ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

REDES DE COMPUTADORES I – APRESENTAÇÃO DA UNIDADE CURICULAR

Network Devices

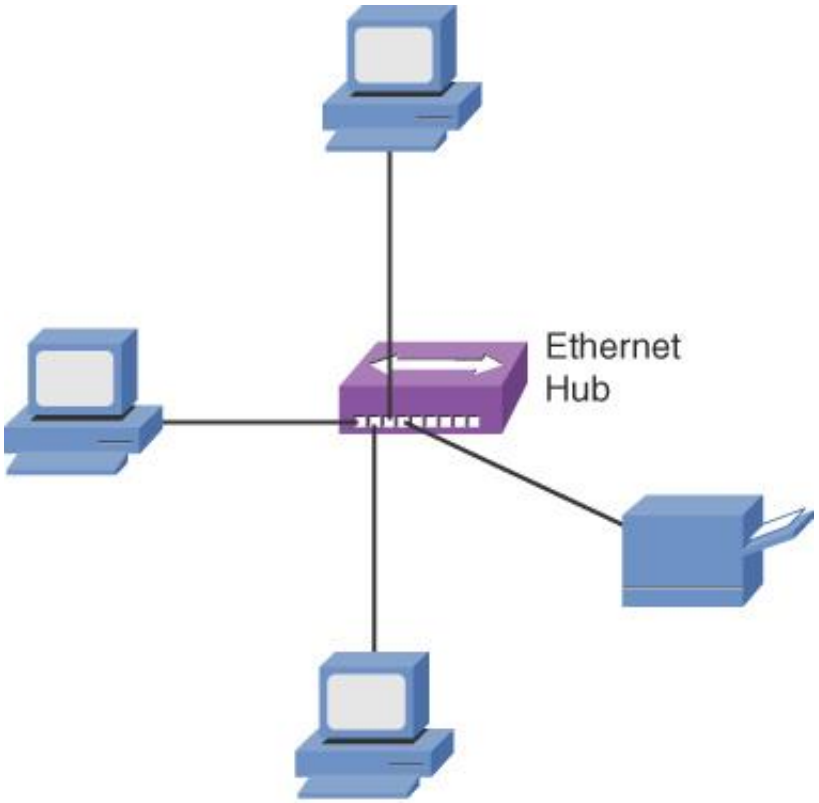
- Layer 2 switch
- Layer 3 capable switch
- Router
- Hub
- Access point
- Bridge
- Wireless LAN controller
- Load balancer
- Proxy server
- Repeater
- Voice gateway
- Media converter
- Intrusion prevention system (IPS)/intrusion detection system (IDS) device
- Firewall
- Voice over Internet Protocol (VoIP) phone
- Printer
- Physical access control devices
- Cameras
- Heating, ventilation, and air conditioning (HVAC) sensors
- Internet of Things (IoT)

Hubs

Hubs

- Network deviceused to interconnect network components, such as clients and servers. Hubs vary in the number of available ports. A hub does not perform inspection of the traffic it passes. Rather, a hub simply receives traffic in a port and repeats that traffic out all of its other ports.
- **Passive hub**: This type of hub does not amplify (that is, electrically regenerate) received bits.
- **Active hub**: This type of hub regenerates incoming bits as they are sent out all the ports on a hub other than the port on which the bits were received.
- **Smart hub**: The term smart hub usually implies an active hub with enhanced features, such as support for Simple Network Management Protocol (SNMP).

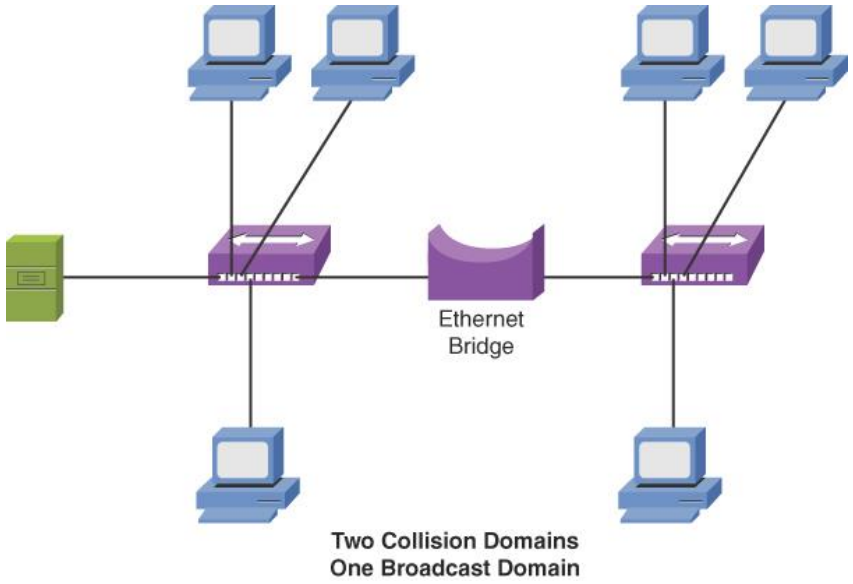
Hubs



Bridges

Bridges

- connect different types of networks. While this was important so that the two networks could communicate, it also ended up creating additional broadcast domains.

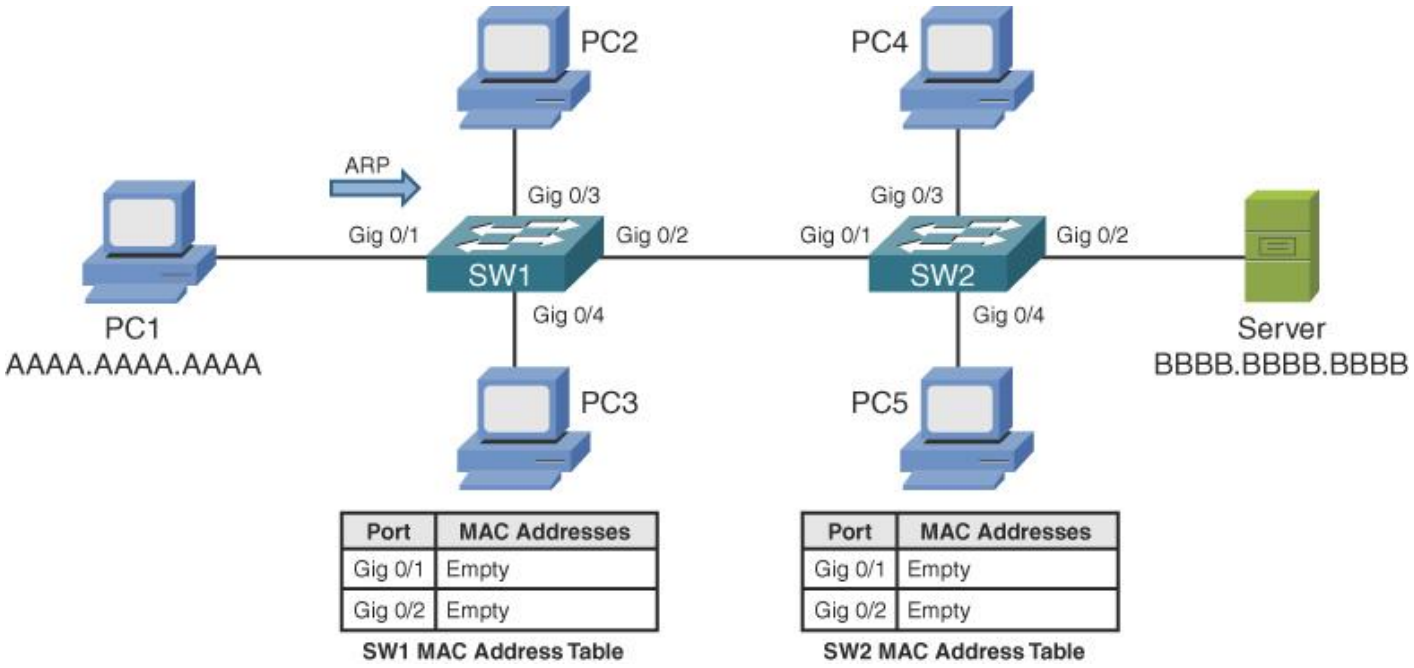


Layer 2 Switch

Layer 2 Switch

- Data Link Layer switch, is a network device that operates at the second layer of the OSI (Open Systems Interconnection) model. Its primary function is to forward data frames between devices within a local area network (LAN) based on their MAC (Media Access Control) addresses, which are unique hardware identifiers assigned to network interface cards (NICs) or other network devices.
- Layer 2 switches use a technique called MAC address learning to maintain a MAC address table, which is essentially a mapping of MAC addresses to corresponding ports on the switch. When a data frame arrives at a switch, it examines the destination MAC address and looks it up in its MAC address table. If the switch finds a match, it forwards the frame to the appropriate port connected to the destination device. If the destination MAC address is unknown or not in the table, the switch broadcasts the frame to all connected ports except the incoming port, a process known as flooding.

Layer 2 Switch



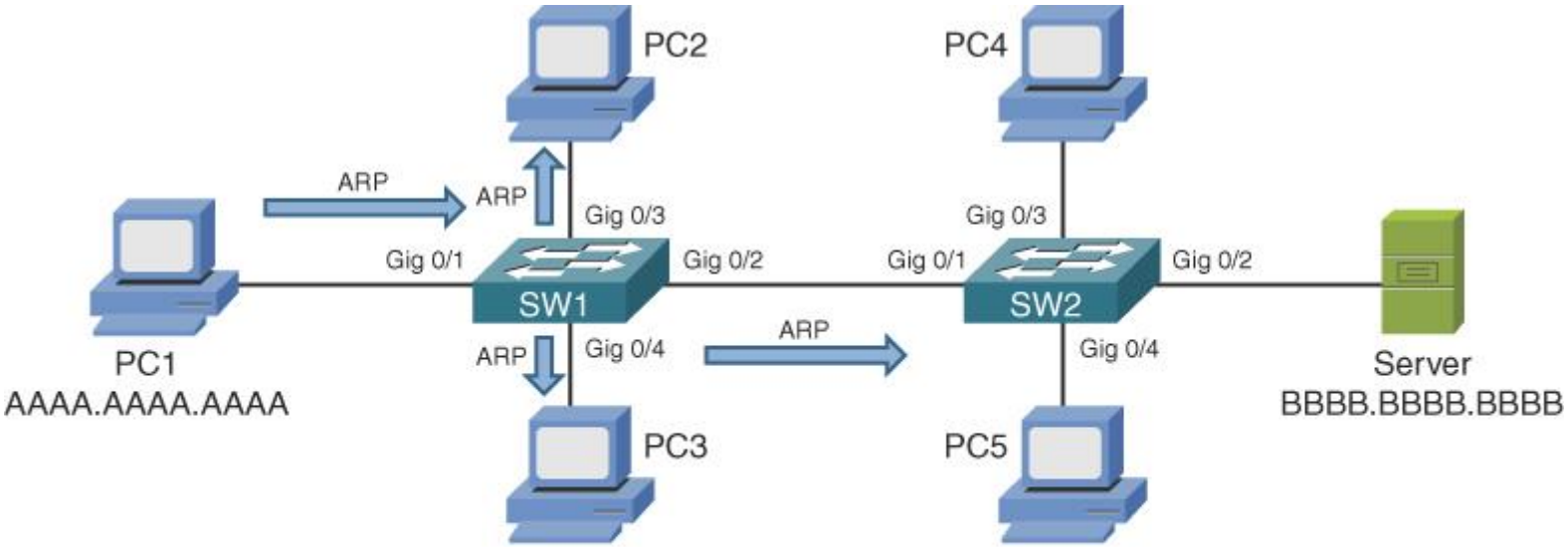
Port	MAC Addresses
Gig 0/1	Empty
Gig 0/2	Empty

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	Empty
Gig 0/2	Empty

SW2 MAC Address Table

Layer 2 Switch



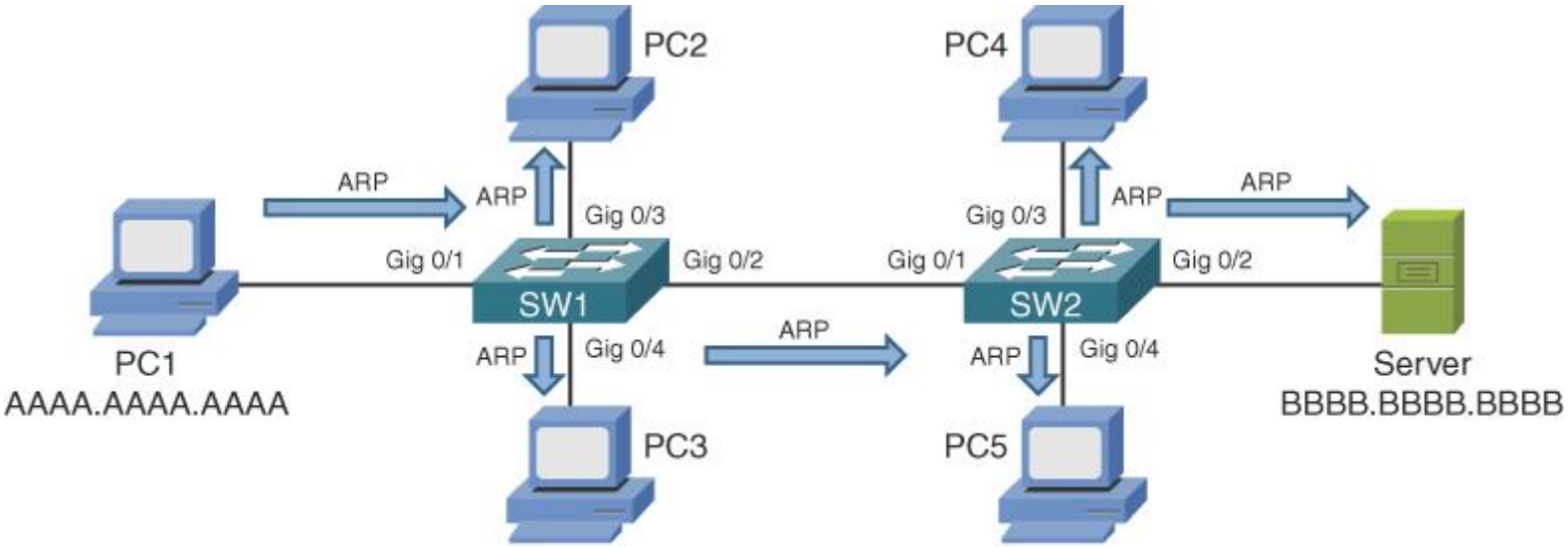
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	Empty
Gig 0/2	Empty

SW2 MAC Address Table

Layer 2 Switch



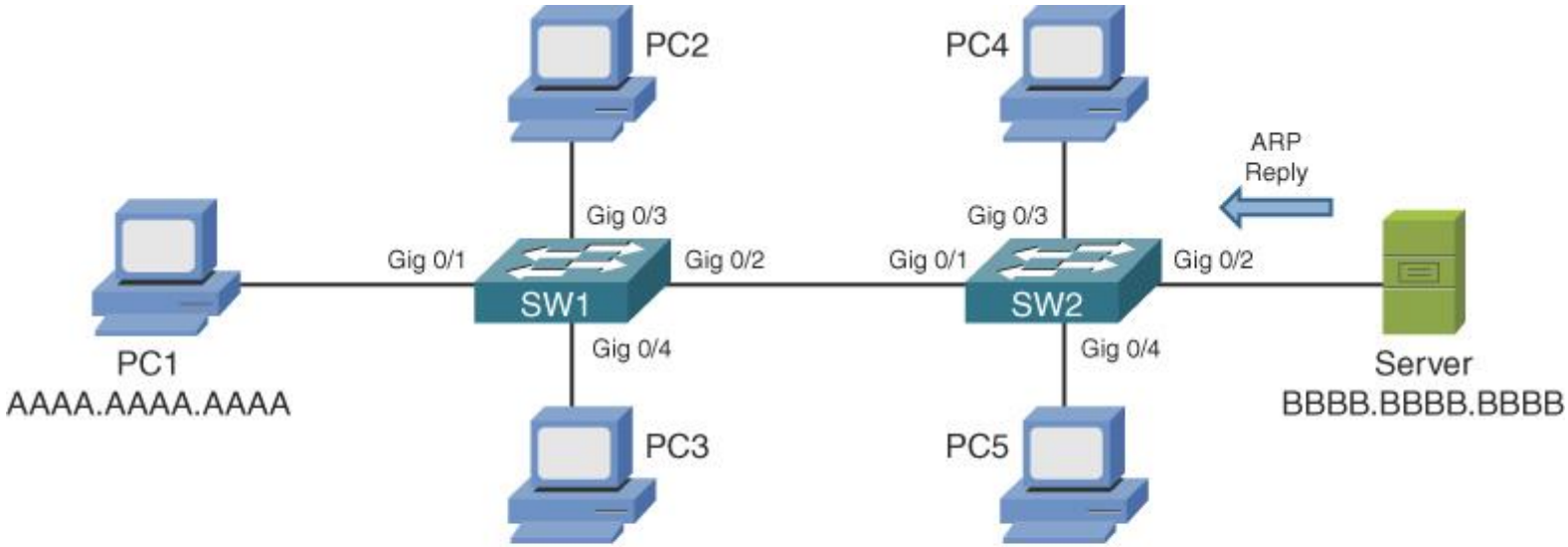
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW2 MAC Address Table

Layer 2 Switch



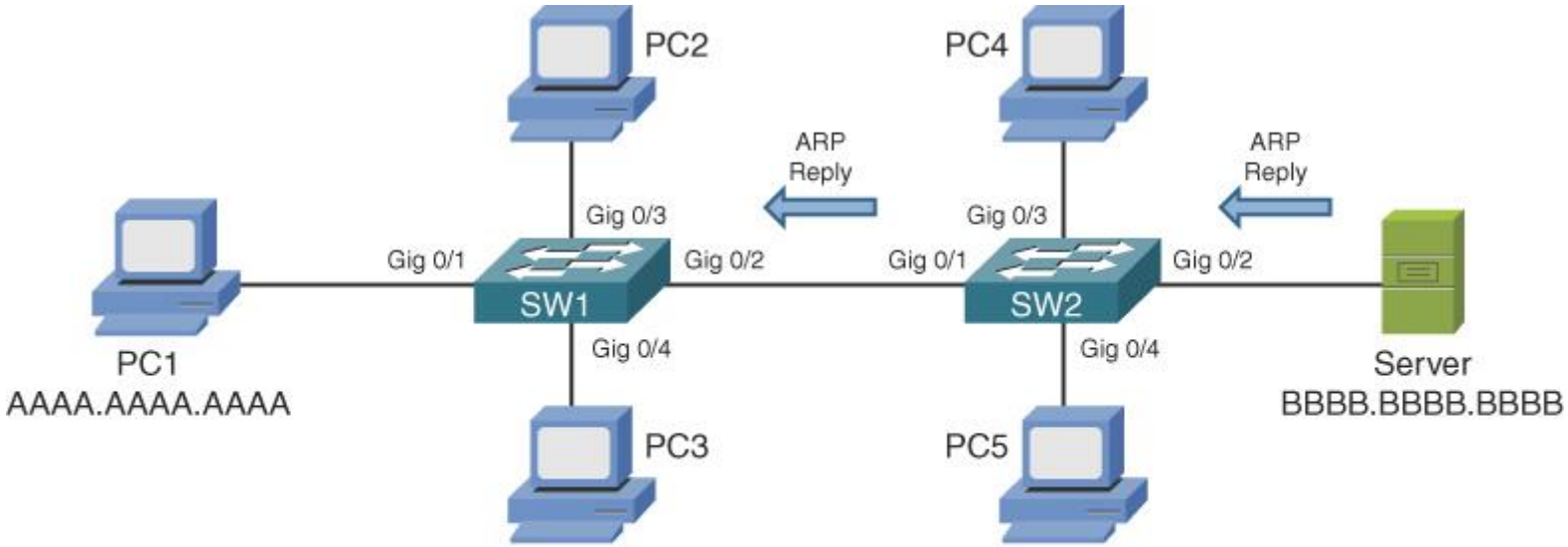
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW2 MAC Address Table

Layer 2 Switch



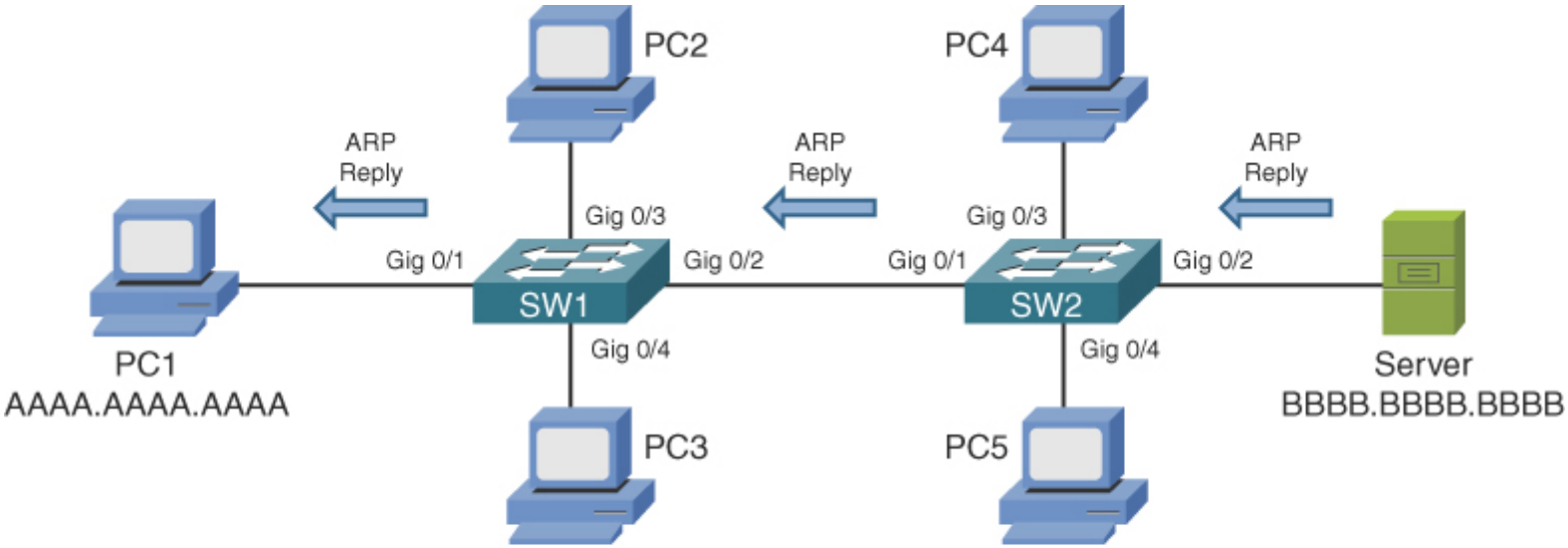
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	Empty

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW2 MAC Address Table

Layer 2 Switch



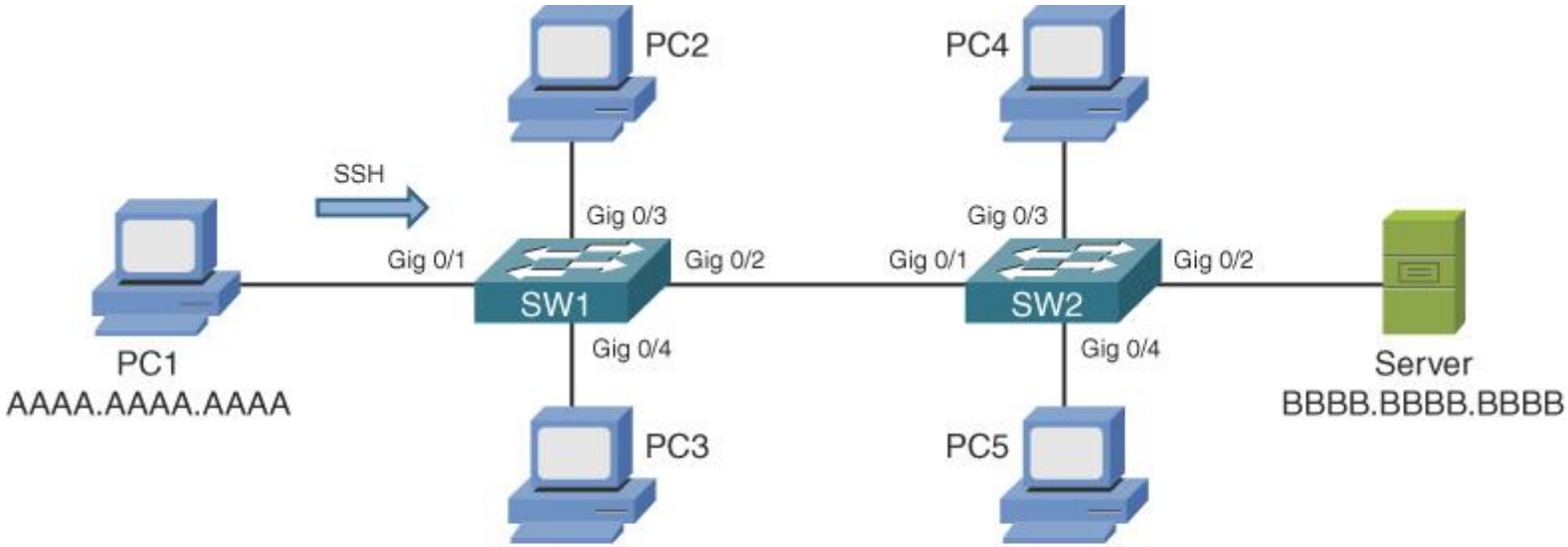
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW2 MAC Address Table

Layer 2 Switch



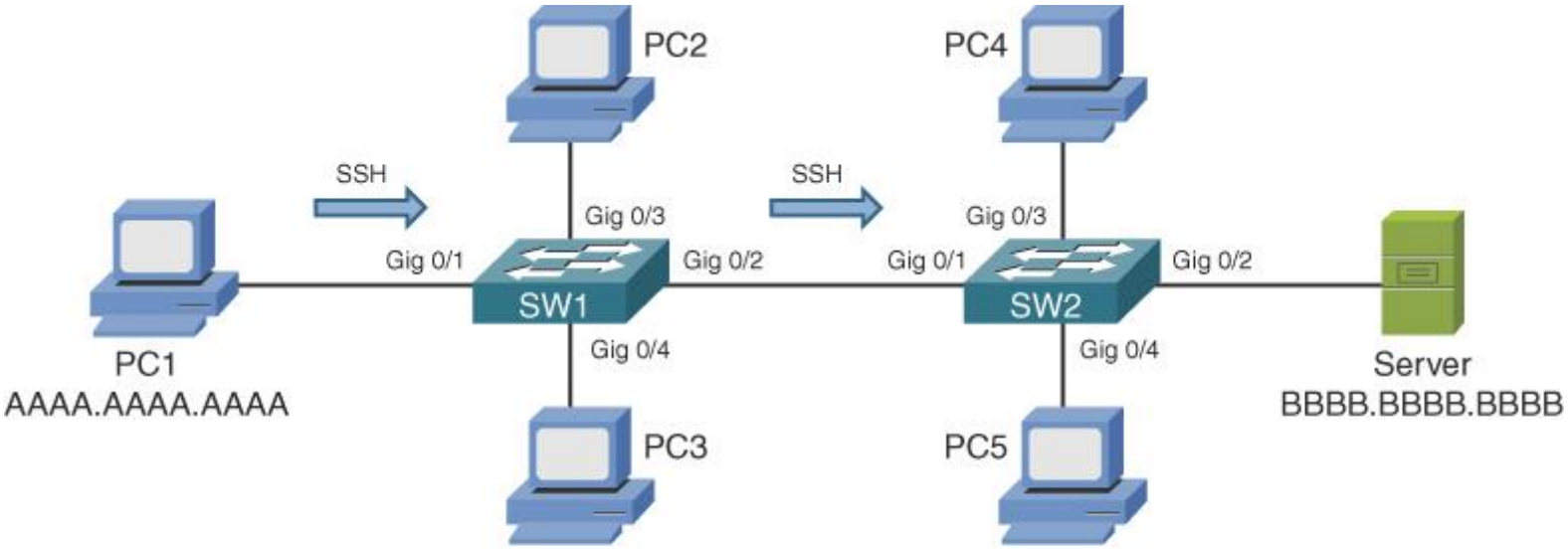
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW2 MAC Address Table

Layer 2 Switch



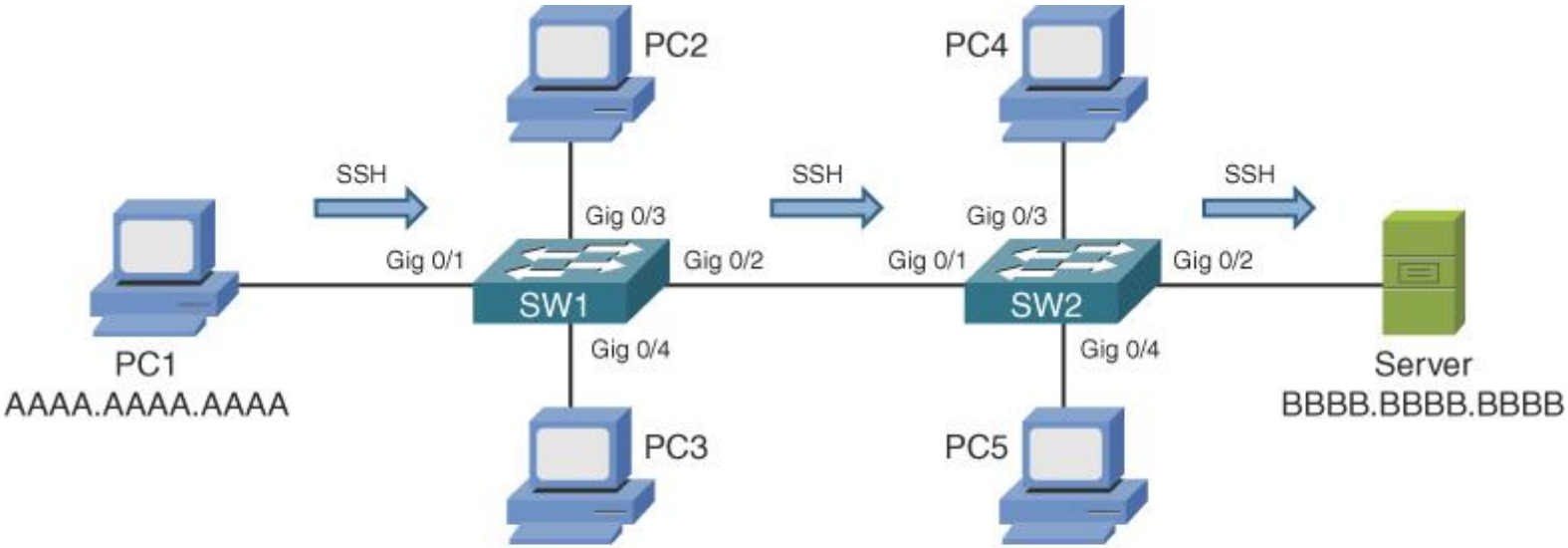
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW2 MAC Address Table

Layer 2 Switch



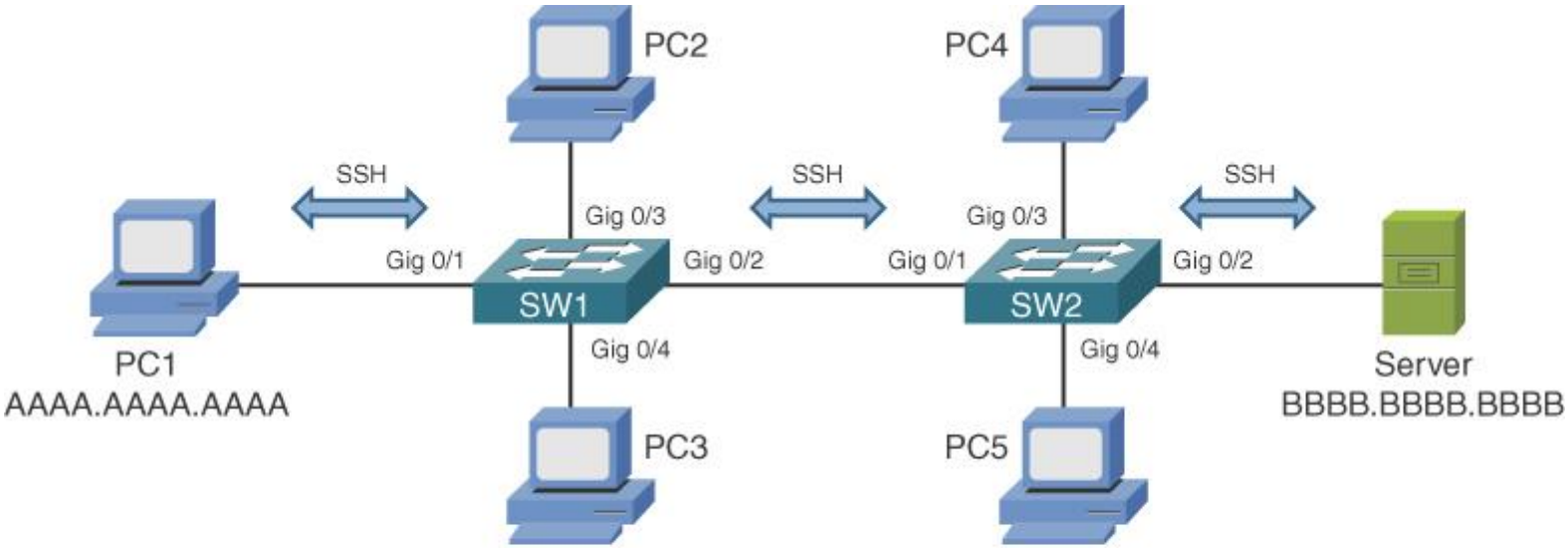
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW2 MAC Address Table

Layer 2 Switch



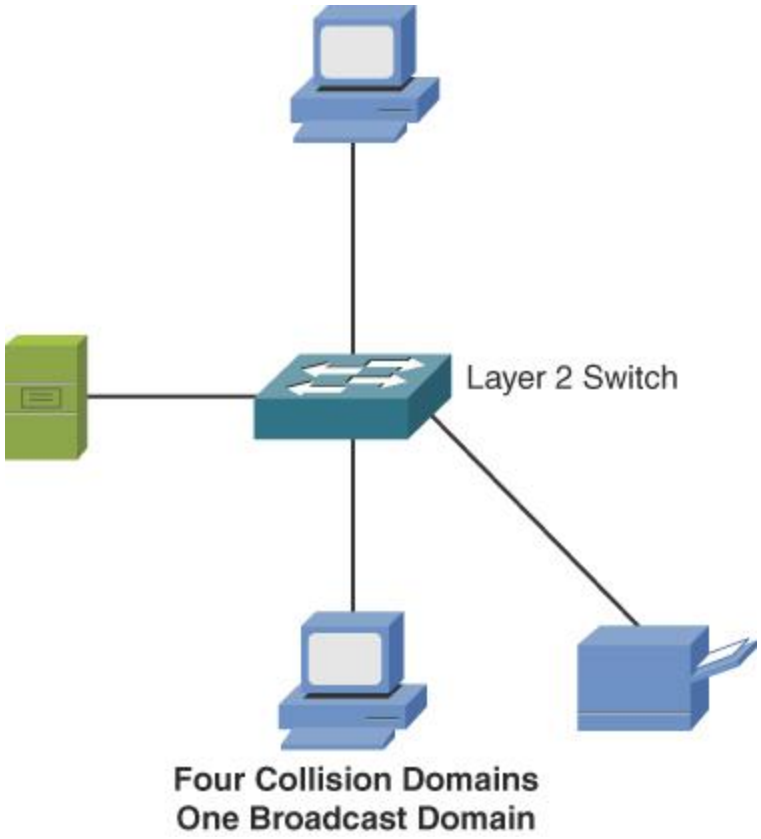
Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

SW1 MAC Address Table

Port	MAC Addresses
Gig 0/1	AAAA.AAAA.AAAA
Gig 0/2	BBBB.BBBB.BBBB

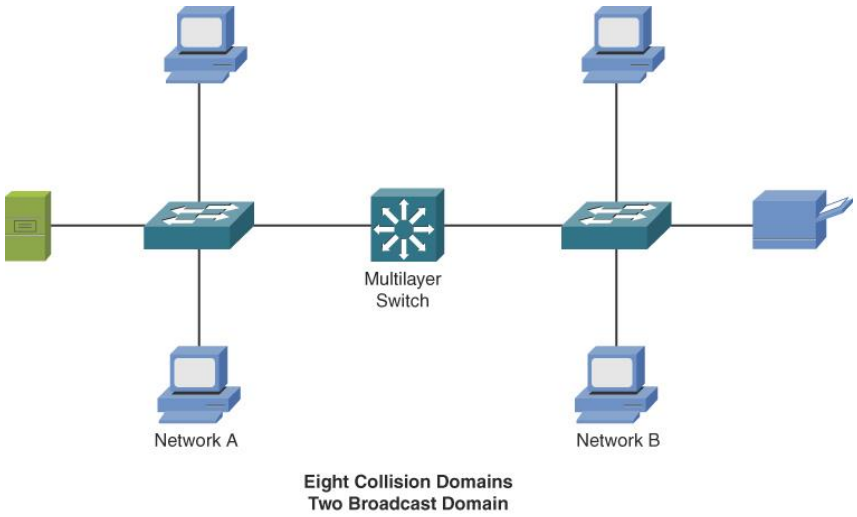
SW2 MAC Address Table

Layer 2 Switch



Layer 3 Switch

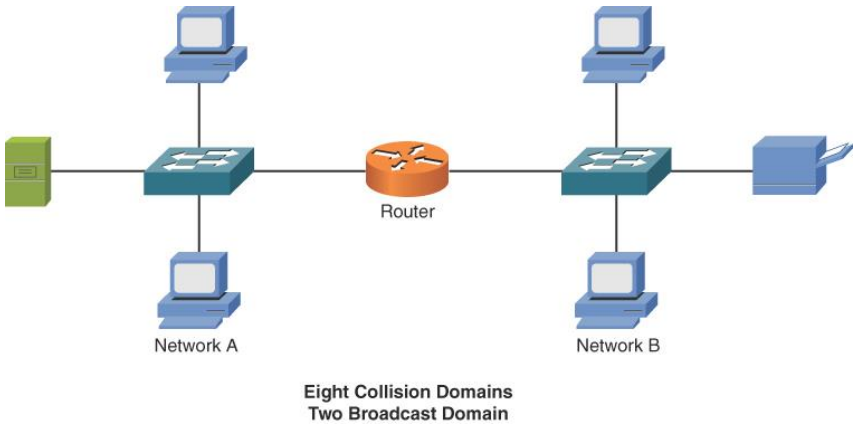
- Layer 3 Switch
- A Layer 3 switch, also known as a multilayer switch or a network switch with routing capabilities, is a network device that combines the features of a Layer 2 switch and a router. It operates at both the Data Link Layer (Layer 2) and the Network Layer (Layer 3) of the OSI (Open Systems Interconnection) model. Layer 3 switches forward data based on MAC addresses (like Layer 2 switches) and IP addresses (like routers), which allows them to efficiently route traffic between different IP networks or subnets within a local area network (LAN) or a larger network environment.



Routers

•Router

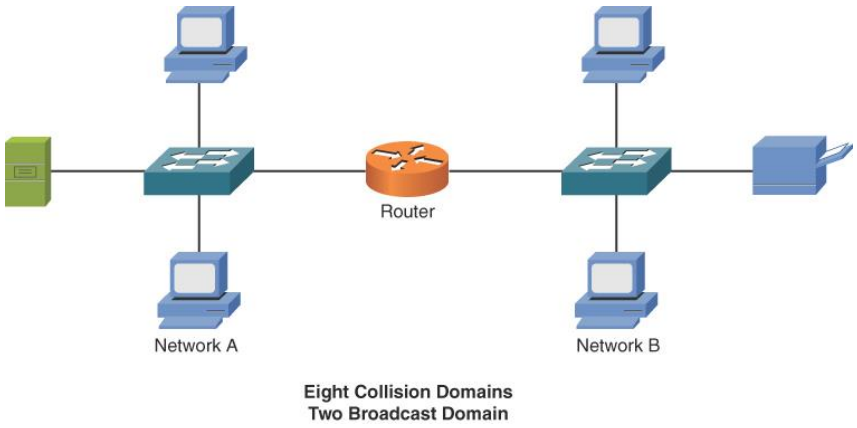
- A network router is a networking device that forwards data packets between different networks or subnets, acting as a gateway connecting these networks. Routers operate at the Network Layer (Layer 3) of the OSI (Open Systems Interconnection) model and primarily use IP (Internet Protocol) addresses to determine the best path for forwarding data packets to their intended destinations.



Routers

•Router

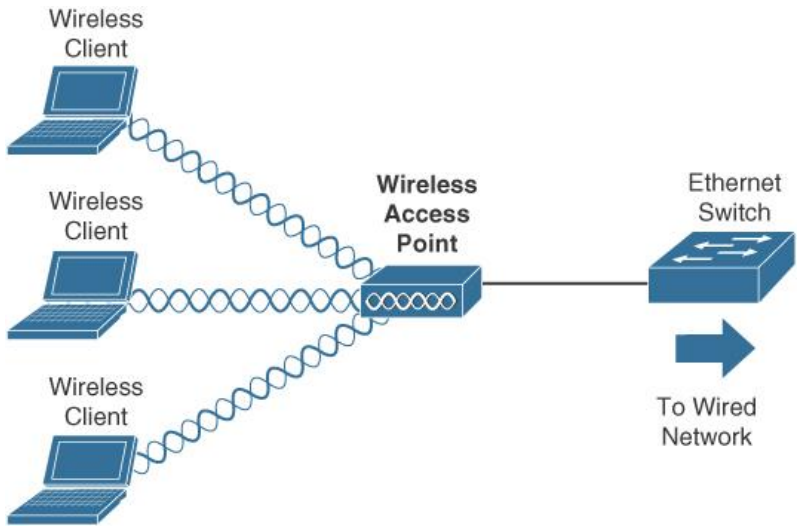
1. Operate at the Network Layer (Layer 3) of the OSI model, dealing with IP addresses and IP packets.
2. Connect different IP networks or subnets and route traffic between them.
3. Utilize routing tables and routing protocols to determine the best path for forwarding data packets.
4. Provide essential networking functions, such as Network Address Translation (NAT), which enables multiple devices on a private network to share a single public IP address for Internet access.
5. Support security features like firewall capabilities, access control lists (ACLs), and VPN (Virtual Private Network) termination for secure communication between remote networks or users.



Wireless access point (AP)

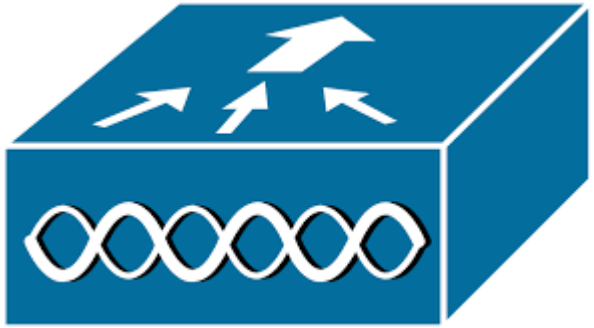
•AP

- In wireless networks, a device that permits wireless clients to access the network. Access points tend to fall into two categories: lightweight and autonomous. A lightweight AP cannot perform control plane functions and requires a wireless LAN controller (WLC) for the control plane. An autonomous AP does not require a WLC.



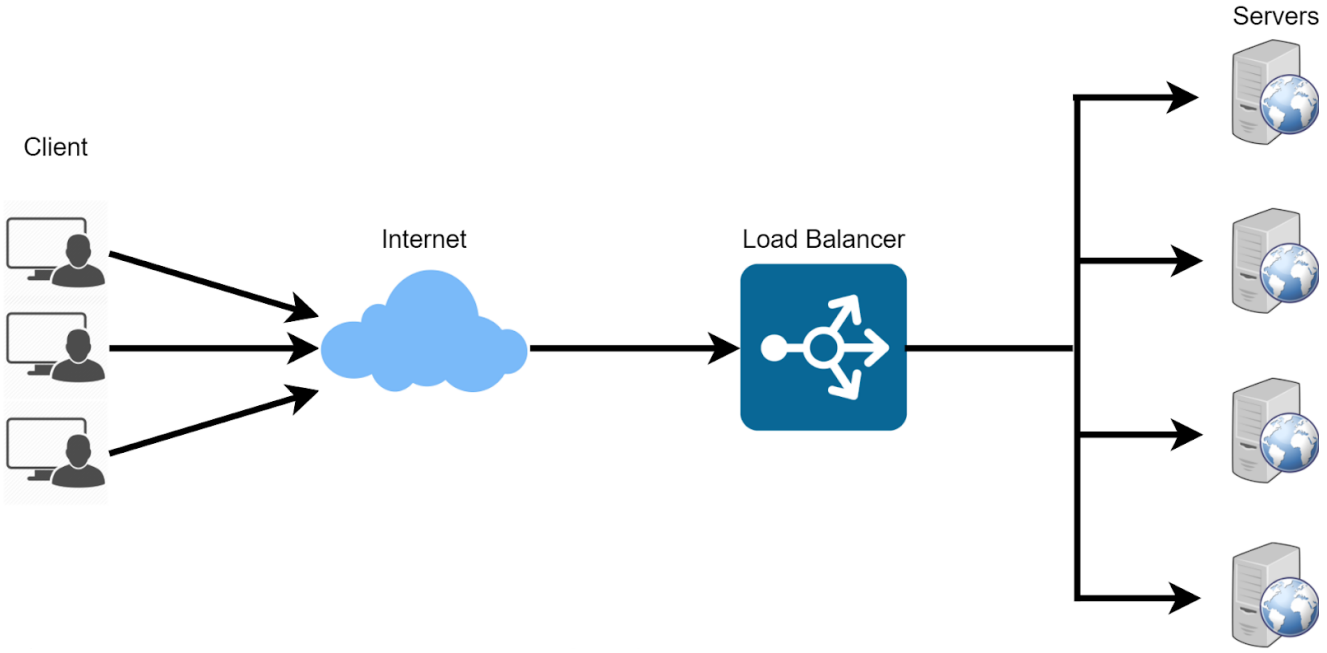
Wireless LAN Controller

- Access points types: autonomous and lightweight.
- A Wireless LAN (Local Area Network) Controller, often abbreviated as WLC, is a network device used to manage, configure, and monitor multiple wireless access points within a Wi-Fi network. The primary function of a WLC is to centralize and simplify the management of wireless access points, ensuring consistent performance, security, and policy enforcement across the entire wireless network.



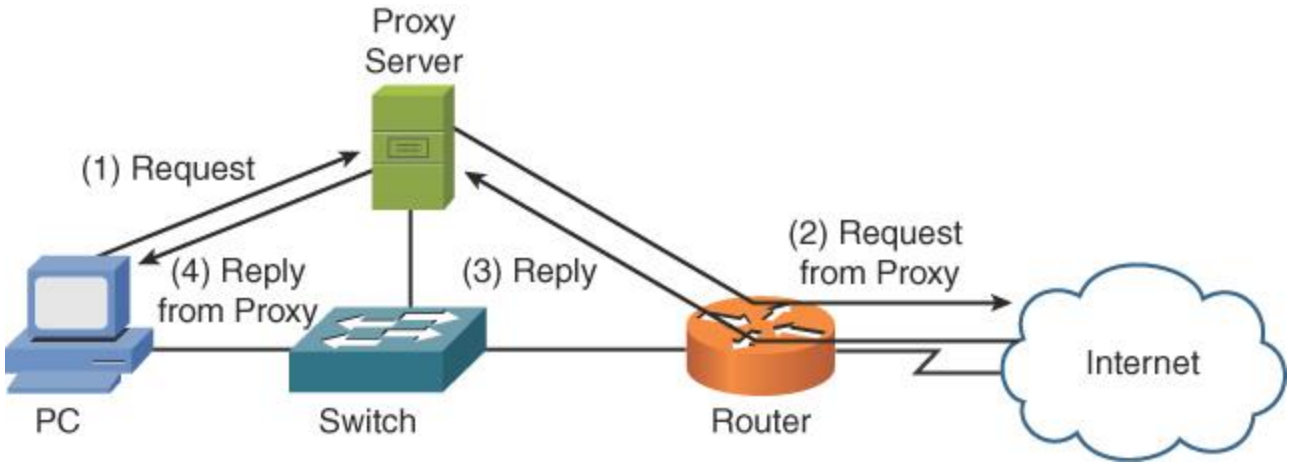
Load Balancer

•A network load balancer is a networking device or service that distributes network traffic across multiple servers or resources to optimize resource utilization, minimize response time, and ensure high availability and reliability.



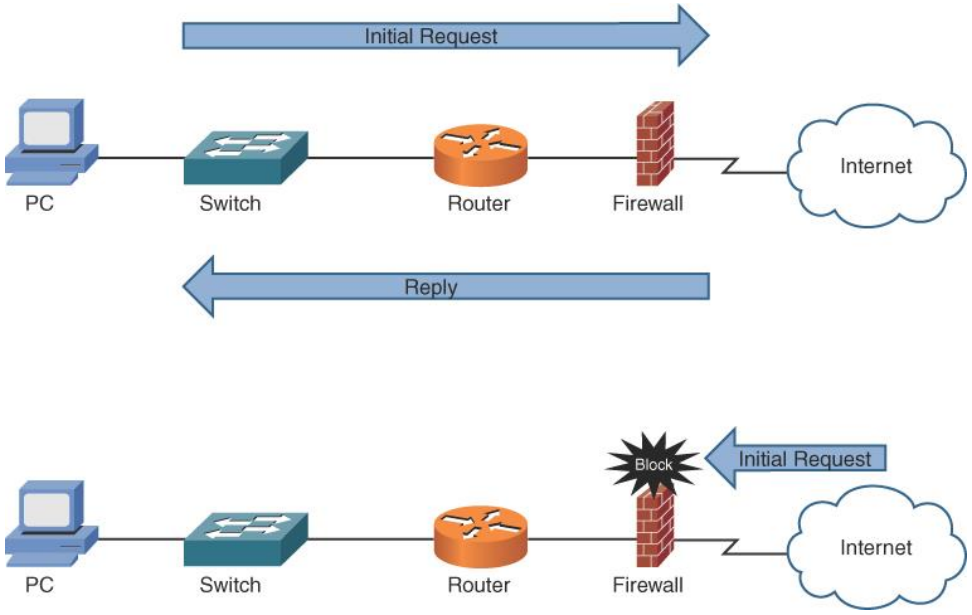
Proxy Servers

•A server that intercepts requests being sent from a client and forwards those requests to their intended destination. The proxy server then sends any return traffic to the client that initiated the session. This provides address hiding for the client. Also, some proxy servers conserve WAN bandwidth by offering a content-caching function. In addition, some proxy servers offer URL filtering to, for example, block users from accessing social networking sites during working hours.



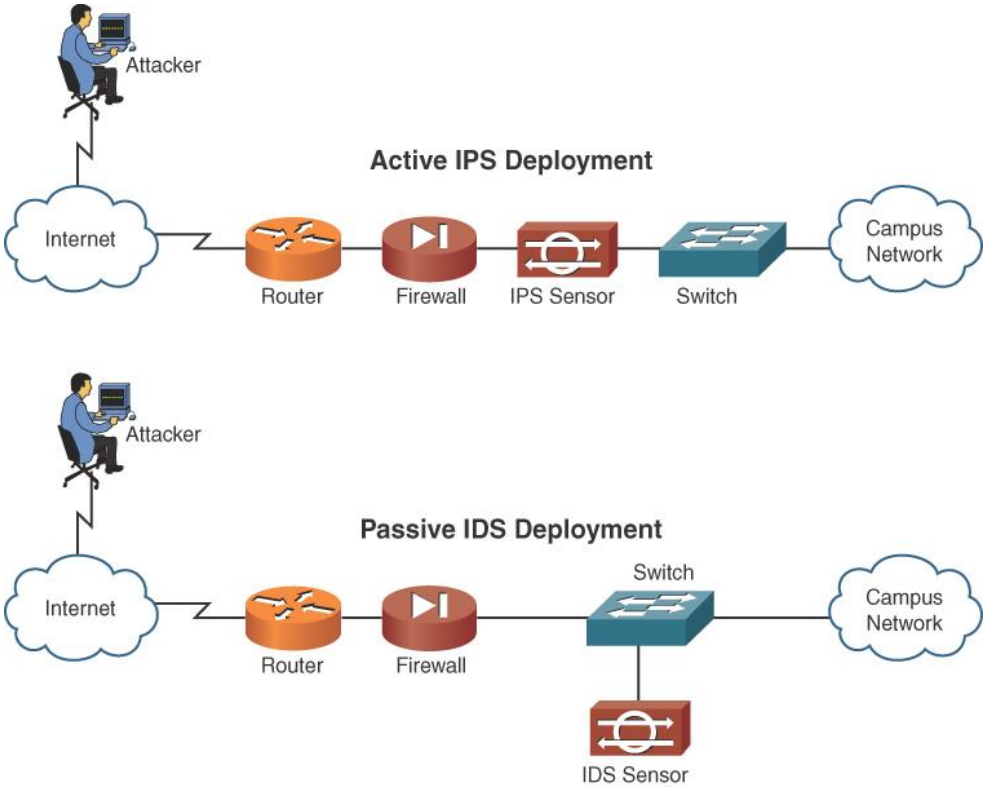
Firewalls

•Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a trusted internal network and an untrusted external network, such as the Internet. Firewalls can be implemented as hardware, software, or a combination of both.



Intrusion Detection and Prevention

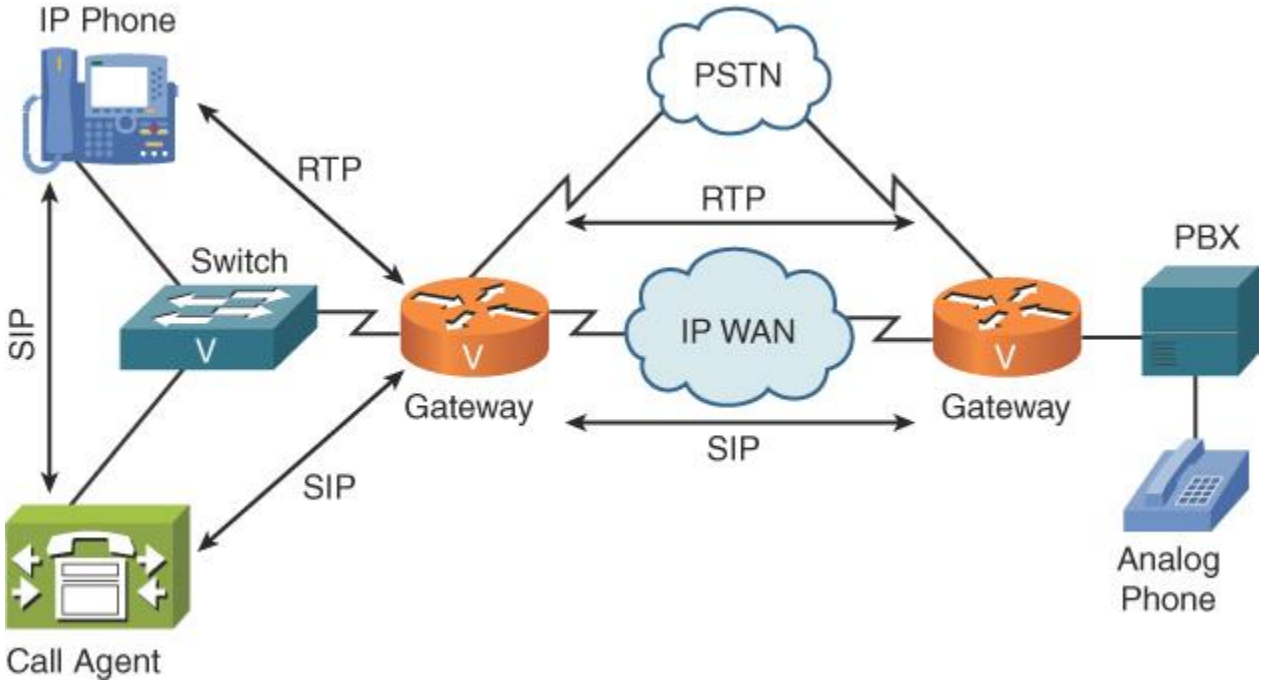
- intrusion detection system (IDS) device An system that seeks to recognize attack traffic and prevent that traffic from entering a network or devices.
- intrusion prevention system (IPS) A system that seeks to alert administrators regarding a cybersecurity attack but that typically does not prevent the attack through its own actions.



Voice over IP Protocols and Components

- Voice over IP (VoIP) protocols are a set of rules and standards that enable the transmission of voice and multimedia data over the internet. They manage signaling, media negotiation, and packetization of audio and video data. Some common VoIP protocols include:
  - Session Initiation Protocol (SIP): SIP is a widely used signaling protocol for establishing, modifying, and terminating multimedia sessions, such as voice calls and video conferences. It manages session initiation, authentication, and call routing.
  - Real-time Transport Protocol (RTP): RTP is a protocol used to transmit audio and video data in real-time over IP networks. It provides mechanisms for packet sequencing, timing reconstruction, and jitter management to ensure smooth delivery of media streams.
  - Real-time Transport Control Protocol (RTCP): RTCP works alongside RTP and provides feedback on the quality of service (QoS) during a multimedia session. It monitors data transmission and reports on packet loss, jitter, and delay, helping to optimize network performance.
  - H.323: H.323 is an older suite of protocols for multimedia communication over IP networks. It includes signaling, call setup, and media transport components, but has been largely superseded by SIP due to its complexity and limited flexibility.
  - Media Gateway Control Protocol (MGCP): MGCP is a call control protocol used to manage media gateways, which are devices that convert between different media formats, such as analog phone lines and digital VoIP networks. MGCP enables centralized control of media gateways by a call agent or softswitch.
- These protocols work together to ensure reliable, efficient, and high-quality VoIP communication over the internet.

Voice over IP Protocols and Components

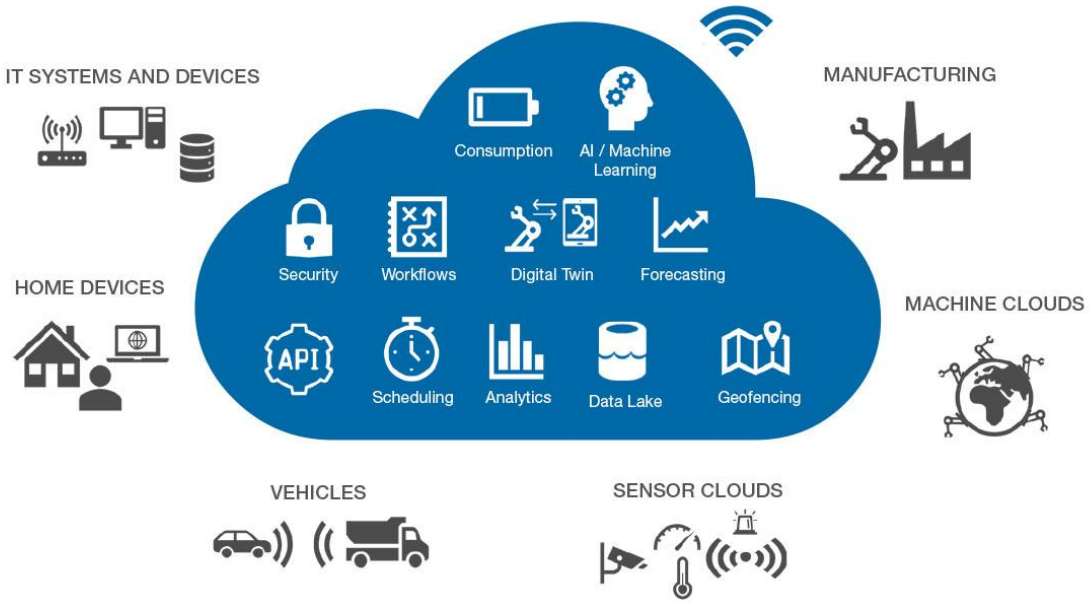


Voice over IP Protocols and Components

Protocol/Device	Description
IP phone	An IP phone is a telephone with an integrated Ethernet connection. Although users speak into a traditional analog handset (or headset) on the IP phone, the IP phone digitizes the user's speech, packetizes it, and sends it out over a data network (via the IP phone's Ethernet port). While an IP phone is a common example of a VoIP endpoint, an alternative is software running on a computer.
Call agent	A call agent is a repository for a VoIP network's dial plan. For example, when a user dials a number from an IP phone, the call agent analyzes the dialed digits and determines how to route the call toward the destination.
Gateway	A gateway in a VoIP network acts as a translator between two different telephony signaling environments. previous slide both gateways interconnect a VoIP network with the PSTN. Also, the gateway on the right interconnects a traditional PBX with a VoIP network.
PBX	A private branch exchange (PBX) is a privately owned telephone switch traditionally used in corporate telephony systems. Although a PBX is not typically considered a VoIP device, it connects into a VoIP network through a gateway, as shown previous slide.
Analog phone	An analog phone is a traditional telephone, like the ones individuals used to have in their homes. Even though an analog phone is not typically considered a VoIP device, it can connect to a VoIP network via a VoIP adapter or, as shown previous slide, via a PBX, which is connected to a VoIP network.
SIP	Session Initiation Protocol (SIP) is a signaling, setup, and management protocol used with voice and video sessions over IP networks. SIP, in conjunction with other protocols, specifies the encoder/decoder (codec) that will be used for voice and video connections over the network.
RTP	Real-Time Transport Protocol (RTP) is a protocol that carries voice and interactive video. Notice previous slide that the bidirectional RTP stream does not flow through the call agent.

Other network Devices

- Printer
- Physical Access Control Devices
- Cameras
- Heating, Ventilation, and Air Conditioning (HVAC) Sensors



Internet of Things (IoT)

- The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity, allowing them to collect, exchange, and analyze data. IoT devices can communicate and interact with one another, as well as with central systems or human users, enabling automation, remote monitoring, and improved decision-making.
- Z-Wave
- ANT+
- Bluetooth
- NFC
- IR
- RFID
- 802.11
- SIGFOX

Supervisory Control and Data Acquisition (SCADA)

- Industrial Control Systems/Supervisory Control and Data Acquisition (SCADA)
- SCADA systems are commonly used in industries such as power generation, water treatment, oil and gas, manufacturing, and transportation. They help improve efficiency, safety, and reliability by enabling operators to monitor and control processes from a central location, often in real-time.
- A typical SCADA system consists of the following components:
  - Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs): These devices are connected to sensors and actuators, gathering data and executing control commands in the field.
  - Communication networks: These networks transmit data between RTUs/PLCs and the central control system. They can include wired or wireless connections, and may use various communication protocols.
  - Human-Machine Interface (HMI): The HMI is the graphical interface used by operators to monitor and interact with the SCADA system. It displays process data, system status, and alarms, allowing operators to issue commands and adjust settings.
  - Data servers and historians: These components collect, store, and analyze process data for trending, reporting, and decision-making purposes.
  - Control software: The control software processes data, applies control logic, and manages communication with field devices and operators.

Supervisory Control and Data Acquisition (SCADA)

- Industrial Control Systems/Supervisory Control and Data Acquisition (SCADA)
- SCADA systems are commonly used in industries such as power generation, water treatment, oil and gas, manufacturing, and transportation. They help improve efficiency, safety, and reliability by enabling operators to monitor and control processes from a central location, often in real-time.
- A typical SCADA system consists of the following components:
  - Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs): These devices are connected to sensors and actuators, gathering data and executing control commands in the field.
  - Communication networks: These networks transmit data between RTUs/PLCs and the central control system. They can include wired or wireless connections, and may use various communication protocols.
  - Human-Machine Interface (HMI): The HMI is the graphical interface used by operators to monitor and interact with the SCADA system. It displays process data, system status, and alarms, allowing operators to issue commands and adjust settings.
  - Data servers and historians: These components collect, store, and analyze process data for trending, reporting, and decision-making purposes.
  - Control software: The control software processes data, applies control logic, and manages communication with field devices and operators.

LAB

- Labs
  - 1.2.2.1 Packet Tracer - Adding IoT Devices to a Smart Home
  - 1.2.2.3 Packet Tracer - Connect and Monitor IoT Devices
  - 4.1.1.6 Packet Tracer - Explore the Smart Home
  - 6.1.4.7 Packet Tracer - Configure Firewall Settings

Bibliografia

- SEQUEIRA, Anthony. *CompTIA Network+ N10-008 Cert Guide*. Pearson IT Certification, 2021.
- ODOM, Wendell. *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press, 2019.
- ODOM, W. CCNA 200-301, Volume 1 Official Cert Guide. 2019.
- Cisco Netacad Course Resources