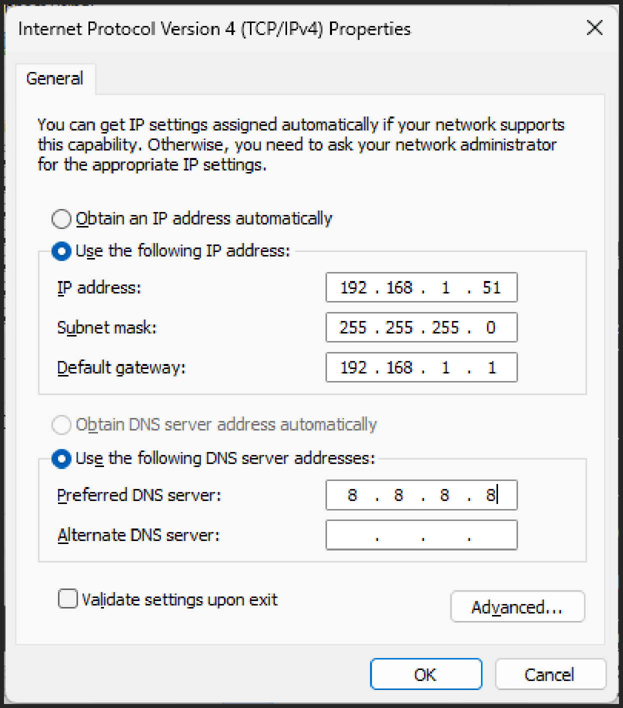
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 51

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

□ Validate settings upon exit

- Select OK Twice to save.

Addressing SOHO Router Problems

Similar to a computer, a SOHO Router has a CPU+ROM+RAM and a micro operating system to manage all the internal operations of a Router. Most routers are never turned off, which may cause unknown and/or unexplainable issues due to prolonged use; in such scenarios, perform a cold reboot and confirm if the issue is resolved.

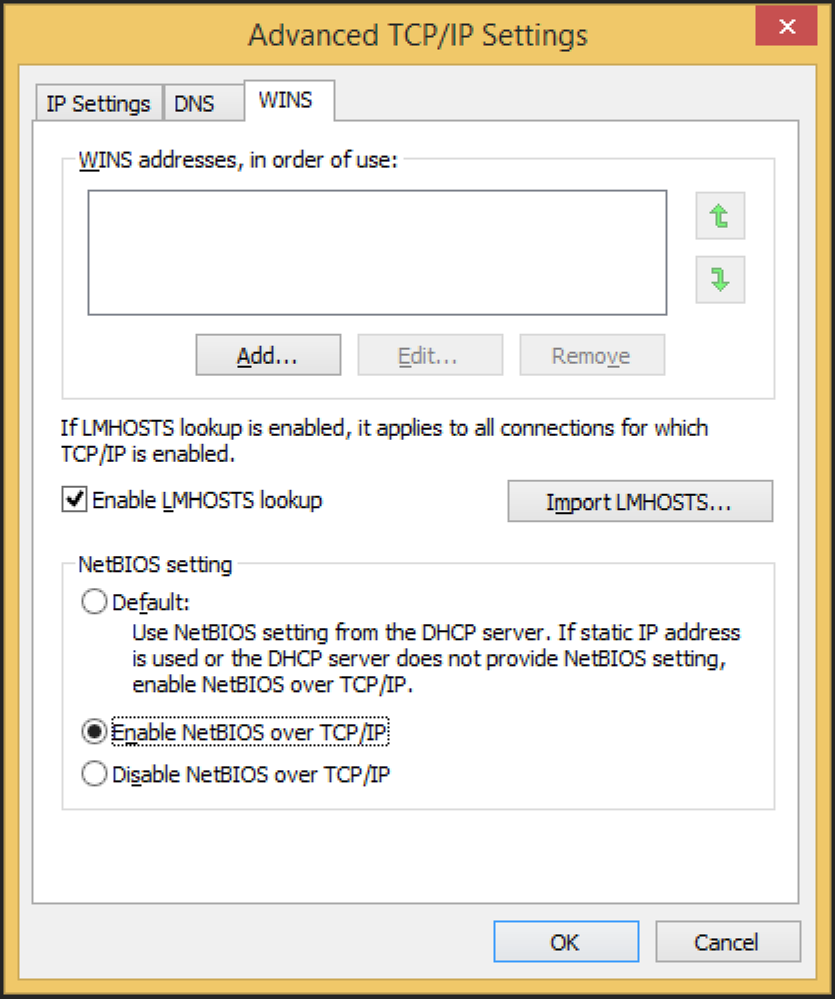
Some manufacturers fix specific issues and release updated micro operating systems referred to as “Firmware” time-to-time, which should be updated on a case to case basis if available. SOHO Routers can also be reset to factory settings, but details related to network & ISP settings must be available to reconfigure (if required). Updating Firmware requires technical expertise, it is recommended to take extra caution.

Tip: Download Firmware only from Manufacturer’s website. Make sure a. correct model/firmware is downloaded and b. there are NO power outage or disconnects during firmware update, as it may damage the device.

Server Message Block

- SMB is a network protocol that enables file sharing, printer sharing, and resource sharing on Microsoft Windows networks.
- Uses TCP/UDP ports 137, 138, 139, and 445, with port 445 being the primary one for modern implementations.

- To check settings for NETBIOS over TCP/IP:
  - START > RUN > NCPA.CPL, Right-click “Local Area Connection” & Select “Properties”
  - Select “Internet Protocol Version 4 (TCP/IP)” & Select “Properties”
  - Select “Advanced” & Select “WINS” Tab



Advanced TCP/IP Settings

WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

● Enable NetBIOS over TCP/IP

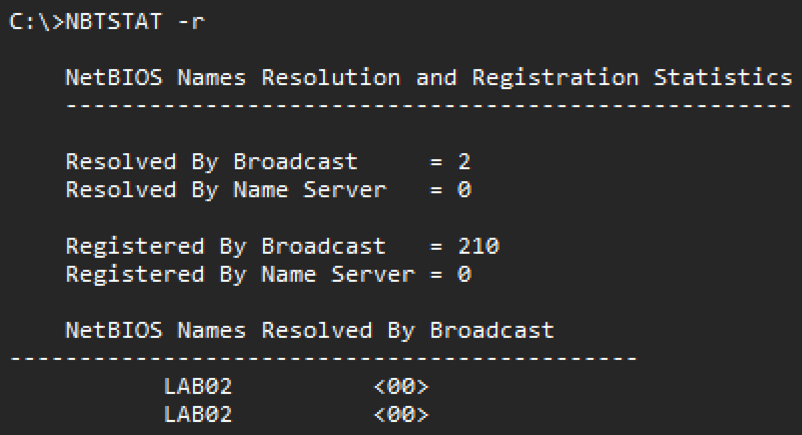
○ Disable NetBIOS over TCP/IP

TCP/IP settings, Enable NETBIOS over TCP/IP option

- Select “Enable NetBIOS over TCP/IP”, Select “OK” Twice
- Select “Close”

NBTSTAT is a utility for troubleshooting NetBIOS over TCP/IP (Microsoft Windows based networks).

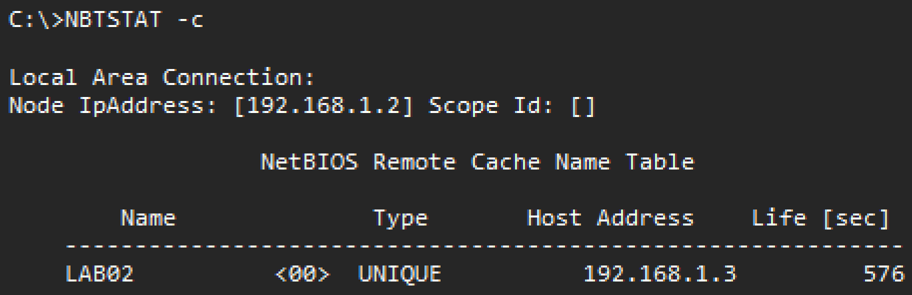
- View Statistics
  - CMD > nbtstat -r



```
C:\>NBTSTAT -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 2
    Resolved By Name Server   = 0

    Registered By Broadcast   = 210
    Registered By Name Server = 0

    NetBIOS Names Resolved By Broadcast
---------------------------------------------
           LAB02          <00>
           LAB02          <00>
```

Input to view statistics

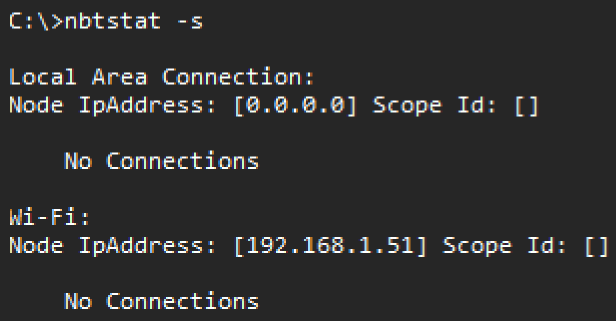
- View Cache
  - CMD > nbtstat -c



```
C:\>NBTSTAT -c

Local Area Connection:
Node IpAddress: [192.168.1.2] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    LAB02          <00>  UNIQUE          192.168.1.3         576
```

Input to view cache

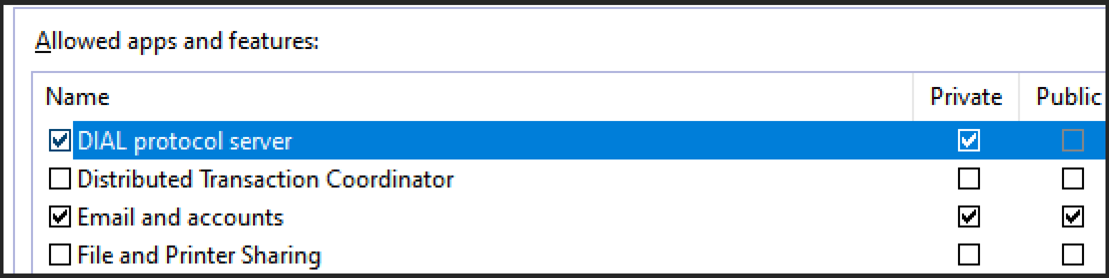
- View Sessions
  - CMD > nbtstat -s



```
C:\>nbtstat -s

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No Connections

Wi-Fi:
Node IpAddress: [192.168.1.51] Scope Id: []

    No Connections
```

Input to view sessions

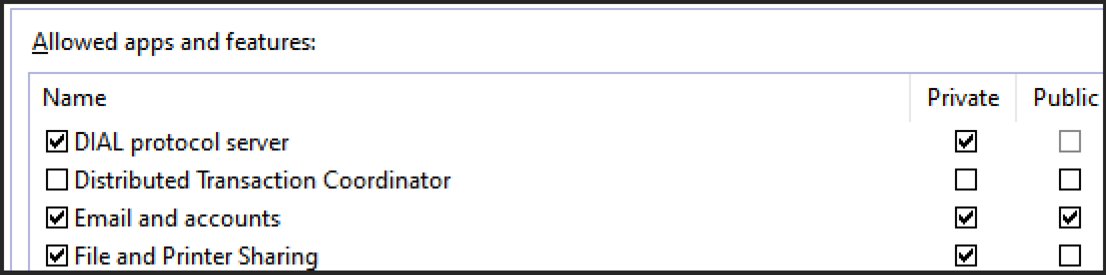
- Add File & Print Sharing Services to Windows Firewall Exceptions List
  - START > RUN > FiREWALL.CPL
  - Select “Allow an app or feature through Windows Defender Firewall”
  - Select “Change Settings”



Allowed apps and features:

Name	Private	Public
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Email and accounts	☑	☑
□ File and Printer Sharing	□	□

  - Scroll and locate “File and Printer Sharing”

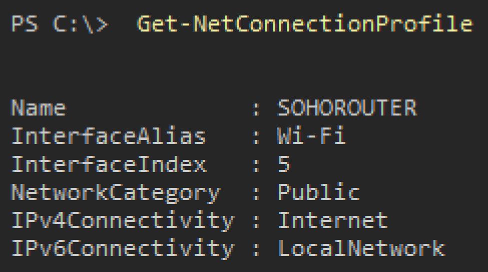


Allowed apps and features:

Name	Private	Public
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ Email and accounts	☑	☑
☑ File and Printer Sharing	☑	□

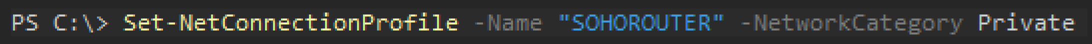
  - Check under Private, Select OK

- Change Public to Private Network via Powershell
  - CMD > Powershell
  - Powershell > Get-NetConnectionProfile



```
PS C:\>  Get-NetConnectionProfile


Name             : SOHOROUTER
InterfaceAlias   : Wi-Fi
InterfaceIndex   : 5
NetworkCategory  : Public
IPv4Connectivity : Internet
IPv6Connectivity : LocalNetwork
```

  - Powershell > Set-NetConnectionProfile -Name "CONNECTION" -NetworkCategory Private

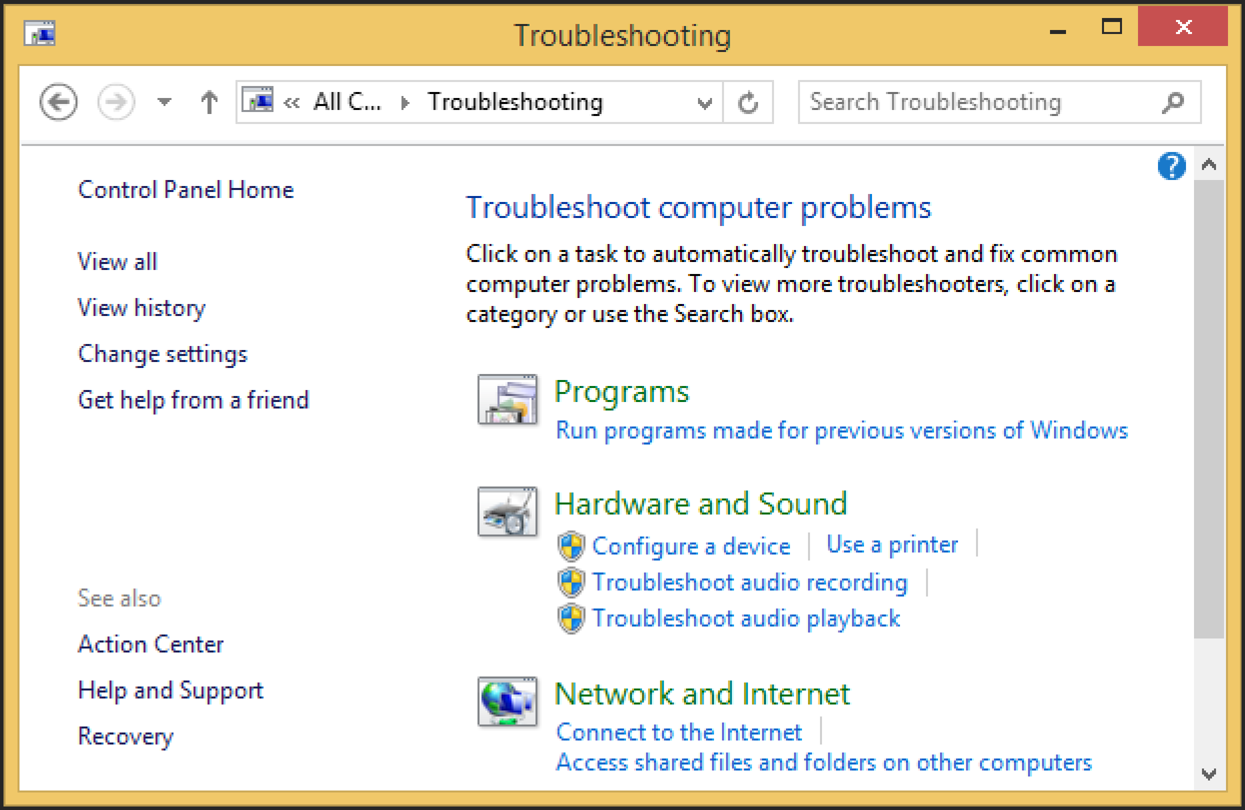


```
PS C:\> Set-NetConnectionProfile -Name "SOHOROUTER" -NetworkCategory Private
```

Using Troubleshooter

Troubleshooter included within the Operating System (Microsoft Windows) may be used for identifying and fixing certain issues.

- To launch troubleshooter:
  - Control Panel > Troubleshooting



Troubleshoot computer problems

Click on a task to automatically troubleshoot and fix common computer problems. To view more troubleshooters, click on a category or use the Search box.

Programs

Run programs made for previous versions of Windows

Hardware and Sound

Configure a device | Use a printer | Troubleshoot audio recording | Troubleshoot audio playback

Network and Internet

Connect to the Internet | Access shared files and folders on other computers

Troubleshooting Applet

- For example, select "Connect to the Internet" under Network and Internet to initiate troubleshooting Internet connectivity related issues.

Answer Keys

Quiz 01

1. Networking is best defined as:

A. Sharing of Resources
B. Connectivity between desktop computers
C. Connectivity between mobile computers
D. The Internet

2. Resources that can be shared in a network:

A. CD-ROM Drive
B. Hard Disk Drive
C. Internet Connectivity
D. All of the above

3. Maximum number of computers in a network:

A. 10
B. 20
C. 100
D. Unlimited

4. _____ defines network connectivity within a limited area such as a home or a small office network.

A. LAN
B. MAN
C. WAN
D. PAN

5. _____ defines network connectivity between networks within a city.

A. LAN
B. MAN
C. WAN
D. PAN

6. _____ defines network connectivity between networks across the globe.

A. LAN
B. MAN
C. WAN
D. PAN

7. Acronym - LAN.

A. Limited Area Network
B. Legacy Area Network
C. Local Area Network
D. Local Assisted Network

8. Acronym - WAN.

A. World Area Network
B. Wide Access Network
C. Wide Area Network
D. Wide Assisted Network

9. Acronym - MAN.

A. Mini Area Network
B. Metropolitan Area Network
C. Macro Area Network
D. Metropolitan Assisted Network

10. Acronym - PAN.

A. Professional Area Network
B. Personal Area Network
C. Pinned Area Network
D. Pinned Assisted Network

11. _____ refers to a computer that provide resources.

A. Client
B. Server
C. Mobile
D. Smart Net

12. _____ refers to computers that access resources.

A. Client
B. Server
C. Mobile
D. Smart Net

13. _____ model utilizes centralized security.

A. Personal Network B. Peer-to-Peer
C. Client-Server D. Mobile Area Network

14. _____ are referred to as service requestors.

A. Servers B. Clients C. Peer-to-Peer D. Client-Server

15. _____ are referred to as service providers.

A. Servers B. Clients C. Peer-to-Peer D. Client-Server

16. _____ refers to network of networks.

A. Intranet B. Internet C. LAN D. WAN

17. _____ refers to private networks used by organizations, not accessible by public.

A. Intranet B. Internet C. Peer-to-Peer D. Client-Server

18. In _____ data is sent as digital signals by using entire bandwidth of a media.

A. Broadband B. Baseband C. Digiband D. Analogband

19. In _____ data is sent as analog signals by using portion of a bandwidth.

A. Broadband B. Baseband C. Digiband D. Analogband

20. Examples of Broadband:

A. DSL B. Cable Internet C. Ethernet D. Both A & B

21. Example of Baseband:

A. Ethernet B. DSL C. Cable Internet D. Both B & C

22. Acronym - TDM.

A. Telecommunication Division Multiplier B. Time Division Multiplexing
C. Tele Division Multiplexing D. Transfer Division Multiplexing

23. Acronym - FDM.

A. Fast Division Multiplexing B. Fine Division Multiplier
C. Far Division Multiplexing D. Frequency Division Multiplexing

24. _____ refers to one-way communication.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

25. _____ refers to two-way communication but one direction at a time.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

26. _____ refers to simultaneous two-way communication.

A. Simplex B. Duplex C. Half-Duplex D. Full-Duplex

27. Acronym - CSMA/CD.

A. Collision Sense Multiple Access/Carrier Detect
B. Collision System Multiple Access/Carrier Detect
C. Carrier Sense Multiple Access/Collision Detect
D. Collision Sense Multiple Access/Carrier Divide

28. One-to-One communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

29. One-to-Many communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

30. One-to-All communication: _____.

A. Broadcast B. Multicast C. Unicast D. Basecast

31. Examples of Circuit switching networks:

A. PSTN B. ISDN C. GSM D. All of the above

32. Examples of Packet Switching Networks:

A. IP B. X.25 C. Frame relay D. All of the above

Quiz 02

1. Acronym - ISO.

A. Internal Standards Organization [✓ B. International Standards Organization]
C. Internet Standards Organization D. Intranet Standards Organization

2. Acronym - OSI.

A. Open Systems Internet B. Open Systems Intranet
C. Open Service Interconnect [✓ D. Open Systems Interconnection]

3. _____ is the first layer of the OSI Model.

A. Transport B. Network C. Data-link [✓ D. Physical]

4. _____ is the second layer of the OSI Model.

A. Presentation B. Session C. Transport [✓ D. Data-link]

5. _____ is the third layer of the OSI Model.

A. Presentation B. Session C. Transport [✓ D. Network]

6. _____ is the top-most layer of the OSI Model.

[✓ A. Application] B. Presentation C. Session D. Transport

7. Sub-layers of data-link layer are:

A. Session [✓ B. MAC] [✓ C. LLC] D. Application

8. _____ layer defines the electrical and physical specification.

A. Transport B. Data-link [✓ C. Physical] D. Both A & B

9. _____ layer handles physical addressing.

A. Physical [✓ B. Data-link] C. Application D. Presentation

10. _____ layer handles logical addressing and routing.

A. Presentation [✓ B. Network] C. Session D. Transport

11. _____ layer handles end-to-end communications between devices on a network.

A. Data-link B. Application C. Presentation [✓ D. Session]

12. _____ layer deals with standards for data formats; encryption & compression.

A. Physical B. Data-link [✓ C. Presentation] D. Application

13. Examples of layer 1 protocols:

A. DSL B. RS-232 C. 100BASE-TX [✓ D. All of the above]

14. Examples of layer 2 protocols:

A. Ethernet B. PPP C. Token Ring D. All of the above

15. Examples of layer 3 protocols:

A. IP B. IPX C. ICMP D. All of the above

16. Examples of layer 4 protocols:

A. TCP B. UDP C. SCTP D. All of the above

17. Examples of layer 5 protocols:

A. PAP B. PPTP C. L2TP D. All of the above

18. Examples of layer 6 protocols:

A. ASCII B. MIDI C. SSL D. All of the above

19. Examples of layer 7 protocols:

A. HTTP B. POP3 C. DSL D. All of the above

20. Unit of measurement at Layer 1.

A. bits B. frames C. packets D. segments

21. Unit of measurement at Layer 2.

A. bits B. frames C. packets D. segments

22. Unit of measurement at Layer 3.

A. bits B. frames C. packets D. segments

23. Unit of measurement at Layer 4.

A. bits B. frames C. packets D. segments

24. ___ model has 4 layers.

A. OSI Model B. TCP/IP Model C. MIME Model D. Presentation Model

Quiz 03

1. IEEE standard related to Ethernet _________________.

A. IEEE 802.11 B. IEEE 803.21 C. IEEE 802.3 D. IEEE 802.6

2. IEEE standard related to Bluetooth:

A. IEEE 802.3 B. IEEE 802.12 C. IEEE 802.14 D. IEEE 802.15

3. Which network topology allows computers to be connected to a centralized device?

A. Bus B. Star C. AD-HOC D. Mesh

4. Components used in Bus topology:

A. T-Connector B. BNC Connector C. Co-Axial Cable D. All of the above

5. Components used in Star topology:

A. RJ-45 B. Twisted-pair cable C. Switch D. All of the above

6. _____ is used for amplifying and re-transmitting weak signals.

A. Access Point B. Bridge C. Repeater D. All of the above

7. Advantage of a network switch over a hub:

A. Filters Frames B. Operates at Layer 2
C. Reduces Collision D. All of the above

8. In 10base2 '10' refers to:

A. 10 Meters B. 10 Mbps C. 10 Mbps D. Both B & C

9. In 10base2 'base' refers to:

A. Broadband B. Baseband C. Narrowband D. Wideband

10. In 10base2 '2' refers to:

A. 200 Meters B. 200 Mbps C. 2 Mbps D. 200 Feet

11. 10Base2 is also known as:

A. Broadband B. Thinnet C. Thicknet D. Baseband

12. 10Base5 is also known as:

A. Broadband B. Thinnet C. Thicknet D. Baseband

13. Acronym - UTP.

A. Ultimate Twisted Pair B. Unwinded Twisted Pair
C. Unshielded Twisted Pair D. Unlimited Twisted Pair

14. Speed of Ethernet:

A. 10 Mbps B. 100 Mbps C. 1000 Mbps D. 10000 Mbps

15. Speed of Fast Ethernet:

A. 10 Mbps B. 100 Mbps C. 1000 Mbps D. 10000 Mbps

16. In 100baseT 'T' refers to:

A. Twisted-Pair B. Telecommunication C. Thin-Pair D. Tele-Pair

17. Category of UTP that support speeds greater than 100 Mbps:

A. Cat 1 B. Cat 2 C. Cat 3 D. Cat 5

18. Category of UTP that support speeds greater than 1000 Mbps:

A. Cat 3 B. Cat 5e C. Cat 6 D. Both B & C

19. Category of UTP used in Telephone lines:

A. Cat 1 B. Cat 2 C. Cat 3 D. Cat T

20. Maximum distance supported by UTP _____.

A. 100 Feet B. 1000 Feet C. 100 Meters D. 10 Meters

21. IEEE 802.3 Specification corresponds to _____ standard.

A. 10BASE2 B. 100BASE-TX C. 1000BASE-T D. 1000BASESX

22. Type of cable that uses light as the media for transmitting signals:

A. Co-Axial B. UTP C. STP D. Fiber-optic

23. Type of cable that is not susceptible to EMI:

A. Co-Axial B. UTP C. STP D. Fiber-optic

24. Type of material used for protecting cables against fire:

A. PVC B. Plenum C. STP D. UTP

25. Type of cable preferred for connecting dissimilar devices:

A. Single-mode fiber B. Straight through
C. Cross over D. PVC Coated

26. Type of cable preferred for connecting similar devices:

A. Single-mode fiber B. Straight through C. Cross over D. PVC Coated

27. Type of NIC for use in desktop computers.

A. PCI B. PCIe C. USB D. All of the above

28. Type of NIC for use in laptop computers.

A. PCI B. CardBus C. ExpressCard D. ISA

29. _____ is a unique hardware address assigned to an NIC.

A. MAC B. IP C. IPX D. TCP

30. MAC addresses are _____ addresses.

A. 16-bit B. 32-bit C. 48-bit D. 64-bit

31. Example of a valid MAC address:

A. 00-B0-D0-1D-F5-5B B. 192.168.2.5
C. 00-B0-D000-B0-D000-B0-D000-B0-D0 D. server05

32. Connectors for Ethernet card _____.

A. RJ-11 B. RJ-58 C. RJ-45 D. RJ-E

33. Connectors for telephones _____.

A. RJ-11 B. RJ-58 C. RJ-45 D. RJ-E

34. _____ is a special chip that allows loading of an operating system over a network.

A. WOL B. Boot ROM C. MAC ROM D. RIS

35. Procedure through which devices choose common transmission parameters such as speed; duplex mode and flow control:

A. Auto-negotiation B. Auto-duplex C. Auto-connection D. Auto-speed

36. Layer 1 device _____.

A. Hub B. Bridge C. Switch D. Router

37. Layer 2 devices _____.

A. Hub B. Bridge C. Switch D. Router

38. Layer 3 devices _____.

A. Hub B. Bridge C. Switch D. Router

39. _____ is a multi-port repeater.

A. Hub B. Bridge C. Switch D. Router

40. _____ is a multi-port bridge.

A. Hub B. Switch C. Router D. Access Point

41. MAC Addresses are also known as _____.

A. Logical Address B. Routing Address C. Network Address [✓ D. Physical Address]

42. Type of switch that do not require administrative configuration:

A. Managed [✓ B. Unmanaged] C. Typical D. Custom

43. Acronym - VLAN.

A. Visual LAN [✓ B. Virtual LAN] C. Vertical LAN D. Viral LAN

44. Device that helps reduce broadcast domains:

A. Hub [✓ B. Switch] C. Router D. Access Point

45. _____ reduces collisions and improves security.

A. WLAN B. Wi-Fi [✓ C. VLAN] D. CSMA/CD

46. System that supplies electricity through Ethernet cables:

A. VLAN [✓ B. PoE] C. WOL D. CSMA/CA

47. Methods used in switching:

A. Store and forward B. Cut through C. Fragment free [✓ D. All of the above]

48. Device used for creating patch cables:

A. Patch Tool [✓ B. Crimping Tool] C. Cable Tester D. Loopback Adapter

49. 2-pair Straight-through pin / cable configuration:

A. 1-2; 2-1; 3-6; 6-3
B. 1-3; 3-1; 2-6; 6-2
[✓ C. 1-1; 2-2; 3-3; 6-6]
D. 1-6; 6-1; 2-3; 3-2

50. 2-pair Cross-over pin / cable configuration:

[✓ A. 1-2; 2-1; 3-6; 6-3]
B. 1-3; 3-1; 2-6; 6-2
C. 1-1; 2-2; 3-3; 6-6
D. 1-6; 6-1; 2-3; 3-2

51. Command-line utility for viewing MAC address:

A. IPCONFIG [✓ B. GETMAC] C. VIEWMAC D. HOSTNAME

52. MAC addresses are usually displayed in _____ format.

A. ASCII [✓ B. Hexadecimal] C. Numeric D. Encrypted

53. Utility for viewing or modifying settings of network interface cards:

A. GETMAC B. Device Manager C. Disk Manager D. Network Manager

54. Correct syntax for viewing MAC address with manufacturer / model details:

A. GETMAC B. GETMAC /v C. IPCONFIG /m D. IPCONFIG /L

55. _____ resolves IP addresses to MAC addresses.

A. ARP B. DHCP C. DNS D. WINS

56. Command to view ARP Cache

A. GETMAC B. IPCONFIG C. ARP D. PING

57. _____ is used for network management & monitoring.

A.SMTP B.SNMP C.POP3 D.FTP

58. Type of Connectors used for Fiber-Optic NIC.

A. RJ-11 B. RJ-45 C. MT-RJ D. BNC

59. Acronym - NEXT (Context: Signaling):

A. Null End Crosstalk B. Null Ethernet Crosstalk
C. Near End Crosstalk D. All of the above

60. Acronym - FEXT (Context: Signaling):

A. Field End Crosstalk B. Far End Crosstalk
C. Federation End Cross Talk D. Far Ethernet Crosstalk

Quiz 04

1. IEEE standards for WLAN (Wi-Fi):

[✓ A. 802.11 b/g] [✓ B. 802.11 a] [✓ C. 802.11 n] [✓ D. 802.11 ac]

2. Radio Frequency - IEEE 802.11 a:

A. 2.4 GHz B. 2.8 GHz [✓ C. 5 GHz] D. None

3. Radio Frequency - IEEE 802.11 b/g:

[✓ A. 2.4 GHz] B. 2.8 GHz C. 5 GHz D. Both A & C

4. Radio Frequency - IEEE 802.11 ac:

A. 2.4 GHz B. 2.8 GHz [✓ C. 5 GHz] D. All of the above

5. Radio Frequency - IEEE 802.11 n:

A. 2.4 GHz B. 2.8 GHz C. 5 GHz [✓ D. Both A & C]

6. Maximum speed supported by IEEE 802.11b:

[✓ A. 11 Mbps] B. 54 Mbps C. 600 Mbps D. 1 Gbps

7. Maximum speed supported by IEEE 802.11a:

A. 11 Mbps [✓ B. 54 Mbps] C. 600 Mbps D. 1 Gbps

8. Maximum speed supported by IEEE 802.11g:

A. 11 Mbps [✓ B. 54 Mbps] C. 600 Mbps D. 1 Gbps

9. Maximum speed supported by IEEE 802.11n:

A. 11 Mbps B. 54 Mbps [✓ C. 600 Mbps] D. 1 Gbps

10. Maximum speed supported by IEEE 802.11ac:

A. 11 Mbps B. 54 Mbps C. 600 Mbps [✓ D. 6.77 Gbps]

11. WLAN utilizes _____ technologies for transmissions:

[✓ A. OFDM] B. IR C. Bluetooth D. None

12. Tethering is also referred to as:

[✓ A. Mobile Hotspot] B. Wireless Fidelity C. NFC D. None

13. Device required for setting up a Wi-Fi Network:

A. Repeater [✓ B. Access Point] C. Hub D. Router

14. Peer-to-Peer wireless networks are referred to as:

A. Infrastructure Networks B. ADHOC Networks
C. Peer Level Networks D. All of the above

15. Infrastructure wireless networks require:

A. Repeater B. Access Point C. Hub D. Router

16. Device that acts as a bridge between wired and wireless networks:

A. Repeater B. Access Point C. Hub D. Router

17. Acronym - SSID:

A. Secure Set Identifier B. Simple Set Identifier
C. Synchronous Set Identifier D. Service Set Identifier

18. SSID - Maximum number of characters:

A. 8 B. 16 C. 32 D. 64

19. In wireless networks a device may be associated with _____ SSIDs:

A. 4 B. 1 C. 12 D. Unlimited

20. Dual band devices typically

A. Allow use of both 2.4 GHz and 5 GHz B. Supports longer range
C. Supports more than 1 SSID D. None of the above

21. Acronym - WAP:

A. Wired Access Point B. Wireless Access Point
C. Wireless Area Point D. Wired Area Point

22. _____ refers to unauthorized access of wireless networks.

A. Postpaid B. Secure Connect C. Piggybacking D. None

23. Ways to protect wireless networks:

A. Disable SSID Broadcast B. Implement WPA C. Change default SSID D. All of the above

24. Acronym - WEP

A. Wireless Equivalent Privacy B. Wired Equivalent Privacy
C. Wi-Fi Equivalent Privacy D. Wireless Encrypted Privacy

25. Acronym - WPA

A. Wireless Protected Access B. Wired Protected Access
C. Wi-Fi Protected Access D. Wi-Fi Protected Array

26. Acronym - TKIP

A. Temporal Key Integrity Practice B. Temporary Key Integrity Protocol
C. Temporal Key Intelligent Protocol D. Temporal Key Integrity Protocol

27. Items that cause interference to wireless signals:

A. Steel B. Concrete C. Wood D. All of the above

28. 64 bit WEP uses _____ hexadecimal characters.

A. 8 B. 12 C. 26 D. 10

29. 128 bit WEP uses _____ hexadecimal characters.

A. 8 B. 12 C. 26 D. 10

30. Most recent wireless encryption standard:

A. 128 bit WEP B. 64 bit WEP C. WPA D. WPA2

31. _____ utilizes per-packet key.

A. PoE B. WEP C. WPA D. NoN

32. Acronym - WPS

A. Wireless Protected Setup B. Wi-Fi Protected Setup
C. Wired Protected Setup D. Wired Protected Sync

33. Devices that cause interference to wireless signals:

A. Cordless Phones B. Microwave Ovens C. Baby Monitors D. All of the above

34. Acronym - AES

A. Analytical Encryption Standard B. Alternate Encryption Standard
C. Adverse Encryption Standard D. Advanced Encryption Standard

35. Acronym - MIMO.

A. Multiple-Input; Multiple-Out B. Minute-Input; Minute-Out
C. Micro-Input; Micro-Out D. Macro-Input; Macro-Out

36. MIMO technique is used in:

A. IEEE 802.11g B. IEEE 802.11b C. IEEE 802.11n D. Both A & B

37. Technique that allows connections only if a WAP finds matching address:

A. WEP B. WPA C. MAC Authentication D. IP Spoofing

38. The term 'IBSS' refers to:

A. Switched Networks B. Infrastructure Networks
C. ADHOC Networks D. Managed Networks

39. The term 'BSS' refers to:

A. Switched Networks B. Infrastructure Networks
C. ADHOC Networks D. Managed Networks

40. Acronym - ESS.

A. Emulated Service Set B. Extended Service Setup
C. Extended Service Set D. Emulated Service Setup

41. Acronym - IBSS.

A. Internet BSS B. Intranet BSS C. Inline BSS D. Independent BSS

42. Network access method used in wireless networks:

A. CSMA/CD B. CSMA/CA C. CSMA/Wi-Fi D. CSMA/CF

43. Acronym - CSMA/CA

A. Carrier Sense Multiple Access/Collision Avoidance
B. Career Sense Multiple Access/Collision Avoidance
C. Carrier Sense Multiple Access/Collision Access
D. Career Sense Multiple Access/Collision Access

44. Acronym - QAM

A. Quad Processor Modulation B. Quadrature Amplitude Modulation
C. Quad Amplifier D. None of the above

45. Technology that allows to form a network using electricity Lines:

A. Powerline B. DSL C. Cable D. ISDN

46. Standards related to Powerline

A. IEEE 1801 B. HomePlug AV C. IEEE 1901 D. IEEE 802.11

47. Standard related to FireWire

A. IEEE 1901 B. IEEE 802.11 C. IEEE 1284 D. IEEE 1394

48. Speeds supported by FireWire

A. 400 Mbps B. 800 Mbps C. 1600 Mbps D. 400 Gbps

Quiz 05

1. 'Set of rules for communication' refers to ______.

A. Protocol B. Service C. Interface D. Network Device

2. Protocols at Layer 3 ______.

A. IP B. ICMP C. IGMP D. DSL

3. ______ layer of the OSI model refers to logical addressing and routing.

A. Physical B. Data-link C. Network D. Session

4. Examples of Proprietary protocols:

A. NetBEUI B. IPX/SPX C. AppleTalk D. All of the above

5. Examples of Open standard protocol:

A. NetBEUI B. IPX/SPX C. AppleTalk D. TCP/IP

6. Acronym - NetBEUI.

A. NetBIOS Extended User Interface
B. Network Extended User Interface
C. NetBIOS Expanded User Interface
D. Network Expanded User Interface

7. Acronym - IPX/SPX.

A. Internetwork Packet Exchange/Sequenced Packet Exchange
B. Intranetwork Packet Exchange/Sequenced Packet Exchange
C. Internetwork Protocol Exchange/Sequenced Protocol Exchange
D. Intranetwork Protocol Exchange/Sequenced Protocol Exchange

8. Acronym - TCP/IP.

A. Transmission Connection Protocol / Internet Protocol
B. Transmission Control Packet / Internet Packet
C. Transmission Control Protocol / Internet Protocol
D. Transmission Control Protocol / Internet Packet

9. Advantages of TCP/IP.

A. Open Standard B. Multiple Network framework
C. Routable D. All of the above

10. Proprietary protocol used in early Microsoft Windows networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

11. Proprietary protocol used in Apple computer networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

12. Proprietary protocol used on Novell NetWare networks:

A. NetBEUI B. IPX C. IPv4 D. AppleTalk

13. IPv4 uses ______ bit addressing scheme.

A. 4 B. 8 C. 32 D. 64

14. IPv6 uses ______ bit addressing scheme.

A. 8 B. 32 C. 64 D. 128

15. ______ is the entity that oversees global IP address allocation.

A. IEEE B. IETF C. IANA D. ISO

16. Acronym - IANA.

A. Internet Assigned Numeric Authority B. Intranet Assigned Numbers Authority
C. Internet Automated Numbers Authority D. Internet Assigned Numbers Authority

17. Maximum number of IP addresses in IPv4

A. 65536 B. 4294967296 C. 256 D. 16

18. Maximum number of IP addresses in IPv6:

A. 4294967296
B. 340282366920938463463374607431768211456
C. 42949672964294967296
D. 34028236692093846346

19. Class reserved for multicasting:

A. Class A B. Class B C. Class C D. Class D

20. IP address range for Class A:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

21. IP address range for Class B:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

22. IP address range for Class C:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

23. IP address range for Class D:

A. 0.0.0.0 - 127.255.255.255
B. 128.0.0.0 - 191.255.255.255
C. 192.0.0.0 - 223.255.255.255
D. 224.0.0.0 - 239.255.255.255

24. IP address range for Class E:

A. 128.0.0.0 - 191.255.255.255
B. 192.0.0.0 - 223.255.255.255
C. 224.0.0.0 - 239.255.255.255
D. 240.0.0.0 - 255.255.255.255

25. _____ addresses are used for communicating between computers on the Internet.

A. Multicast B. Private C. Public D. Broadcast

26. _____ addresses are used for communicating between computers on a LAN.

A. Multicast B. Private C. Public D. Broadcast

27. IP addresses reserved for private networks:

A. 10.0.0.0 - 10.255.255.255
B. 172.16.0.0 - 172.31.255.255
C. 192.168.0.0 - 192.168.255.255
D. All of the above

28. _____ is used for identifying the network and host ID portions of an IP address.

A. Gateway B. Subnet Mask C. DNS Address D. WINS Address

29. Range reserved for loopback addresses:

A. 10.0.0.0 – 10.255.255.255 B. 172.16.0.0 - 172.31.255.2
C. 127.0.0.1 – 127.255.255.255 D. 240.0.0.0 - 255.255.255.255

30. Default subnet mask for Class A range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

31. Default subnet mask for Class B range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

32. Default subnet mask for Class C range of IP addresses:

A. 255.0.0.0 B. 255.255.0.0 C. 255.255.255.0 D. 255.255.255.255

33. 169. 255.255.255.255 address represents:

A. A Unicast address B. A Multicast address
C. A Broadcast address D. A Gateway address

34. Example of an IPv6 address:

A. 123.123.123.123
B. 2001:0db8:85a3:0042:1000:8a2e:0370:7334
C. A0:10:20:10:12:14
D. V6:123.123.123.133

35. Protocol used for automating IP configuration:

A. ARP B. DHCP C. DNS D. WINS

36. ______ are protocols that do not resolve names to IP addresses.

A. DDNS B. DNS C. WINS D. None

37. ______ indicates network messages or timeouts at layer 3.

A. ARP B. ICMP C. IGMP D. BOOTP

38. DHCP Sequence:

A. Offer; Discover; Request; Acknowledge
B. Discover; Request; Acknowledge; Offer
C. Discover; Offer; Request; Acknowledge
D. Request; Offer; Discover; Acknowledge

39. Purpose of APIPA:

A. Assigns IP address to each computer from a SOHO Router
B. Self-assigns each computer a private IP address
C. Assigns DNS addresses on a DHCP enabled network
D. Routes packets from one logical network to another

40. Acronym - APIPA.

A. Automatic Public IP Addressing B. Activated Private IP Addressing
C. Activated Public IP Addressing D. Automatic Private IP Addressing

41. Range reserved for APIPA:

A. 10.0.0.0 - 10.255.255.255
B. 192.168.0.0. - 192.168.255.255
C. 169.254.1.0 - 169.254.254.255
D. 172.16.0.0 - 172.16.255.255

42. Command utility for viewing IP address:

A. GETMAC B. IPCONFIG C. TELNET D. IPMAC

43. Utility & Syntax for viewing complete IP configuration:

A. IPMAC /Complete
B. IPMAC /ALL
C. IPCONFIG /Complete
D. IPCONFIG /ALL

44. Command line utility for checking network connectivity:

A. NETSTAT B. IPCONFIG C. PING D. NBTSTAT

45. PING uses _____ protocol.

A. IP B. ICMP C. IGMP D. HTTP

46. Syntax for unlimited packets:

A. PING address -n B. PING address -t C. PING address -l D. PING address -p

47. Command line utility for managing ARP cache table:

A. IP2MAC B. ARP C. PING D. All of the above

48. Syntax for testing local machine's IP:

A. Ping 127.0.0.1 B. Ping localhost C. Ping 127.1.2.3 D. All of the above

49. Syntax for releasing IP address:

A. IPCONFIG /RELEASE B. IPCONFIG /RENEW
C. IPCONFIG /ALL D. IPCONFIG /REFRESH

50. Syntax for renewing IP address:

A. IPCONFIG /RELEASE B. IPCONFIG /RENEW
C. IPCONFIG /ALL D. IPCONFIG /REFRESH

51. Acronym - CIDR.

A. Classful Inter Domain Routing B. Classful Intra Domain Routing
C. Classless Inter Domain Routing D. Classless Intra Domain Routing

52. Purpose of CIDR:

A. Manipulates MAC address B. Manipulates DNS address
C. Replaces IPv4 with IPv6 D. Allows variable Network and host addresses

53. In _____ routing packets are transmitted through fixed routes.

A. Dynamic B. Static C. Variable D. Fixed

54. In _____ routing routing of packets are determined by routers.

A. Dynamic B. Static C. Variable D. Fixed

55. Command line utility for viewing route and to measure transit delays of a packet:

A. TRACERT B. PATHPING C. ROUTE D. IPCONFIG

56. Command line utility for viewing and manipulating routing tables:

A. TRACERT B. PATHPING C. ROUTE D. IPCONFIG

57. Command line utility that combines the power of both PING and TRACERT:

A. TRACEPING B. TRACEPATH C. PINGPATH D. PATHPING

58. Syntax for viewing routing table:

A. Route Print B. Router Print C. Routing Print D. Routable Print

59. Examples of routable protocols:

A. IPX/SPX B. TCP/IP C. OSPF D. RIP

60. Examples of routing protocols:

A. OSPF B. RIP C. IS-IS D. All of the above

Quiz 06

1. Features of UDP.

A. Connection-less & Unreliable B. No sequencing
C. No acknowledgment or re-transmission D. All of the above

2. Features of TCP.

A. Reliable & Connection-oriented B. Sequencing
C. Flow Control and re-transmission D. All of the above

3. Number of ports per IP address:

A. 16000 B. 65530 C. 65536 D. Unlimited

4. Well-known port numbers range:

A. 0-1024 B. 0-1023 C. 1024-49151 D. 12001-65535

5. Registered port numbers range:

A. 0-1024 B. 0-1023 C. 1024-49151 D. 12001-65535

6. Default port number for HTTP:

A. 8080 B. 80 C. 12000 D. 21

7. Default port number for FTP:

A. 8080 B. 80 C. 12000 D. 21

8. Default port number for POP3:

A. 20 B. 53 C. 110 D. 25

9. Default port number for SMTP:

A. 20 B. 53 C. 110 D. 25

10. Default port number for DNS:

A. 20 B. 53 C. 110 D. 25

11. Default port number for TELNET:

A. 23 B. 55 C. 443 D. 25

12. Default port number for HTTPS:

A. 23 B. 55 C. 443 D. 25

13. Command line utility for viewing network statistics:

A. ICMP B. NETSTAT C. NETVIEW D. NET

14. Methods for name resolution:

A. HOSTS file B. LMHOSTS file C. DNS D. All of the above

15. Centralized name resolution methods:

A. DNS B. WINS C. DDNS D. All of the above

16. _____ naming resolution is used on networks utilizing dynamic IP addresses.

A. DNS B. WINS C. DDNS D. HOSTS

17. Location of HOSTS file in Microsoft Windows:

A. C:\Windows\System\Drivers\etc
B. C:\Windows\System32\Drivers\etc
C. C:\Windows\System32\HOSTNAMES\
D. C:\Windows\etc

18. DNS utilizes a _____ naming system.

A. Symmetrical B. Hierarchical C. Asymmetrical D. Variable

19. Domain names are managed by:

A. IETF B. IEEE C. ICANN D. ISO

20. Acronym - ICANN.

A. Internet Corporation for Automated Names and Numbers
B. Intranet Corporation for Automated Names and Numbers
C. Internet Corporation for Assigned Names and Numbers
D. Intranet Corporation for Assigned Names and Numbers

21. Command line utility for querying DNS servers:

A. PING B. TRACERT C. NSLOOKUP D. NAMEDNS

22. Syntax for viewing DNS resolver cache:

A. NSLOOKUP /DNS B. IPCONFIG /DISPLAYDNS
C. IPCONFIG /FLUSHDNS D. NSLOOKUP /CACHE

24. Syntax for clearing DNS Cache:

A. NSLOOKUP /DNS B. IPCONFIG /DISPLAYDNS
C. IPCONFIG /FLUSHDNS D. NSLOOKUP /CACHE

24. ___ is used for secured transmissions.

A. SSL B. TLS C. DNS D. All of the above.

Quiz 07

1. Which of the following WAN technology is the slowest?

A. ISDN B. Dial-Up C. DSL D. Cable

2. Which of the following connectivity utilizes a 56K modem?

A. ISDN B. PSTN C. DSL D. Both B & C

3. Protocols used in dial-up networking:

A. PPP B. SLIP C. PPPoE D. PPPoA

4. Advantages of PPP over SLIP.

A. Support for Dynamic IP address B. Support for protocols other than TCP/IP
C. Support for services such as Windows Firewall D. Support for Layer 1

5. Acronym - ISDN.

A. Internet Services for Digital Network B. Intranet Services for Digital Network
C. Integrated Services for Digital Network D. Integrated Services for DSL Network

6. Acronym - DSLAM.

A. Direct subscriber line access multiplexer B. Direct subscriber line access multiplier
C. Digital subscriber line access multiplexer D. Digital subscriber line access multiplier

7. Device used for splitting voice and data at a customer's premises in a DSL connection:

A. SOHO Router B. Wi-Fi Router C. DSL Modem D. DSL Splitter

8. DSL uses _____ protocols.

A. PPP B. SLIP C. PPPoE D. Ethernet

9. Acronym - PPPoE.

A. Packet-to-Packet Protocol Over Ethernet B. Point-to-Point Packet Over Ethernet
C. Point-to-Point Protocol Over Ethernet D. Point-to-Packet Protocol Over Ethernet

10. Acronym - PPPoA.

A. Packet-to-Packet Protocol Over ATA B. Point-to-Point Packet Over ATM
C. Point-to-Point Protocol Over ATM D. Point-to-Packet Protocol Over ATA

11. _____ refers to private network over the Internet.

A. WLAN B. DSL C. WiMAX D. VPN

12. Acronym - VPN.

A. Virtual Public Network B. Virtual Private Network
C. Vertical Private Network D. Vertical Public Network

13. Protocols used in VPN:

A. PPP B. PPTP C. L2TP D. SLIP

14. Acronym - PPTP.

A. Private to Public Tunneling Protocol B. Point to Point Teredo Protocol
C. Point to Point Tunneling Protocol D. Private to Public Tunneling Protocol

15. Acronym - L2TP.

A. Level 2 Teredo Protocol B. Level 2 Tunneling Protocol
C. Layer 2 Teredo Protocol D. Layer 2 Tunneling Protocol

16. Encryption used in L2TP:

A. AED B. IP C. IPSec D. 3DES

17. _____ controls incoming & outgoing traffic.

A. DSL B. Anti-Virus Software C. Firewall D. WAP

18. Acronym - NAT.

A. Network Application Translation B. Network Address Translation
C. Nano Address Translation D. Network Application Technology

Summary

Hope this guide was helpful in understanding the basics of networking. Although it does not cover topics in-depth, we encourage readers to explore authentic websites and tutorials for further learning and a deeper understanding.

Credits (Our Sincere Thanks!)

We sincerely thank the creators of the following images and icons used in this material:

https://github.com/KDE/oxygen-icons
https://www.freepik.com/free-vector/profession-icons-collection_1043177.htm
https://www.freepik.com/free-vector/switches-sockets-realistic-set_4186281.htm
https://www.freepik.com/free-icon/wifi_858765.htm
https://www.vecteezy.com/vector-art/159146-free-ports-icons-vector
https://www.flaticon.com/free-icon/bluetooth_636191
https://www.freepik.com/free-vector/old-black-phone_1012648.htm
https://www.freepik.com/free-vector/vintage-tv_763025.htm
https://www.freepik.com/free-vector/twisted-cable-white_6690733.htm
https://www.freepik.com/free-vector/electric-shielded-cable-with-cooper-wires-set_6690797.htm
https://www.freepik.com/free-vector/high-speed-mobile-internet-realistic-set-with-satellites-smartphone-with-title-5g-isolated_7286408.htm
https://www.freepik.com/free-vector/mail-illustration_5254240.htm
https://www.freepik.com/free-vector/network-security-color-icons_3813300.htm
https://www.freepik.com/free-vector/blue-globe_795339.htm
https://www.flaticon.com/free-icon/folder_891094
https://www.freepik.com/free-vector/collection-machines-used-offices-isolated_2631307.htm
https://www.freepik.com/free-vector/modern-cctv-camera-with-realistic-design_2994123.htm