**Routers vs Switch**

**Router**: A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses and allowing multiple devices to use the same Internet connection.

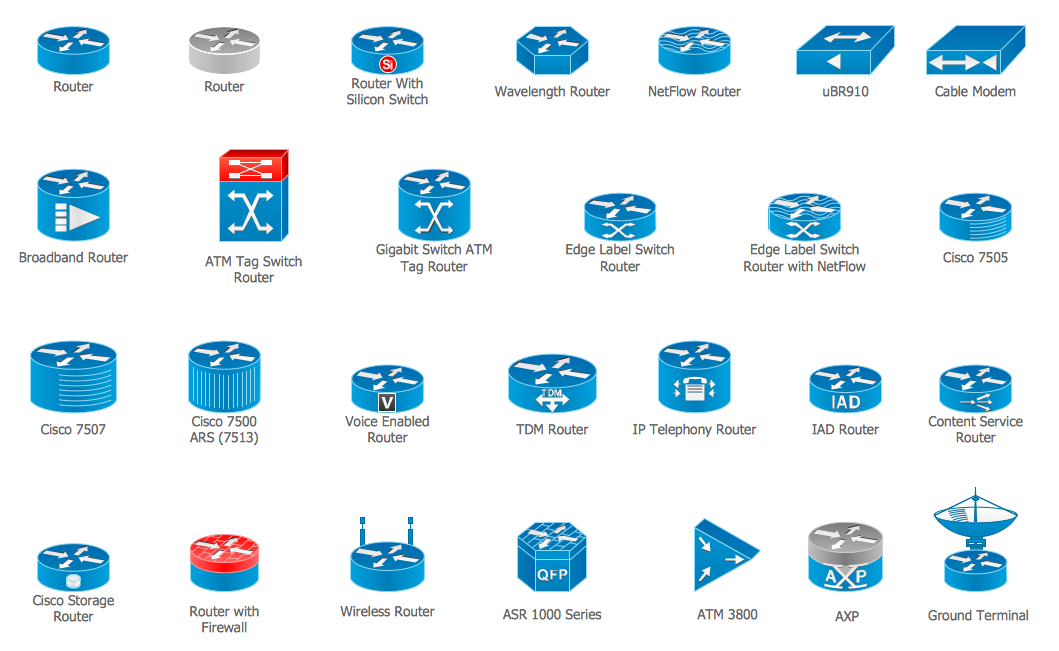
There are several types of routers, but most routers pass data between [LANs (local area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) and [WANs (wide area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

**What are some of the security challenges associated with routers?**

**Vulnerability exploits:** All hardware-based routers come with automatically installed software known as firmware that helps the router perform its functions. Like any other piece of software, router firmware often contains vulnerabilities that cyber attackers can exploit (one [example](https://threatpost.com/netgear-zero-day-takeover-routers/156744/)), and router vendors periodically issue updates to patch these vulnerabilities. For this reason, router firmware needs to be updated regularly. Unpatched routers can be compromised by attackers, enabling them to monitor traffic or use the router as part of a [botnet](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/).

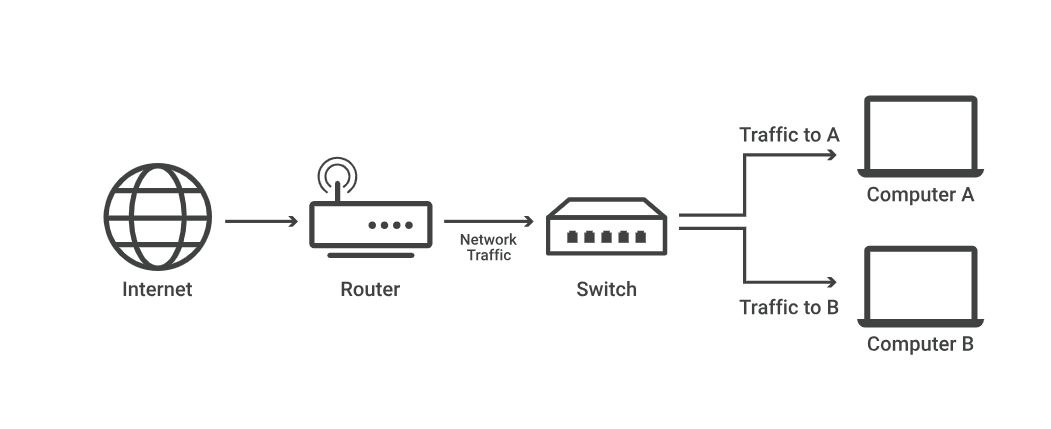
**DDoS attacks:** Small and large organizations often are the targets of distributed denial-of-service (DDoS) attacks directed at their network infrastructure. Unmitigated [network layer DDoS attacks](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) can overwhelm routers or cause them to crash, resulting in network downtime. [Cloudflare Magic Transit](https://www.cloudflare.com/magic-transit/) is one solution for protecting routers and networks from these kinds of DDoS attacks.

**Administrative credentials**: All routers come with a set of admin credentials for performing administrative functions. These credentials are set to default values, such as "admin" as the username and "admin" as the password. The username and password should be reset to something more secure as soon as possible: attackers are aware of the common default values for these credentials and can use them to gain control of the router remotely if they are not reset.



**Switch:**

A network switch connects devices within a network (often a [local area network, or LAN](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/)\*) and forwards [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to and from those devices. Unlike a [router](https://www.cloudflare.com/learning/network-layer/what-is-a-router/), a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

****

**What is a layer 2 switch? What is a layer 3 switch?**

Network switches can operate at either [OSI](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/) layer 2 (the data link layer) or [layer 3](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) (the [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/)). Layer 2 switches forward data based on the destination MAC address (see below for definition), while layer 3 switches forward data based on the destination [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/). Some switches can do both.

**What is a layer 2 switch? What is a layer 3 switch?**

Network switches can operate at either [OSI](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/) layer 2 (the data link layer) or [layer 3](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) (the [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/)). Layer 2 switches forward data based on the destination MAC address (see below for definition), while layer 3 switches forward data based on the destination [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/). Some switches can do both.

A diagram of a computer network

Description automatically generated

Network-based cyber attacks

Network-based attacks are attacks designed to compromise network security by either eavesdropping on or intercepting and manipulating network traffic. These may be active attacks, wherein the hacker manipulates network activity in real-time; or passive attacks, wherein the attacker sees network activity but does not attempt to modify it.

The more prevalent kinds of network attacks are:

Sniffing

A sniffing attack involves an attacker getting into the network data-stream and reading, monitoring or capturing full packets of data flowing between a client and a server. A hacker intercepting a network packet containing unencrypted information can cause severe damage to the organization or entity that owns the data. Data compromised may include sensitive information like account credentials, bank details, and different kinds of Personally Identifiable Information (PII).  Sniffing attacks can either be active (involving both data access and manipulation) or passive (where the attacker only sees the information but does not actively interfere in its transmission). Examples of tools used for sniffing attacks are Wireshark, tcpdump, dSniff and Debookee.

Eavesdropping

Eavesdropping attacks are similar to sniffing attacks, except that they are usually passive, easier to carry out and may not involve full packets of data. They involve an attacker listening to information flowing between networks to get private information, and often target one-on-one communication.  These, too, are difficult to detect. [Investopedia describes eavesdropping attacks](https://www.investopedia.com/terms/e/eavesdropping-attack.asp) as involving a weakened connection between client and server that allows the attacking entity to send network traffic to itself. “Any device in the network between the transmitting device and the receiving device is a point of weakness, as are the initial and terminal devices themselves”, it says. Tools used to carry out these attacks include Wireshark, tcpdump, and Ettercap.

Spoofing

Spoofing refers to a malicious actor pretending to be a legitimate entity or someone s/he is not. In the context of network security, it usually means “a [computer spoofing](https://www.forcepoint.com/cyber-edu/spoofing) an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server”.Attackers often gain access to otherwise off-limits networks that use IP addresses for user authentication by using IP address spoofing. They may also use what is known as ARP spoofing to link their own Media Access Control (MAC) to a legit IP address, thus gaining access to data meant for a different IP owner. DNS spoofing lets hackers divert traffic to an IP address other than where it was originally directed. Spoofing attacks are used more frequently (and successfully) on unprotected non-enterprise systems than on larger enterprise systems because the latter are usually equipped with better detection and mitigation tools.

Denial-of-Service

Denial-of-Service (DoS) attacks block or disrupt an organization or business’s ability to use its own resources such as network bandwidth, system resources (CPU, memory), and application resources (web server, DNS server). In a typical DoS attack, the perpetrator floods the target network with authentication requests or pings that have invalid return addresses, thus using up all the network’s resources and blocking its regular operations. Common DoS attacks include Ping attacks, Syn attacks, Flooding, and Reflection and Recursion. A Distributed Denial of Service (DDoS) attack is a more advanced form of a DoS attack where the target network is flooded by requests not from a single server or machine but from multiple attack points (sometimes to the tune of thousands).

DoS attacks can be mitigated using Firewall or Operating System rules, contacting upstream service providers to investigate the origin of the attack, backing up data from time to time to minimize damage from a potential attack, and good planning. Some organizations use a mitigation strategy known as “black hole routing” to defend against DoS attacks. The blackholing method detects and directs excessive traffic into a “black hole” or a null route, to keep the target network from crashing. However, because blackholing treats all kinds of network traffic – both malicious and legitimate – the same way, it should be used sparingly.

Network-based attacks – Defense and mitigation

The mitigation methods and tools to defend against network attacks fall into four main categories:

Management

**Manage patch application** – A good patch management policy will mandate regular tracking of patch releases for all software in use by an organization and implementation of patches as soon as they are released.

**Reduce attack surface**– Reducing the attack surface involves removing any unused or unnecessary applications and services from all computing devices in an organization. In his book [*Security Engineering: A Guide to Building Dependable Distributed Systems*](https://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523), Ross J. Anderson says, “There is usually no reason for every workstation in your company to be running a mail server, and ftp server and DNS, and stripping things down can greatly reduce the attack surface.”

**Segment the network** – Segmenting is one of the easiest ways for organizations to protect their networks. It refers to the practice of splitting a larger network into small sub-networks that are independent of one another. The biggest benefit of segmentation is the extra incident-response time it provides businesses when an attack occurs. Segmenting also makes it easier for organizations to keep their sensitive data relatively more secure, and limit access to critical data.

**Switch from default to secure configuration** – Enterprises must, as a rule, periodically monitor and change all installed software’s security settings to the most secure configuration possible. Often, new software continues to be used with default settings for long periods of time, leading to breaches that could easily have been prevented had someone bothered to change the settings.

Filtering

**Firewalls** – The most commonly used filtering tool to block network attacks is the firewall. The firewall acts as a filter between a local system and internet traffic that it detects to be malicious. Firewalls deal with bad network packets by (1) discarding them or modifying them to make them safe, or by (2) copying them to a log or audit trail. Firewalls or filters can act on three different levels: IP packets, the TCP session level, and the application level.

**Packet filtering** refers to a firewall inspecting packet addresses and port numbers to (for instance) make sure that traffic coming from IP addresses known to be “bad” is kept out, in addition to performing more routine firewalls tasks such as allowing traffic only to specific port numbers.

**TCP-level filtering** works by “reassembling and examining all the packets in each TCP session”. It can also be used for DNS filtering, in addition to providing Virtual Private Network (VPN) functionality for traffic encryption purposes.

**Application-level filtering** – Application-level filters function as proxies for one or more services and include things like email filters and web proxies. Using app-level filters comes with its own set of problems, however, one of which is the constant race between firewall manufacturers and hackers who are quick to find holes even in the latest filtering software.  These filters also tend to be expensive, particularly when used on high-bandwidth web content.

Intrusion detection

Intrusion Detection Systems (IDS) scan the network for signs of compromise or an ongoing attack (such as incoming spam, packets from forged IP addresses, or someone trying to make a connection with a botnet controller) and raise an alarm if any malicious activity is detected.

The most commonly used intrusion detection mechanism is monitoring and detecting when a threshold (such as number of failed logins) is crossed.

Other categories include:

**Misuse Detection systems t**hat look for a signature or defining characteristic of an attack.

**Anomaly Detection systems** that look for unusual changes in behavior patterns to detect uncatalogued attacks.

Encryption

Network encryption, or any kind of encryption for that matter, involves encoding data to hide it from anyone who is not authorized to see it. Encrypted data can be accessed or decrypted using a decryption key. Home networks are usually encrypted using WPA or WPA2 encryption algorithms, while web browsers use what is known as the Secure Sockets Layer (SSL) protocol. One often hears about how HTTPS is more secure than HTTP; this is because HTTPS uses an SSL certificate that encrypts all information being transmitted between the client and server. It also uses an additional security layer known as the Transport Layer Security (TLS) protocol.

A note on key length: As a general rule, the longer the decryption key, the more difficult it will be for a hacker to crack. As technology evolves, decryption keys get longer, 128-bit encryption being the current accepted standard.