Common Network Connectivity Devices

Network Interface Card

Today, it is almost impossible or at least very rare that a computer without **network interface card (NIC)** hardware can connect over a network. NIC is a circuit board that is installed in a computer to provide a dedicated network connection to the computer. It is also called **network interface controller, network adapter**, or **LAN adapter**. It provides the **physical**, **electrical**, and **electronic connections** to the network media. The NIC is called a **Layer 2** device because the information it uses for communication, the **MAC address**, resides on the **Data Link layer**. A NIC either is an expansion card or is built right into the computer's motherboard. Today, almost all NICs are built into the computer motherboard, providing 10, 100, and 1000 megabits per second (Mbps), but there was a time when all NICs were expansion cards that plugged into motherboard expansion slots. In some notebook computers, NIC adapters can be connected to the USB port or through a PC card slot.

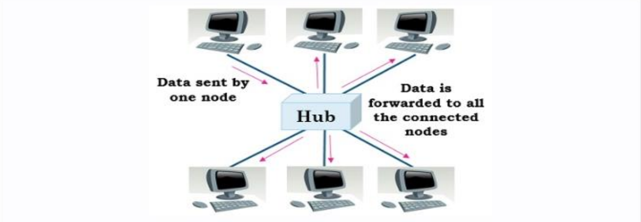
> Q: What is NIC?
> A: NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.
>
> - Interview Q&A

Hub

Hub is an elementary networking device, as it provides very simple functionality of establishing a connection between several devices. It does not have **segmentation capability**. Additionally, the device serves as the connector of the different LAN segments. It is generally used in an Ethernet environment with physical star/logical bus topology. The devices are connected to the hub with the help of twisted-pair cables. The chief purpose of the hub is to transfer the data packets to each device connecting it. Hubs are essentially repeaters, operating on bits. They are thus **physical-layer** devices.

A hub

Hub does not perform any filtration which means that each chunk of data is transmitted to all the connected end devices even if it is not a destined device. That is the reason it is said to be an unintelligent device. The hub works in the single collision domain, in other words, they are based on the *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) standard.*



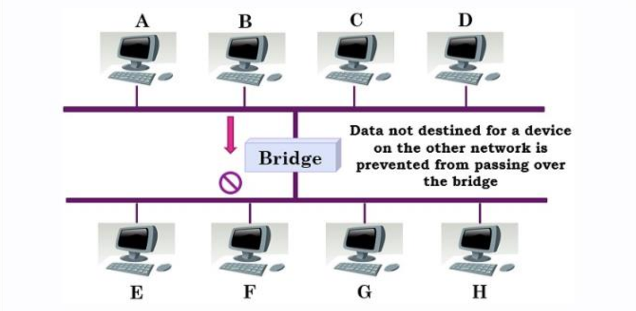
A single collision domain

Today, hubs are considered obsolete and **switches** are commonly used instead. Hubs have numerous disadvantages. They are not aware of the traffic that passes through them. They create only one large collision domain. A hub typically operates in half-duplex. There is also a **security issue** with hubs since the traffic is forwarded to all ports (except the source port), which makes it possible to capture all traffic on a network with a network sniffer!

Tip:
- Hubs are sometimes called multiport repeaters.

Bridge

The bridge is also a networking device that connects two different LAN operating on the same protocol. Furthermore, it is used for *splitting* the larger LAN into smaller networks. The bridge allows the traffic to pass through only if the transmission is sent to a station on the opposite side. When a bridge receives a frame from the network it retrieves the destination address from its header and checks it in a table to find the location where to send the frame. Unlike a hub, the bridge splits the network into LANs which have their own **distinct collision domains**. In contrast to hubs, which are physical-level devices, bridges operate on Ethernet frames (MAC addresses) and thus are **layer-2 devices**.

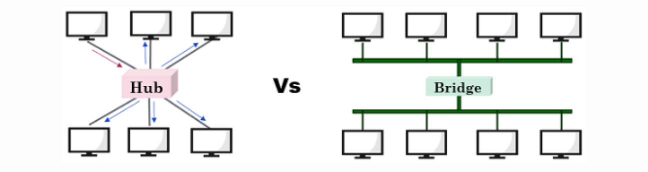

A
B
C
D
Bridge
Data not destined for a device on the other network is prevented from passing over the bridge
E
F
G
H

A network with a bridge

As stated before, a bridge can also split larger networks into smaller networks, but how does it do it? The bridge is placed between two physical network segments and it monitors the flow of data between the two segments. Here the **MAC address** plays an important role in deciding whether the data should be forwarded or discarded based on the condition.

Earlier bridges employ the manual creation of the MAC address list while in modern bridges this task is done automatically by watching the traffic on the network, these bridges are known as **self-learning bridges**. A self-learning bridge builds its table automatically, dynamically and autonomously – without any intervention from a network administrator or from a configuration protocol. They are outdated now and switches are preferred to bridges.

Hub vs. Bridge



Hub vs. Bridge

The crucial difference between the hub and bridge is that the **hub** works on the **physical layer**, but the **bridge** operates on the **data link layer** of the OSI model. Both hub and bridge serve a different purpose. A hub transmits the data to each device connected to it, it broadcasts the data. On the other hand, a bridge is more intelligent which checks and filter data before forwarding it, this mechanism significantly *reduce the network traffic and improve security.* Hub connects two LAN segments whereas the bridge can connect two different LANs.

	HUB	BRIDGE
Basics	Used to connect a number of devices.	Facilitates in the segmentation of the larger network.
Data filtration	Not performed	Conducted
Uses	Multiple ports	Single incoming and outgoing port
Links	Segments of LAN	Two different LANs employing the same protocol.

Switch

Like hubs, a switch is used to connect multiple hosts together, but it has many advantages over a hub. A switch is an **OSI Layer 2** device, which means that it can inspect received traffic and make forwarding decisions. Each port on a switch is a separate collision domain and can run in a full-duplex mode.

A network switch

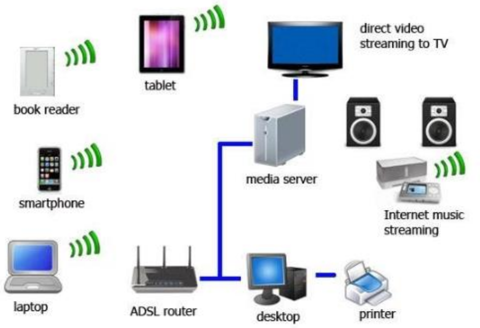
The Ethernet switch has become an integral part of the world's LAN infrastructure. Before switches, hubs received Ethernet frames and forwarded them to every connected device. There was no **privacy** or **security** and **performance** was poor. What the network needed was a more logical device that could make decisions for where to send data and block the traffic flow to irrelevant devices. The switch accomplishes these requirements by executing four basic functions: **Learning, Forwarding, Filtering**, and **Flooding**. These functions are present in a switch by default, right out of the box. No configuration is necessary.

> Q: What is the difference between a hub and a switch?
> A: A hub acts as a multiport repeater. However, as more and more devices connect to it, it would not be able to efficiently manage the volume of traffic that passes through it. A switch provides a better alternative that can improve the performance especially when high traffic volume is expected across all ports.
>
> - Interview Q&A

Router

A **router** is a network device used to connect many, sometimes disparate, network segments together, combining them into what we call an internetwork. A well-configured router can make intelligent decisions about the best way to get network data to its destination. It gathers the information it needs to make these decisions based on a network's particular performance data. As routers use IP addresses to make forwarding decisions, they are considered **Layer 3** devices.

The below figure shows a *small office, home office (SOHO)* router that provides wired and wireless access for hosts and connects them to the Internet without any necessary configuration.



The advantage of a router to a switch is that a router interface should create and maintain broadcast domains and connectivity of WAN services. Router interfaces must be configured and enabled in order to use them effectively.

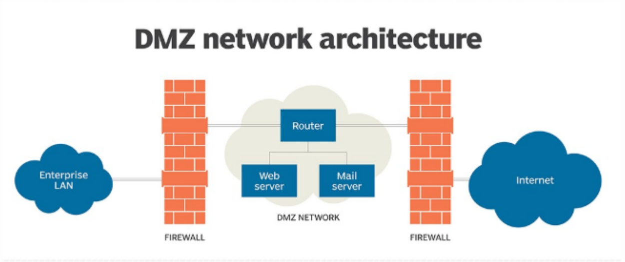
Routers can be multifaceted devices that behave like computers unto themselves with their own complex operating systems—for example, Cisco's IOS. You can even think of them as CPUs that are totally dedicated to the process of routing packets. And due to their complexity and flexibility, you can configure them to actually perform the functions of other types of network devices (like firewalls, for example) by simply implementing a specific feature within the router's software.

Note: Routers can have many different names: **Layer 3 switch** and **multilayer switch** are the most common, besides the name router, of course. Remember, if you hear just the word **switch**, that means a **Layer 2** device. **Routers, Layer 3 switches**, and **multilayer switches** are all **Layer 3** devices.

Firewall

For networks, security is crucial! A **firewall** protects your LAN resources from invaders that prowl the Internet for unprotected networks while simultaneously preventing all or some of your LAN's computers from accessing certain services on the Internet. You can employ them to filter packets based on rules that you or the network administrator create and configure to strictly delimit the type of information allowed to flow in and out of the network's Internet connection. Firewalls operate at *multiple layers of the OSI model*. Some firewalls can operate up to the *Application layer*.

A firewall can be either a stand-alone "*black box*" or a *software* implementation placed on a server or router. Either way, the firewall will have at least two network connections: *one to the Internet* (known as the public side) and *one to the network* (known as the private side). Sometimes, there is a second firewall, as shown in the below figure. This firewall is used to connect servers and equipment that can be considered both *public and private* (like web and email servers). This intermediary network is known as a **demilitarized zone (DMZ)**.

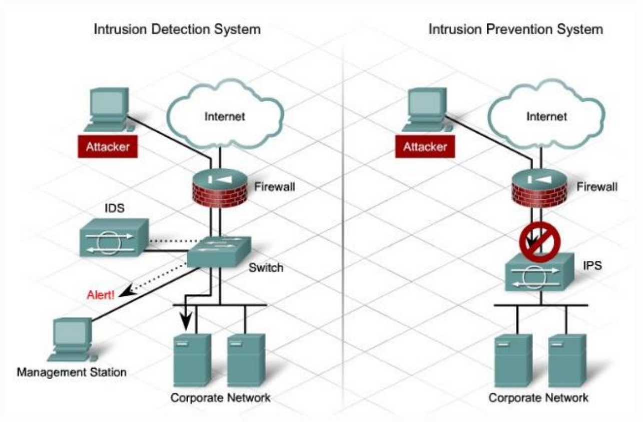


Firewalls are the first line of defense for an Internet-connected network. Without them in place, any network that's connected to the Internet is essentially wide open to anyone with a little technical savvy who seeks to exploit LAN resources and/or access your network's sensitive information.

> Q: Explain what is a firewall?
> A: A firewall is a network security system which is used to monitor and control the network traffic based on some predefined rules. Firewalls are the first line of defense and establish barriers between the internal and external networks in order to avoid attack from untrusted external networks. Firewalls can be either hardware, software or sometimes both.
>
> - Interview Q&A

IDS/IPS

Intrusion detection systems (IDSs) and **intrusion prevention systems (IPSs)** are very important in today's networks. They are network security appliances that monitor networks and packets for malicious activity. An **IDS** is considered *monitor mode* and just records and tells you about problems, whereas an **IPS** can work in real-time to *stop threats* as they occur. The main difference between them is that an IPS works inline to actively prevent and block intrusions that are detected based on the rules you set up. IPSs can send an *alarm, create correlation rules and remediation, drop malicious packets, provide malware protection*, and *reset the connection* of offending source hosts.



IDS and IPS

Other Specialized Devices

Multilayer Switch

A **multilayer switch (MLS)** is a computer networking device that switches on *Open Systems Interconnection (OSI) Layer 2* like an ordinary network *switch* but provides *routing*. A *24-port MLS* gives you the best of both worlds. It operates at *Layer 3 (routing)* while still providing *24 collision domains*, which a router could not do. The major difference between the packet switching operation of a router and that of a Layer 3 or multilayer switch lies in the physical implementation. In routers, packet switching takes place using a microprocessor, whereas a Layer 3 switch handles this by using application-specific integrated circuit (ASIC) hardware.

Layer 3 switches look just like regular Layer 2 switches. The differences are the hardware inside and the operating system.

Why Use a Multilayer Switch?

- Easy for use – Multilayer switches are configured automatically and its Layer 3 flow cache is set up autonomously. And there is no need for you to learn new IP switching technologies for its “plug-and-play” design.
- Faster connectivity – With multilayer switches, you gain the benefits of both switching and routing on the same platform. Therefore, it can meet the higher-performance need for the connectivity of intranets and multimedia applications.

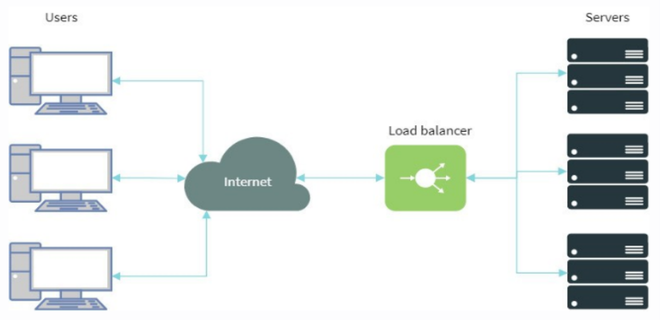
Load Balancer

An average router just sends incoming packets to their specified, correlative IP address on the network, but a **load balancer** can actually send incoming packets to multiple machines hidden behind one IP address.

A **load balancer** acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

In this manner, a load balancer performs the following functions:

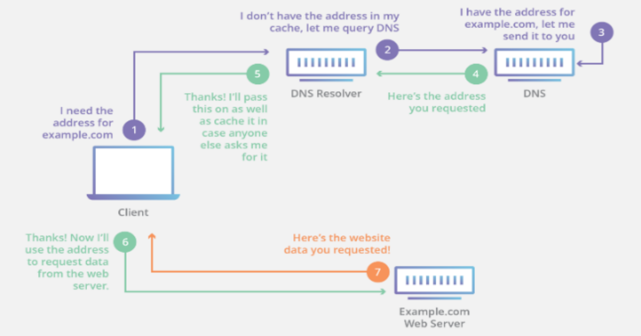
- Distributes client requests or network load *efficiently* across multiple servers
- Ensures high *availability* and *reliability* by sending requests only to servers that are online
- Provides the flexibility to *add* or *remove* servers as needed



Load balancer

Domain Name Service (DNS) Server

Domain Name Service (DNS) is a network protocol that we use to find the IP addresses of hostnames. Computers use IP addresses but for us humans, it’s more convenient to use domain names and hostnames instead of IP addresses. If you want, you could visit *www.clarusway.com* by going directly to IP address 54.164.151.235, but typing in the domain name www.clarusway.com is probably easier.


I don’t have the address in my cache, let me query DNS
I have the address for example.com, let me send it to you
3
2
5
4
DNS Resolver
DNS
Thanks! I’ll pass this on as well as cache it in case anyone else asks me for it
Here’s the address you requested
I need the address for example.com
1
Client
Thanks! Now I’ll use the address to request data from the web server.
6
Here’s the website data you requested!
7
Example.com Web Server

DNS query

DNS is distributed and hierarchical, there are thousands of DNS servers, but none of them has a complete database with all hostnames/domain names and IP addresses. A DNS server might have information for certain domains but might have to query other DNS servers if it doesn’t have an answer.

The process of finding the IP address for any given hostname is known as **name resolution**, and it can be performed in several ways: a HOSTS file (meaning you statically type in all names and IP addresses on each and every host), a request broadcast on the local network, DNS, and Microsoft’s Windows Internet Naming Service (WINS).

On the Internet, domains are arranged in a hierarchical tree structure. The following list includes some of the top-level domains currently in use:

- **.com** A commercial organization. Most companies end up as part of this domain.
- **.edu** An educational establishment, such as a university.
- **.gov** A branch of the U.S. government.
- **.int** An international organization, such as NATO or the United Nations.
- **.mil** A branch of the U.S. military.
- **.net** A network organization.
- **.org** A nonprofit organization.

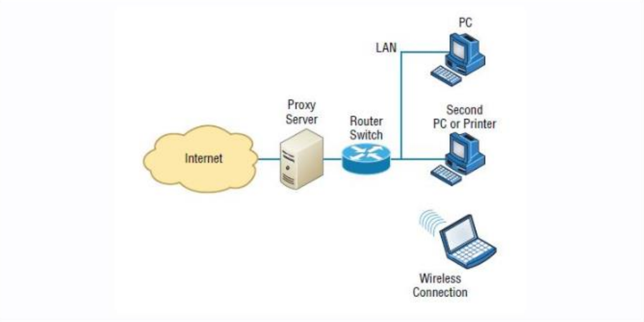
In other parts of the world, the final part of a domain name represents the country in which the server is located (.ca for Canada, .jp for Japan, .uk for Great Britain, and .ru for Russia, for example). Over 130 countries are represented on the Internet.

Proxy Server

A **proxy server** is basically a type of server that handles its client-machine requests by forwarding them on to other servers while allowing granular control over the traffic between the local LAN and the Internet. When it receives a request, the proxy will then connect to the specific server that can fulfill the request for the client that wants it. A proxy server operates at the **Application layer**.

Sometimes the proxy modifies the client’s request or a server’s response to it—or even handles the client’s request itself. It will cache, or “remember,” the specific server that would have normally been contacted for the request in case it’s needed another time. This behavior speeds up the network’s function, thereby optimizing its performance. However, proxy servers can also limit the availability of the types of sites that users on a LAN have access to, which is a benefit for an administrator of the network if users are constantly connected to non-work sites and using all the WAN bandwidth.

The below figure shows where a proxy server would be typically found in a small-to-medium network.



Proxy server

There are also some customized proxy servers for specific purposes. A **web proxy server** is used to maintain web cache to remember visited sites, user data, etc. on the web. On the other hand, a **caching proxy server** locally caches the user requests and use them to speed up the network’s service requests.

Encryption Devices

Encryption allows you to create secure connections over insecure channels. Encrypting your network traffic provides you privacy and authentication.

There are dedicated appliances that can perform encryption as well. The advantage of using these devices is that they normally provide more choice of encryption methods and stronger encryption options. They also offload the process from other devices like routers and servers, which is a good thing since the encryption/decryption process is very processor-intensive and interferes with other functions that those routers and servers might be performing.

Sometimes these devices are called **encryption gateways**. They can either sit in line with a server or a local network, encrypting and decrypting all traffic or function as an application server, encrypting any file sent to them within a network.

An encryption device

While an encryption appliance is dedicated to encryption, a **content filtering appliance** scans the content of what goes through it and filters out specific content or content types. Servers or routers could also do this but the cost is great as this task *slows down* these devices. So a dedicated device takes over this burden from servers or routers and relieves them from this duty. Also, there is usually more functionality and granular control available with a dedicated appliance.

Email is a good example of what you might run through one of these devices to filter out spam and objectionable content before the email is delivered. Another example of the use of a content filter might be to block websites based on the content of the web pages rather than on the basis of the URL or IP address.

A content filtering hardware

Packet Shaper

Packet shaping (also known as traffic shaping) is an Internetworking traffic management technique that delays some or all packets to bring them into compliance with your or your company's traffic profile.

A packet shaper

Traffic shaping is used for a number of purposes:

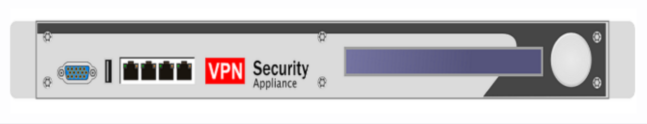
- Time-sensitive data may be given priority over traffic that can be delayed briefly with little-to-no ill effect.
- A large ISP (Internet service provider) may shape the traffic of an independent reseller.
- In a corporate environment, business-related traffic may be given priority over other traffic.
- An ISP may limit the bandwidth consumption for certain applications to reduce costs and create the capacity to take on additional subscribers. This practice can effectively limit a subscriber's "unlimited connection" and is often imposed without notification.
- Traffic shaping could be an integral component of the proposed two-tiered Internet, in which certain customers or services would get traffic priority for a premium charge.

VPN Concentrator

The VPN Concentrator is a networking device acting like a router that allows multiple VPN tunnels to function independently and connect to the network. It's built specifically for creating and managing VPN communication infrastructures.

Through the addition of advanced data packets, security protocols, and new algorithms, a router gets reused into the network device that manages large numbers of VPN tunnels (hundreds to thousands). This is what it's good for:

- Encryption and decryption of data
- Establish and configure VPN tunnels
- Authenticate users
- Assign IP addresses to each individual user on the network
- Ensure the end-to-end delivery of the data packets



A VPN concentrator