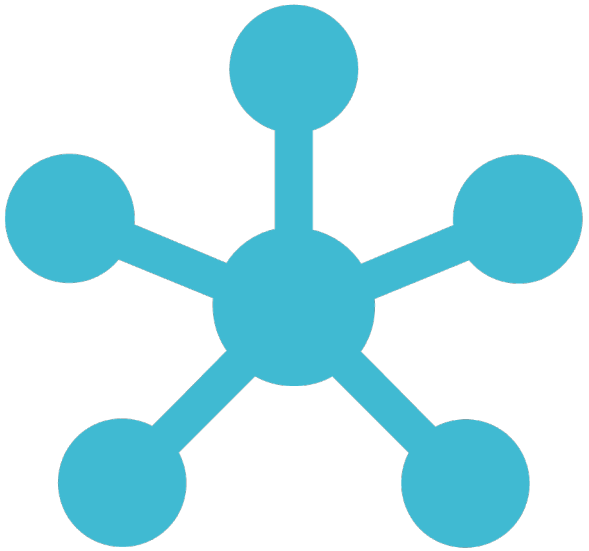
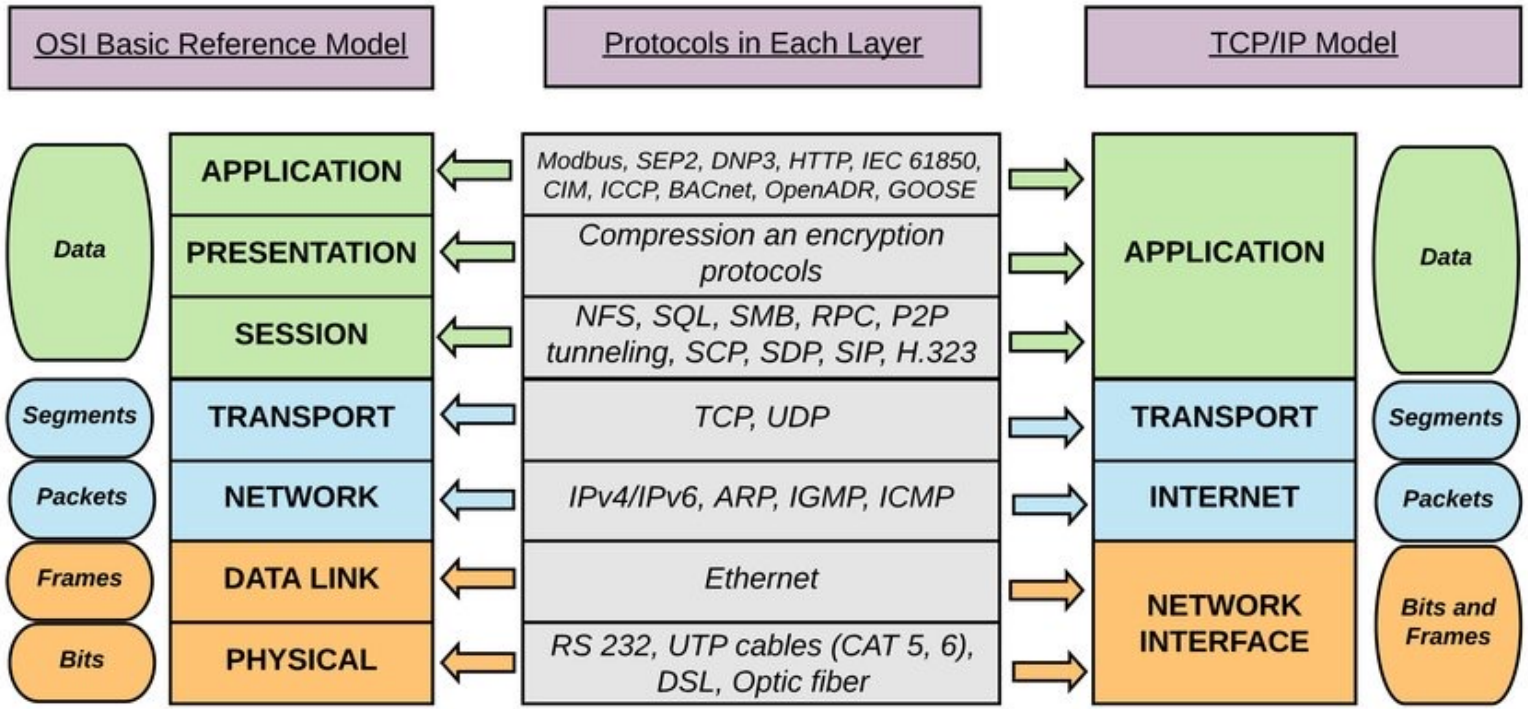


Network Design

10/05/2023


OSI Basic Reference Model
Protocols in Each Layer
TCP/IP Model
Data
APPLICATION
Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE
PRESENTATION
Compression an encryption protocols
SESSION
NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323
APPLICATION
Data
Segments
TRANSPORT
TCP, UDP
TRANSPORT
Segments
Packets
NETWORK
IPv4/IPv6, ARP, IGMP, ICMP
INTERNET
Packets
Frames
DATA LINK
Ethernet
NETWORK INTERFACE
Bits and Frames
Bits
PHYSICAL
RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber

OSI vs TCP/IP

Firewall

Firewalls are designed to protect a network or device from unauthorized access, cyber threats, and malicious activities.

Key Functions

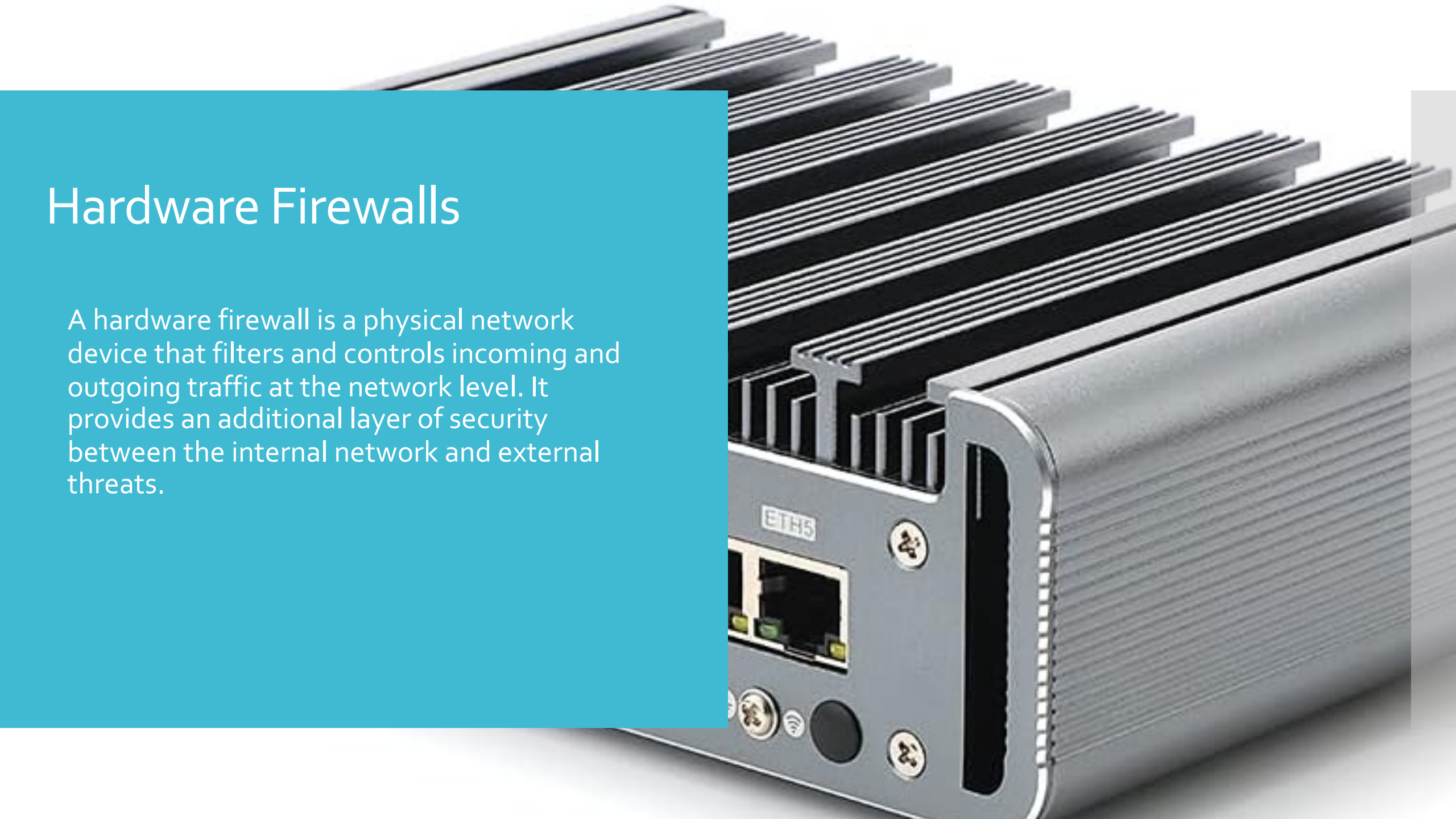
Packet Filtering" (Icon of data packets)	"Stateful or stateless Inspection" (Icon of a firewall analyzing traffic)	"Access Control" (Icon of a gatekeeper)	"Intrusion Detection and Prevention" (Icon of a shield)	"Proxy Services" (Icon of a proxy server)	"Logging and Monitoring" (Icon of logs)

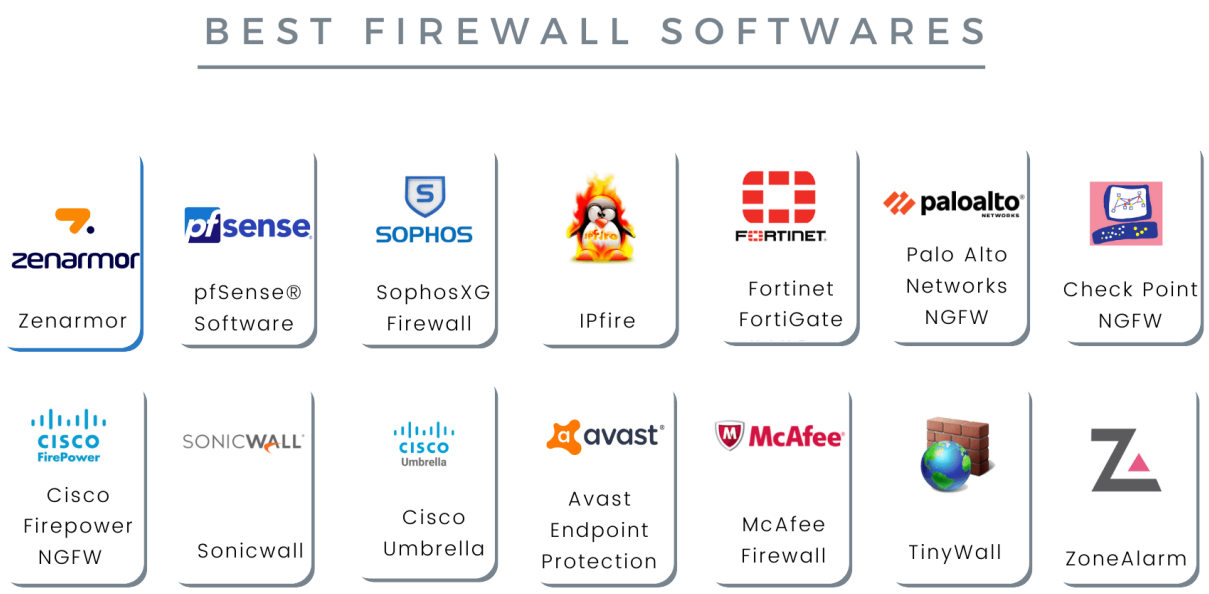
Types of firewall

Hardware Firewalls	Software Firewalls	Next-Generation Firewalls	Cloud-based Firewalls

Hardware Firewalls

A hardware firewall is a physical network device that filters and controls incoming and outgoing traffic at the network level. It provides an additional layer of security between the internal network and external threats.





Software Firewalls

A software firewall is a program or application that runs on a computer or device. It monitors and filters network traffic on that specific device, making it suitable for personal computer protection.

Next-Generation Firewalls

A next-generation firewall combines traditional firewall features with advanced security capabilities. It can analyze application-layer data, perform intrusion detection, and provide more granular control over network traffic."

Router

A router is a networking device that connects different networks together and directs data traffic between them.

Key Functions:

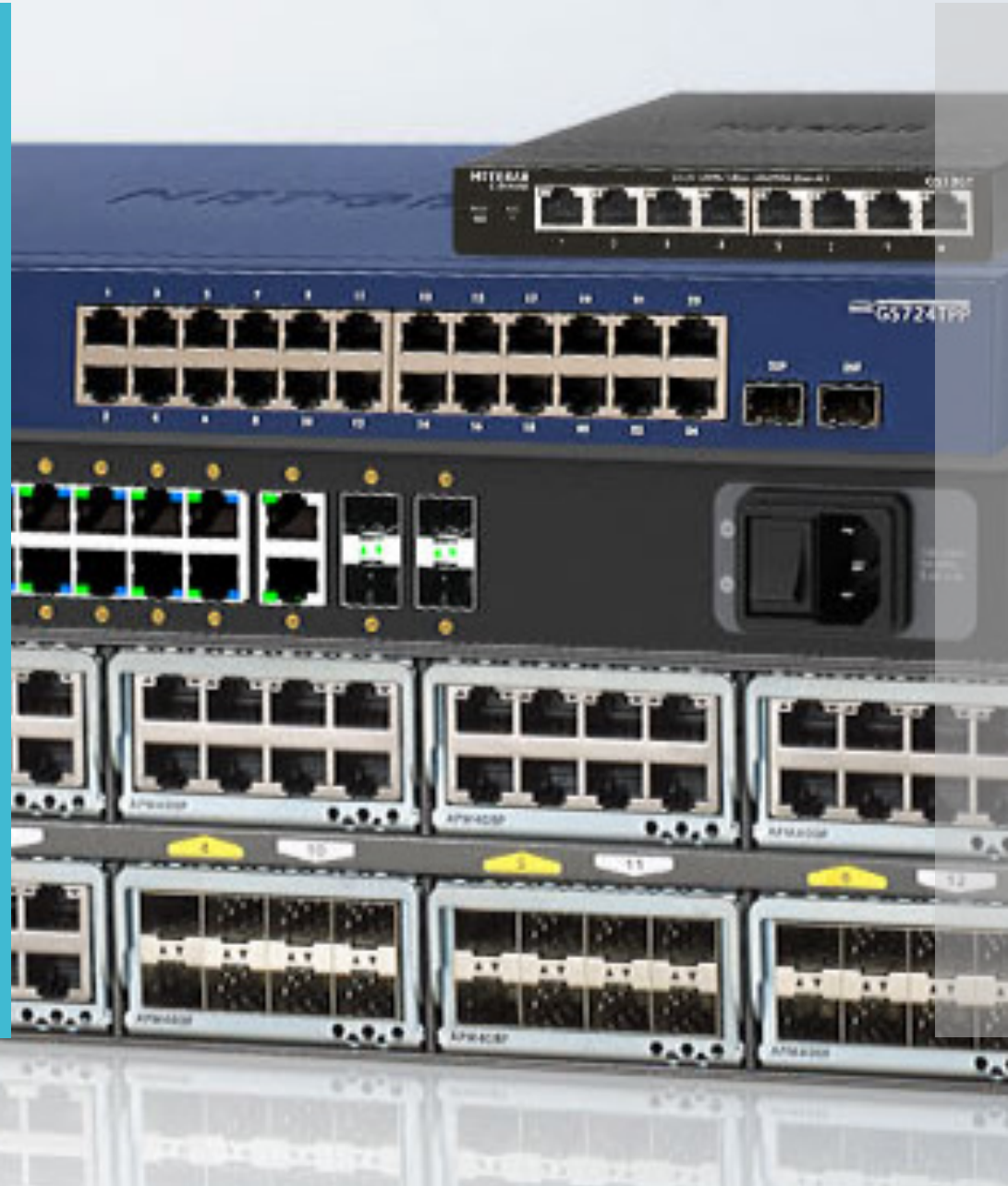
- Network Traffic Routing"
- "Internet Connection Sharing"
- "Firewall and Security"
- "DHCP (Dynamic Host Configuration Protocol)"
- "NAT (Network Address Translation)"

Switch

A switch is a network device that connects multiple devices within a local area network (LAN) and uses MAC addresses to forward data packets to the appropriate destination.

Key Functions

- "Packet Forwarding" (Icon of data packets moving)
- "Broadcast Domain Segmentation" (Icon of segmented LAN)
- "MAC Address Learning" (Icon of a switch learning addresses)
- "Collision Domain Isolation" (Icon of isolated collision domains)

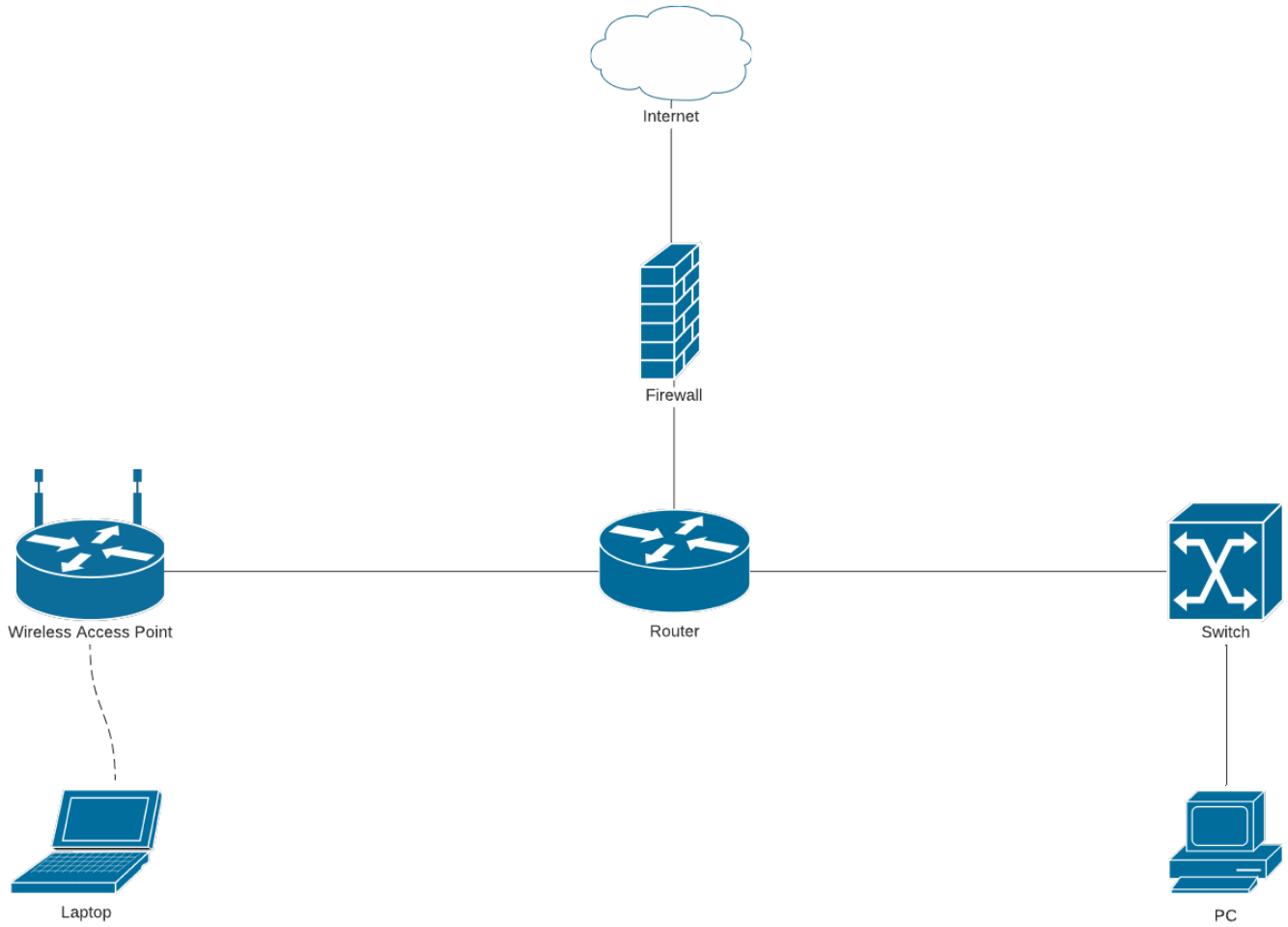


Managed VS Unmanaged

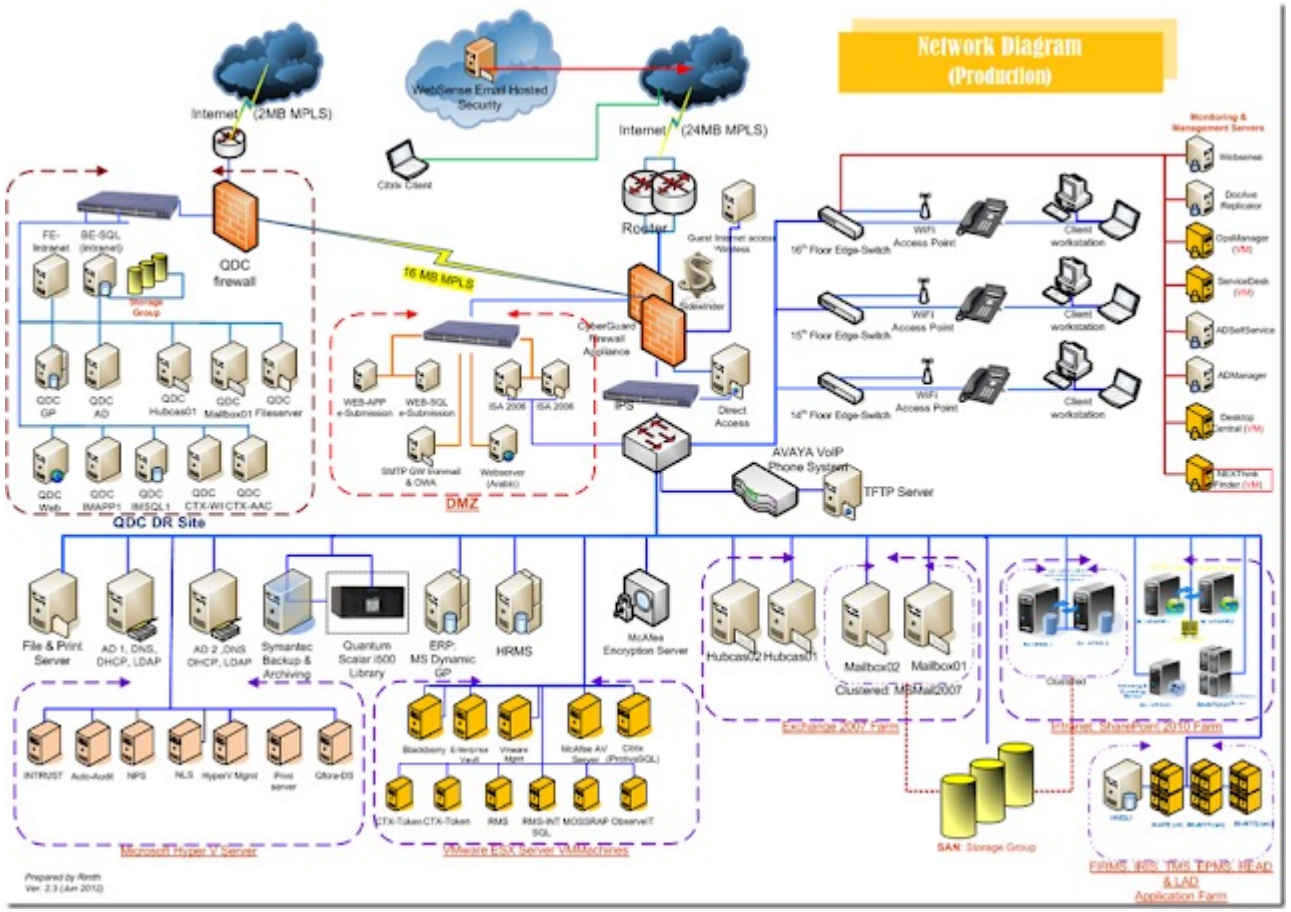
Managed switches offer advanced features and remote management capabilities. Network administrators can configure settings, monitor traffic, and optimize network performance.

Unmanaged switches are plug-and-play devices with no configuration options. They are suitable for basic network setups where simplicity is a priority.

All Together



All Together



IP Addresses

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

- An IP address, short for Internet Protocol address, is a unique numeric identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication.

Subnet Masks

Subnet Mask	CIDR	Binary Notation	Available Addresses Per Subnet
255.255.255.255	/32	11111111.11111111.11111111.11111111	1
255.255.255.254	/31	11111111.11111111.11111111.11111110	2
255.255.255.252	/30	11111111.11111111.11111111.11111100	4
255.255.255.248	/29	11111111.11111111.11111111.11111000	8
255.255.255.240	/28	11111111.11111111.11111111.11110000	16
255.255.255.224	/27	11111111.11111111.11111111.11100000	32
255.255.255.192	/26	11111111.11111111.11111111.11000000	64
255.255.255.128	/25	11111111.11111111.11111111.10000000	128
255.255.255.0	/24	11111111.11111111.11111111.00000000	256
255.255.254.0	/23	11111111.11111111.11111110.00000000	512
255.255.252.0	/22	11111111.11111111.11111100.00000000	1024
255.255.248.0	/21	11111111.11111111.11111000.00000000	2048
255.255.240.0	/20	11111111.11111111.11110000.00000000	4096
255.255.224.0	/19	11111111.11111111.11100000.00000000	8192
255.255.192.0	/18	11111111.11111111.11000000.00000000	16384
255.255.128.0	/17	11111111.11111111.10000000.00000000	32768
255.255.0.0	/16	11111111.11111111.00000000.00000000	65536
255.254.0.0	/15	11111111.11111110.00000000.00000000	131072
255.252.0.0	/14	11111111.11111100.00000000.00000000	262144
255.248.0.0	/13	11111111.11111000.00000000.00000000	524288
255.240.0.0	/12	11111111.11110000.00000000.00000000	1048576
255.224.0.0	/11	11111111.11100000.00000000.00000000	2097152
255.192.0.0	/10	11111111.11000000.00000000.00000000	4194304
255.128.0.0	/9	11111111.10000000.00000000.00000000	8388608
255.0.0.0	/8	11111111.00000000.00000000.00000000	16777216
254.0.0.0	/7	11111110.00000000.00000000.00000000	33554432
252.0.0.0	/6	11111100.00000000.00000000.00000000	67108864
248.0.0.0	/5	11111000.00000000.00000000.00000000	134217728
240.0.0.0	/4	11110000.00000000.00000000.00000000	268435456
224.0.0.0	/3	11100000.00000000.00000000.00000000	536870912
192.0.0.0	/2	11000000.00000000.00000000.00000000	1073741824
128.0.0.0	/1	10000000.00000000.00000000.00000000	2147483648
0.0.0.0	/0	00000000.00000000.00000000.00000000	4294967296

Exercise 1: Basic Subnetting

Given the IP address **192.168.1.0/24**, calculate the following:

Subnet Mask:

Number of Hosts :

Exercise 2: Variable-Length Subnet Mask (VLSM)

You have the network 192.168.0.0/24, and you need to create subnets with varying sizes. Calculate:

Subnet 1: Requires 30 hosts

Subnet 2: Requires 12 hosts

Subnet 3: Requires 6 hosts

Subnet 4: Requires 255 hosts

Exercise 3: Subnetting Practice with CIDR

Given the IP address 172.16.0.0/16, divide it into smaller subnets using CIDR notation.

Create subnets for different departments, such as HR, Sales, and IT. Each subnet should have at least 80 hosts but no more than 254. Calculate the subnet addresses and subnet masks for each.

Exercise 4: Supernetting

You have the following four subnets:

- 192.168.1.0/24,
- 192.168.2.0/24,
- 192.168.3.0/24
- 192.168.4.0/24.
- Determine the supernetwork that can encompass all these subnets with the fewest number of bits in the subnet mask.