Network hardware

In order for a computer to operate on a network, there are ranges of different hardware components that are required.  Local area networks, need Ethernet cables/ Land Cable to connect devices to each other.

Network hardware can be categorized into two types

* LAN
* Internet

LAN Supporting Hardware

Switches

A switch, like a hub, is a device that connects a number of computers together to make a LAN.

The typical use of a switch is at the centre of a star network (or as part of a hybrid network) - the switch has cables plugged into it from each computer.

A switch is a more ‘intelligent’ device than a hub: if it receives a message, it checks who it is addressed to, and only sends it to that specific computer. Because of this, networks that use switches are more secure than those that use hubs, but also a little more expensive.

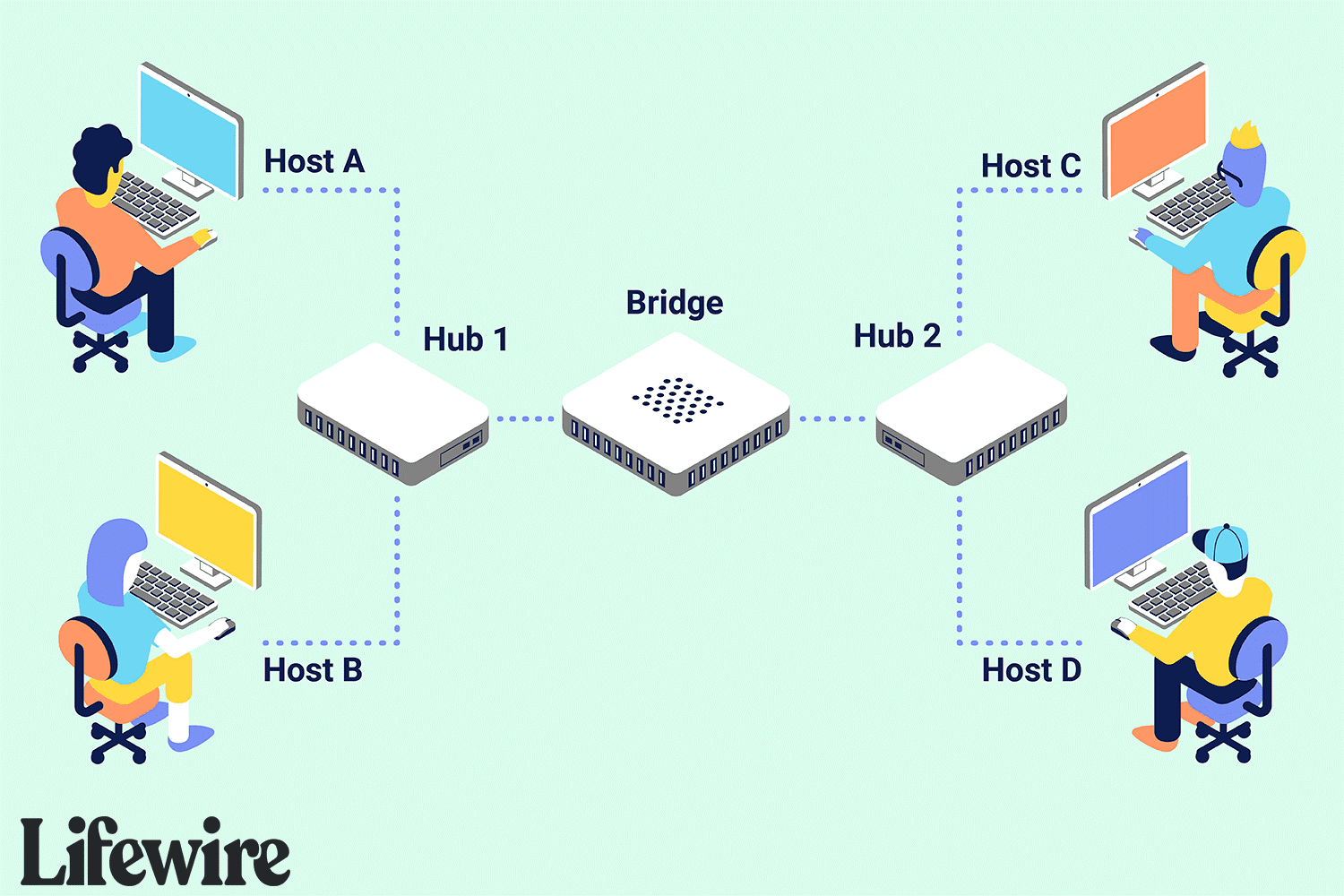
NIC Network interface card (NIC)

NICs enable desktop and laptop computers to connect to a network. NICs are small circuit boards that connect to the motherboard of the device. Smartphones also use a GSM chip to connect to the telephone network. Games consoles contain a NIC card so users can access the internet, download games and play online. It is usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage.

Some computers, such as laptops, have two NICs: one for wired connections, and one for wireless connections (which uses radio signals instead of wires)

* **Wireless Network Interface Card (WNIC):** are the same as the more ordinary NICs, in that they are used to connect devices to the internet or other networks. They use an antenna to communicate with networks via microwaves and normally simply plug into a USB port or can be internal integrated circuit plug in.
* Wireless Access Points (WAP):

Allows devices to connect to the LAN via WiFi (wireless radio communication) instead of using a cable, usually built into router

Bridge

A network bridge, also known as a layer 2 switch, is a hardware device used to create a connection between two separate computer networks or to divide one network into two using the same protocol (connection rules).

Repeater

Network repeaters (also called signal boosters and range extenders) are small devices that receive incoming electrical, wireless, and optical signals and retransmit them to spots that Ethernet and Wi-Fi data transmissions can't reach. They amplify signals on both analogue (copper cable) and digital (fibre optic cable) communication links.

Repeaters can also be used on wireless systems. These are used to boost signals to prevent any ‘dead spots’ in the Wi-Fi zone. These devices plug into electric wall sockets and send out booster signals. They are termed non-logical devices because they will boost all signals which have been detected; they are not selective.

Sometimes, hubs contain repeaters and are known as repeating hubs. All signals fed to the hub are boosted before being sent to all devices in the network, thus increasing the operational range.

There are two main drawbacks of repeating hubs:

* They have only one collision domain. When the signals are boosted and then broadcast to devices, any collisions which might occur are not resolved there and then. One way to deal with this problem is to make use of jamming signals – while this manages the collisions, it also reduces network performance since it involves repeated broadcasts as the collisions are resolved.
* The devices are referred to as unmanaged since they are unable to manage delivery paths and also security in the network.

A repeater operates at the physical layer and is a 2-port device

Router

A Router is a device that transfers data from one network to another in an intelligent way. It can be wireless or cabled. It has the task of forwarding data packets to their destination by the most efficient route. In order to do this, the router has a microcomputer inside it.

The router holds a table in memory that contains a list of all the networks it is connected to, along with the latest information on how busy each path in the network is. This is called the 'routing table'. They have the ability to search routing tables and find the shortest path to the destination.

The router inspects the data package sent to it from any computer on any of the networks connected to it. Since every computer on the same network has the same part of an internet protocol (IP) address, the router is able to send the data packet to the appropriate switch and it will then be delivered using the MAC destination address. If the MAC address doesn’t match any device on the network, it passes on to another switch on the same network until the appropriate device is found. Routers can be wired or wireless devices.

Here's how a router works:

* When a router receives a packet and sees a MAC address (hardware address) that is not on the local segment(network), it discards the MAC address, then looks at the IP address (software address).
* It then searches its routing table, and then sends the packet based on the IP address to the fastest and least congested path, to the router that's connected to the segment that contains that address.

**Gateways**

A gateway is a combination of hardware and software that acts as a "gate" between two networks. It connects two networks that use different protocols.

Where two networks use different protocols, packets must be modified so as to conform to both protocols. The gateway does this modification by transforming the packets by giving it a new sender and receiver address which follows the new protocol but at the same time leaving its contents intact.

The router and the gateway have similar functions in that they regulate network traffic between two or more separate networks, however, Gateways regulate traffic between two dissimilar networks, while routers regulate traffic between similar networks.

Examples of a gateway on an e-mail system allows different e-mail systems to exchange data.

Difference between a gateway and router

A white rectangular box with black text

Description automatically generated

What is an Internet server?

Internet server (web server) - this is a special computer, which is constantly switched on and connected to the Internet so that each Internet user around the world can access your website at all times. This computer is built up with selected high-quality components, which can endure incessant work and high load.

Types of servers

Proxy Server:

Proxy server is an intermediary server between client and the internet. Proxy servers offers the following basic functionalities:

* Firewall and network data filtering.
* Network connection sharing
* Data caching

Purpose of Proxy Servers

* Monitoring and Filtering such as content filtering, filtering encrypted data, bypass filters, logging and eavesdropping.
* Improving performance. It gives quick service by retrieving contents/information from cache.
* Translation; It helps to customize the source site for local users by excluding source content or substituting source content with original local content. In this the traffic from the global users is routed to the source website through Translation proxy
* Accessing services anonymously: The destination server receives the request from the proxy server (anonymously) and thus does not receive information about the end user
* Security: It hides the identity of the user therefore it protects the user network from spam and the hacker attacks.

Chat Server: It serves the users to exchange data in real time e.g WeChat servers.

* FTP Server: It works on one of the oldest of the Internet services, the file transfer protocol. It provides a secure file transfer between computers while ensuring file security and transfer control.
* Mail Server: It transfers and stores mails over corporate networks through LANs, WANs and across the Internet.
* Web Server: It provides static content to a web browser by loading a file from a disk and transferring it across the network to the user's web browser. This exchange is intermediated by the browser and the server, communicating using HTTP.

**Firewall**

A firewall is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer. Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

It monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

**Ethernet**

Ethernet is a protocol used by many wired LANs. It was adopted as a standard by the Institute of Electrical and Electronic Engineers (IEEE) and Ethernet is also known as IEEE 802.3. A network using Ethernet is made up of

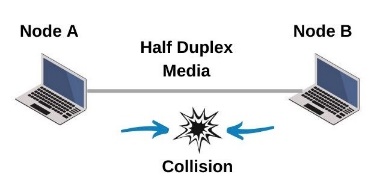
* a node (any device on the LAN)
* medium (path used by the LAN devices, such as an Ethernet cable)
* frame (data is transmitted in frames which are made up of source address and destination address – the addresses are often the MAC address).

When using Ethernet, it is possible for IP addresses to conflict;

* when two devices on the same network have been assigned the same IP address. This can lead to communication problems as network devices use IP addresses to identify and communicate with each other.
* Every network interface card (NIC) has a unique identifier called a MAC address. If two devices on a network have the same MAC address, it can lead to network issues.

**What is Collision?**

Collision, a condition that occurs when two or more computers on a network try to transmit signals at the same time on the shared media. Handling collisions is one of the main functions of a networking access method. In Ethernet standard there is a mechanism that is used to control shared bandwidth and prevent sending data at the same time on a shared media. This mechanism is called “collision”.



## To prevent collision on a network the CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is used

How Collision Works

## Device A and Device B both want to send data onto the network segment at the same time.

## As the devices transmit their data, they listen for any signs of interference or collision on the network. This is done using a technology called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

## If both devices detect that the network is busy (i.e., there's an ongoing transmission), they will wait for a random amount of time before trying to retransmit their data.

## After the random backoff time, Device A and Device B will try to transmit again. If the collision persists, the process repeats until a successful transmission occurs.

## Collision Detection (CSMA/CD)

## CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. It's a set of rules used in Ethernet networks to manage access to the shared communication medium (like a coaxial cable) and to handle collisions if they occur.

## The Process Before a device on the network sends data, it first listens to the network to determine if it's currently in use. It does this by checking for the presence of a carrier signal, which indicates that another device is transmitting data. If the device senses a carrier signal (meaning the network is busy), it will wait until the line is clear before attempting to transmit.

## In Ethernet networks that use CSMA/CD, multiple devices share the same physical communication medium, such as a coaxial cable or a hub-based network. Devices on the network compete for access to this shared medium. They need to take turns sending data to avoid collisions. In a shared medium, there's a possibility that two devices may try to transmit data at the same time. If this happens, a collision occurs. While a device is transmitting data, it continues to listen to the network. If it detects any interference or collision (i.e., it hears its own transmitted signal mixed with another device's signal), it realizes a collision has occurred. The devices involved in the collision stop transmitting at once. They then start a backoff algorithm to decide when to retransmit. After a collision, the devices wait for a random amount of time before trying to retransmit. This helps to avoid repeated collisions. After the backoff period, the devices will try to transmit again. If the network is clear, the transmission should be successful.

## Bit Streaming

## A bit stream is a continuous flow of bits over a network that requires a high speed data communication link (such as fast broadband). This path can be within the computer itself, across computer networks from a source computer (usually some sort of server) to a destination computer.

## Since bit streaming often involves very large files (such as video) it is necessary for the files to undergo some data compression before transmission. It is also necessary to have some form of buffering to ensure smooth playback of the media files.

## Two types of bit-streaming

## Real time bit streaming

## On demand

## Real time

## Real time bit streaming is where data is retrieved live from the source as it is being created. Real time streaming cannot be paused or re-winded, as any data that is not immediately used (e.g video data output to the screen) is discarded.

## Features:

## Low latency(delay) is prioritised over quality – packets that don’t arrive in time are discarded.

## If the data cannot be reliably streamed at the current bit-rate(quality) then a lower bit-rate and quality will be used.

## Used for:

## Live sports television broadcasts

## Online Gaming

## Some financial data

## Some weather data

## Live streaming services (e.g Twitch)

## Controlling UAVs and other autonomous devices.

## On demand

## On demand bit streaming is used to transmit data that has been pre-recorded. The player buffers (waits and saves up packets) until the data can be streamed in the bit-rate selected before starting playback

## Features:

## Data integrity is prioritised over latency.

## If there is insufficient bandwidth to handle the bit stream then buffering will occur and the output will pause or drop frames until the bandwidth increases or a lower bit rate stream is selected.

## Used for:

## Movie playback

## Music streaming (not live radio)

## Video streaming sites such as YouTube

## Sequence of digital signals (bits) transferred over a communication path at high speeds. It requires a fast broadband connection and some form of buffers (short-term memory)

## Bits arrive in the same order they are sent

## Bit rate: number of bits transmitted per second

## How On Demand Bit Streaming Works?

**Step 1 – Connect to the server:** Your computer connects you to the media server (whichever CDN server is best)

**Step 2 – Choose appropriate video file:** The Media Server tests your connection and chooses the appropriate video file from the selection it has available – this can include different formats, video resolution and video bitrate.

**Step 3 – Start sending bits:** The media server starts sending a stream of bits from the server to your computer

**Step 4 – Fill the buffer to above the minimum mark:** Your computer begins to fill it’s streaming buffer (usually stored in RAM) until amount of bits exceeds the minimum required amount.

**Step 5 – Start playing the video:** At this point the computer begins playing the video to the user, removing the played bits of data from the RAM as it does so.

**Step 6 – If the high-water mark is reached:** If the buffer is filled up to above the high level, then a control signal is sent to the media server asking it to pause sending data for a short while.

**Step 7 – If the stream buffer is completely emptied:** if the stream buffer empties the computer will pause the playback until the low-level mark is reached again. If this keeps happening the computer will send a control signal asking for the media server to send a lower resolution/quality stream.

**Comparison between Real time and on demand**

|  |  |
| --- | --- |
| **Real-time** | **On-Demand** |
| Event captured live via video camera that is connected to a computer | Existing digital files converted to encoded bit-streaming format for broadcasting on the internet by uploading to a dedicated server |
| Video signal converted to an encoded streaming video signal | A link for encoded video is placed on website and the user clicks on link to view encoded streaming video |
| Encoded video signal uploaded from computer to a dedicated streaming server via cables or high-speed wireless internet connection | The data is streamed to a buffer in user’s computer and the buffer stops the video from being paused as the bits are streamed |
| Server then sends live images to all users requesting it as a real-time video | As the buffer is emptied, it’s filled again thus providing continuous viewing |
| Cannot be paused, fast-forwarded, etc. | Can be paused, fast-forwarded, etc. |