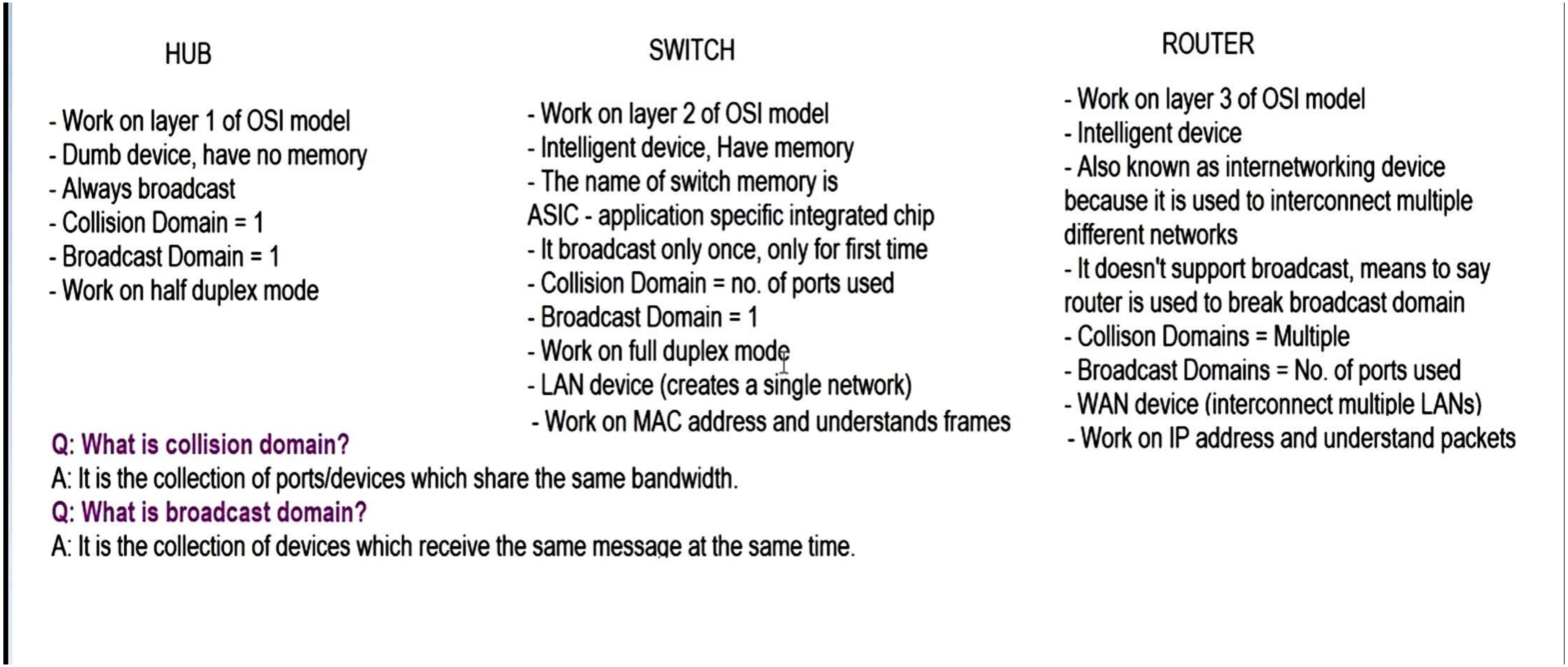
Network Devices:

- Hub
- Bridge
- Switch
- Router
- Gateway
- Access Point
- Firewall
- Wireless Controller
- PBX (Private Branch Exchange)



HUB

- Work on layer 1 of OSI model
- Dumb device, have no memory
- Always broadcast
- Collision Domain = 1
- Broadcast Domain = 1
- Work on half duplex mode

SWITCH

- Work on layer 2 of OSI model
- Intelligent device, Have memory
- The name of switch memory is
ASIC - application specific integrated chip
- It broadcast only once, only for first time
- Collision Domain = no. of ports used
- Broadcast Domain = 1
- Work on full duplex mode
- LAN device (creates a single network)
- Work on MAC address and understands frames

ROUTER

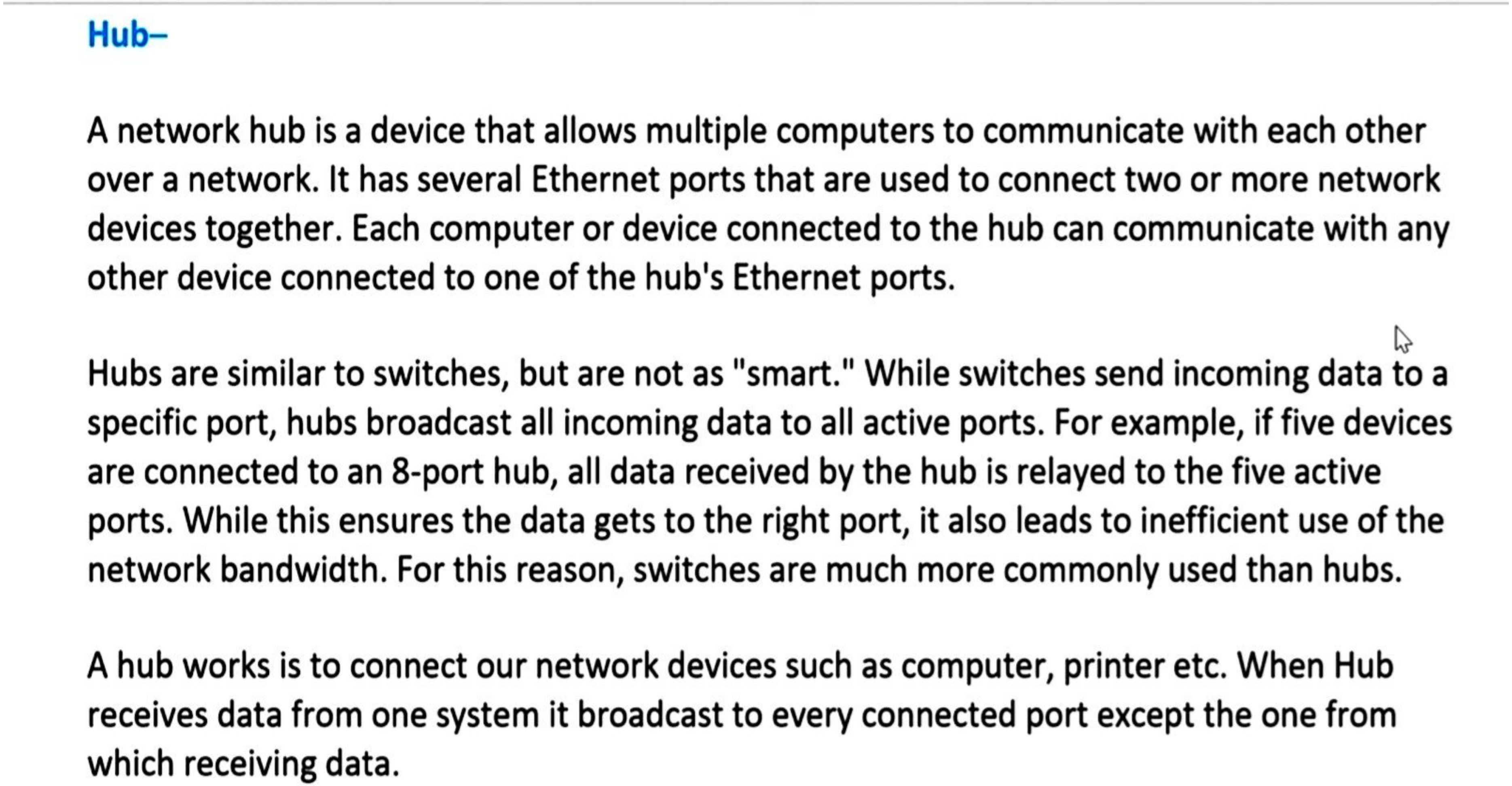
- Work on layer 3 of OSI model
- Intelligent device
- Also known as internetworking device because it is used to interconnect multiple different networks
- It doesn't support broadcast, means to say router is used to break broadcast domain
- Collison Domains = Multiple
- Broadcast Domains = No. of ports used
- WAN device (interconnect multiple LANs)
- Work on IP address and understand packets

Q: What is collision domain?

A: It is the collection of ports/devices which share the same bandwidth.

Q: What is broadcast domain?

A: It is the collection of devices which receive the same message at the same time.



Hub–

A network hub is a device that allows multiple computers to communicate with each other over a network. It has several Ethernet ports that are used to connect two or more network devices together. Each computer or device connected to the hub can communicate with any other device connected to one of the hub's Ethernet ports.

Hubs are similar to switches, but are not as "smart." While switches send incoming data to a specific port, hubs broadcast all incoming data to all active ports. For example, if five devices are connected to an 8-port hub, all data received by the hub is relayed to the five active ports. While this ensures the data gets to the right port, it also leads to inefficient use of the network bandwidth. For this reason, switches are much more commonly used than hubs.

A hub works is to connect our network devices such as computer, printer etc. When Hub receives data from one system it broadcast to every connected port except the one from which receiving data.

Hub has many demerit-

It uses more bandwidth of the network due to unnecessary network broadcast. Hus works on half duplex which means hub can't send or receive data at the same time. Due to this data collision may occur which may corrupt your data or may need to send again.

HUB in brief:

-Layer 1 device

-1 collision domain

-Half duplex

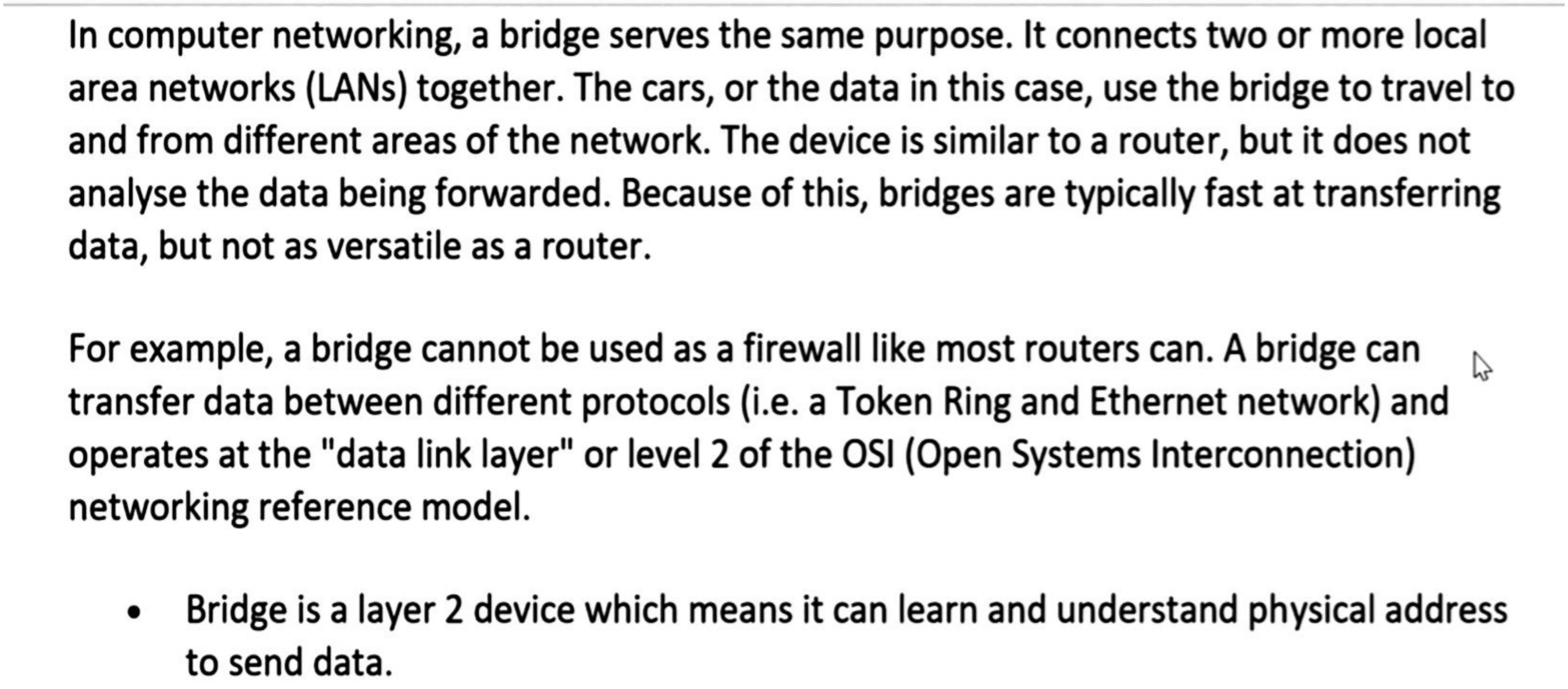
-Wasted Bandwidth

-Security Risks

-Replaced by switches.

Bridge-

When a road needs to extend across a river or valley, a bridge is built to connect the two land masses. Since the average car cannot swim or fly, the bridge makes it possible for automobiles to continue driving from one land mass to another.



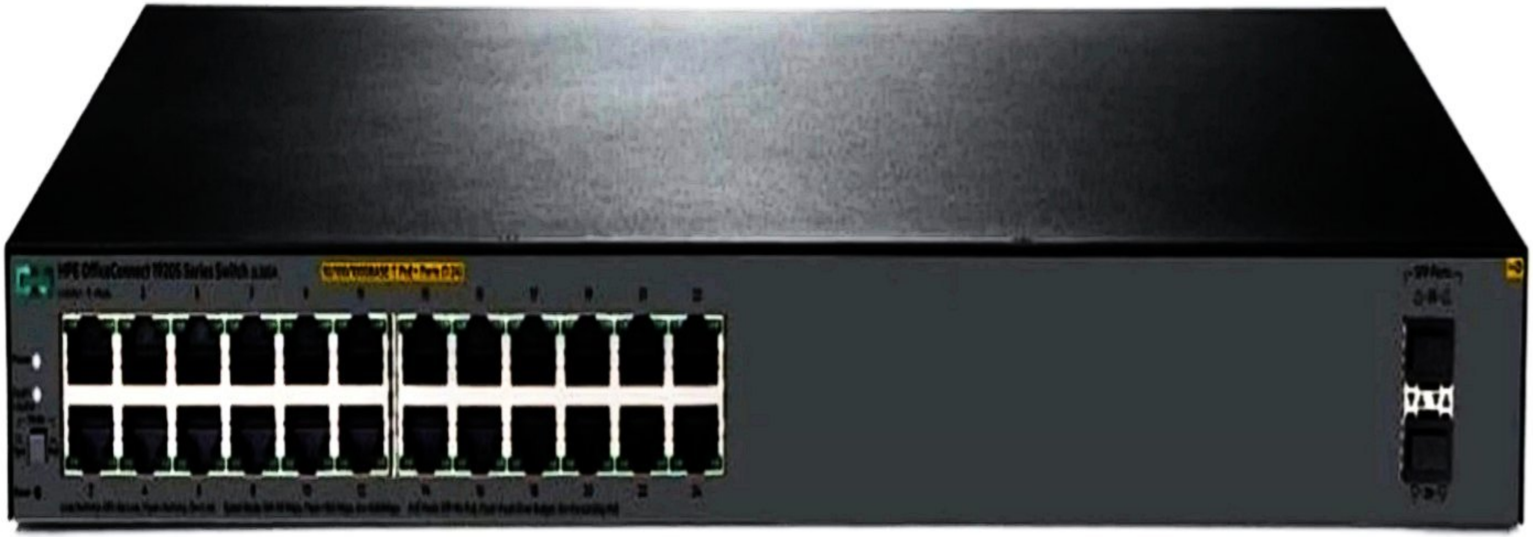
In computer networking, a bridge serves the same purpose. It connects two or more local area networks (LANs) together. The cars, or the data in this case, use the bridge to travel to and from different areas of the network. The device is similar to a router, but it does not analyse the data being forwarded. Because of this, bridges are typically fast at transferring data, but not as versatile as a router.

For example, a bridge cannot be used as a firewall like most routers can. A bridge can transfer data between different protocols (i.e. a Token Ring and Ethernet network) and operates at the "data link layer" or level 2 of the OSI (Open Systems Interconnection) networking reference model.

- Bridge is a layer 2 device which means it can learn and understand physical address to send data.

- It segments LAN into smaller sections
- 2 collision domains it means data can be send or receive on segment of the network at the same time.
- It has usually 2 ports.
- Now a days bridges are not being used anymore it has been replaced by switches.

Switch-

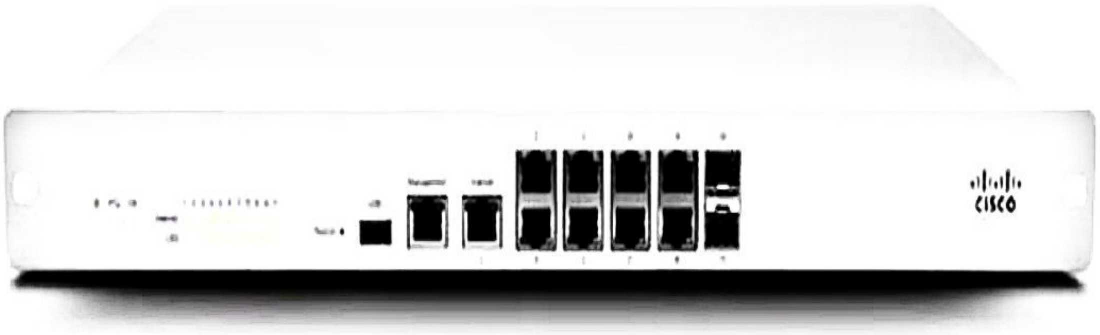


A switch is used to network multiple computers together. Switches made for the consumer market are typically small, flat boxes with 12, 24 and 48 Ethernet ports. These ports can connect to computers, cable or DSL modems, and other switches. High-end switches can have more than 50 ports and often are rack mounted.

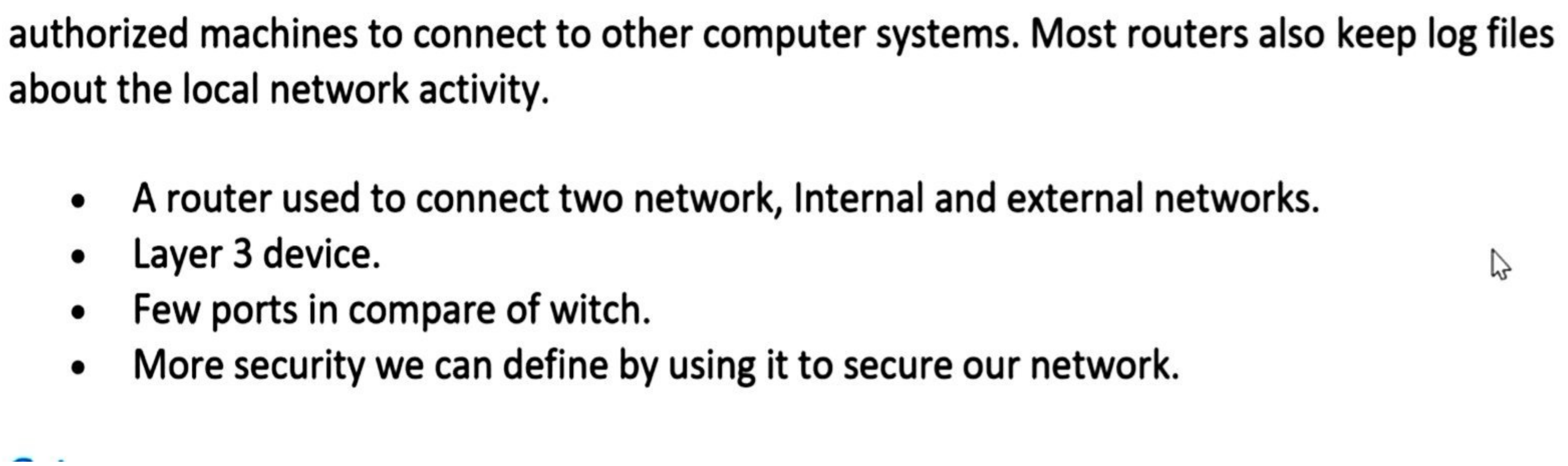
Switches are more advanced than hubs and less capable than routers. Unlike hubs, switches can limit the traffic to and from each port so that each device connected to the switch has a sufficient amount of bandwidth. For this reason, you can think of a switch as a "smart hub." However, switches don't provide the firewall and logging capabilities that routers do. Routers can often be configured by software (typically via a Web interface), while switches only work the way the hardware was designed.

- A switch is a layer 2 device.
- A switch can use Full- Duplex.
- Multiple Collision Domains.
- Save Bandwidth in comparison of Bridge.
- Increased security.

Router-

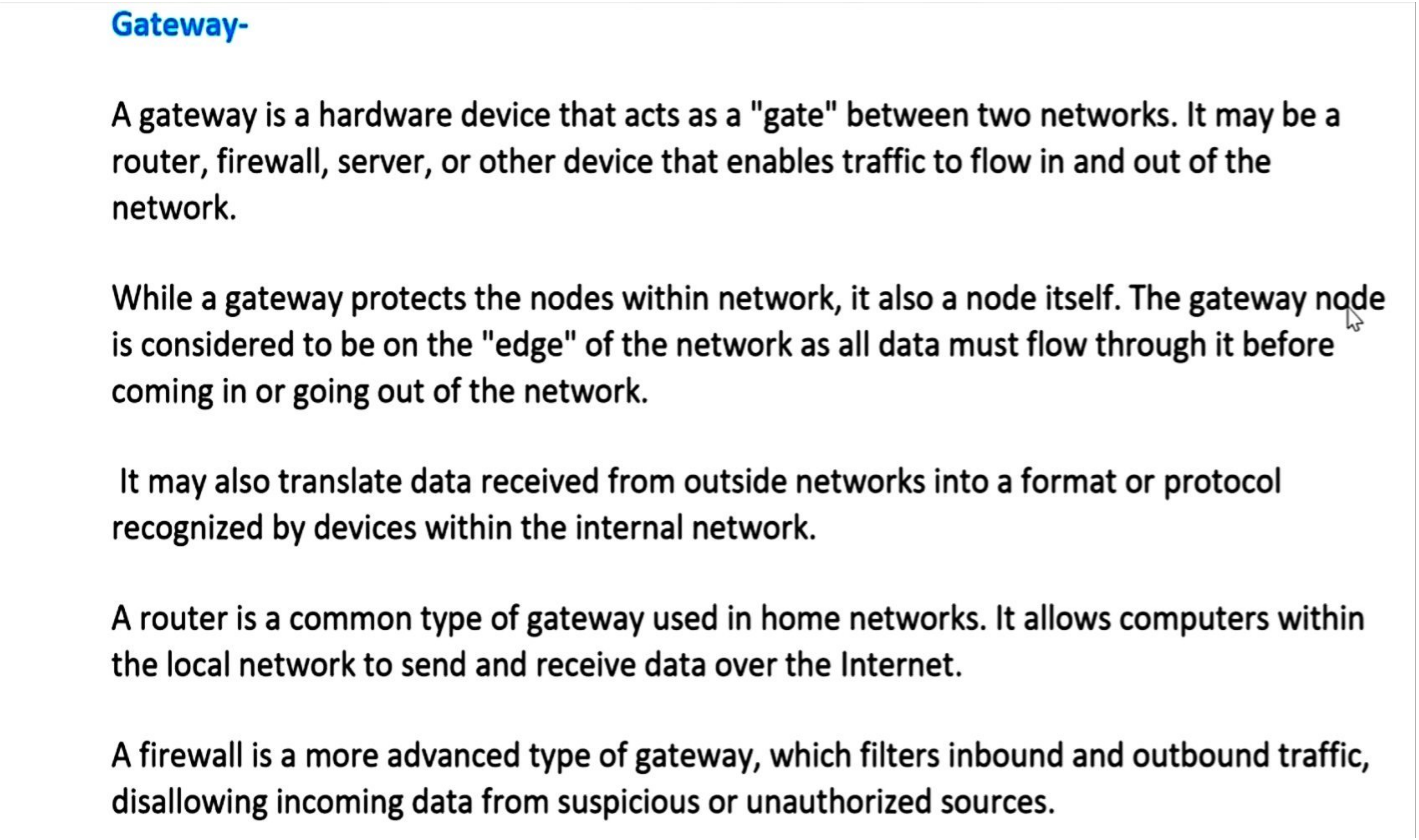


This is a hardware device that routes data (hence the name) from a local area network (LAN) to another network connection. A router acts like a coin sorting machine, allowing only



authorized machines to connect to other computer systems. Most routers also keep log files about the local network activity.

- A router used to connect two network, Internal and external networks.
- Layer 3 device.
- Few ports in compare of witch.
- More security we can define by using it to secure our network.



Gateway-

A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.

While a gateway protects the nodes within network, it also a node itself. The gateway node is considered to be on the "edge" of the network as all data must flow through it before coming in or going out of the network.

It may also translate data received from outside networks into a format or protocol recognized by devices within the internal network.

A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet.

A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources.

A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources.

A proxy server is another type of gateway that uses a combination of hardware and software to filter traffic between two networks. For example, a proxy server may only allow local computers to access a list of authorized websites.

Access point-

An access point is a device, such as a wireless router, that allows wireless devices to connect to a network. Most access points have built-in routers, while others must be connected to a router in order to provide network access. In either case, access points are typically hardwired to other devices, such as network switches or broadband modems.

Access points can be found in many places, including houses, businesses, and public locations. In most houses, the access point is a wireless router, which is connected to a DSL or cable modem. However, some modems may include wireless capabilities, making the modem itself the access point.

Large businesses often provide several access points, which allows employees to wirelessly connect to a central network from a wide range of locations. Public access points can be found in stores, coffee shops, restaurants, libraries, and other locations. Some cities provide public access points in the form of wireless transmitters that are connected to streetlights, signs, and other public objects.

While access points typically provide wireless access to the Internet, some are intended only to provide access to a closed network. For example, a business may provide secure access points to its employees so they can wirelessly access files from a network server.

Also, most access points provide Wi-Fi access, but it is possible for an access point to refer to a Bluetooth device or other type of wireless connection. However, the purpose of most access points is to provide Internet access to connected users.

The term "access point" is often used synonymously with base station, though base stations are technically only Wi-Fi devices. It may also be abbreviated AP or WAP (for wireless access point). However, WAP is not as commonly used as AP since WAP is the standard acronym for Wireless Access Protocol.

Firewall-

A physical firewall is a wall made of brick, steel, or other inflammable material that prevents the spread of a fire in a building. In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet. However, a computer firewall is more of a filter than a wall, allowing trusted data to flow through it.

A firewall can be created using either hardware or software. Many businesses and organizations protect their internal networks using hardware firewalls. A single or double firewall may be used to create a demilitarized zone (DMZ), which prevents untrusted data from ever reaching the LAN.