What is a router? What does a router do on the network?

What is a router? A router is a network device that forwards data packets between computer networks. Understandably, routers direct traffic on the Internet.

Routers are an important piece of technology that most people have in their homes, but many people don't really understand them. Understanding network devices in general and routers in particular will give you many advantages. So what is the role of the router in the network? How do routers work? Join TipsMake to find the answer in the following article!

What is a router?

A router is a device that connects two or more packet-switched networks or subnets. It serves two main 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 transmit data between a LAN (local area network) and a WAN (wide area network). A LAN is a group of connected devices that are limited to a specific geographical area. LAN networks usually require a single router.

In contrast, a WAN is a large network spread over a large geographical area. For example, large organizations and companies operating in multiple locations across the country will need separate LANs for each location, which then connect to other LANs to form a WAN. Because WAN networks are distributed over a large area, many routers and switches are often needed.

Network switches forward data packets between groups of devices on the same network, while routers forward data between different networks.

Here, we will focus on common routers, familiar to everyone. If you want to know more about business routers, scroll down to the end of the article.

Router function

Simply put, **routers connect devices in a network by transferring data packets between them** . This data can be sent between devices or from devices to the Internet. Routers perform this task by assigning local IP addresses to each device on the network. This ensures that the data packet reaches the right place and is not lost in the network.

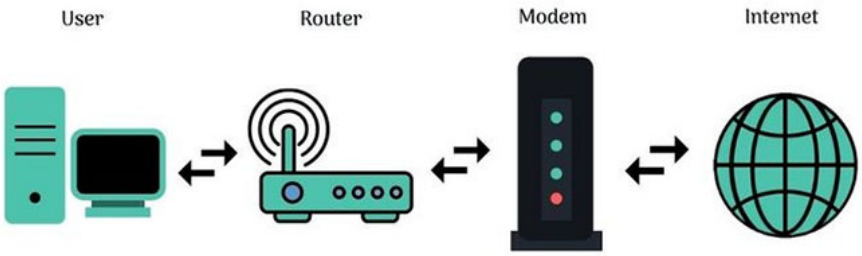
Think of this data as a courier package, it needs a delivery address so it can be sent to the correct recipient. A local computer network is like a suburban road, knowing only the location of the street name without knowing the specific house number in the big world (ie the World Wide Web) is not enough.

This package may be sent to the wrong address with limited information. Therefore, the router ensures that each location (device) has a unique number so that data packets are sent to the correct location. If you need to return data to the sender or send your own packets, the router also does this job. Although it processes each packet individually, it does this very quickly, even when multiple devices send data at the same time.

How is a router different from a modem?

Because modern modems are often equipped with integrated routers, the difference between modem and router is often not of much interest to many people. But anyone who remembers the early days of the Internet knows that they had distinct functions.

You need a modem to connect to the Internet through your ISP and use a router to connect many devices on the network - including the modem. Therefore, the router allows your modem and many devices to transmit data from one location to another. Modem is the path that transmits data to and from the Internet.



You need a modem because there are many different types of signals used by computers compared to the Internet in general. Computers and mobile devices use digital signals, while the Internet operates on analog signals.

The modem converts these signals to the correct format. This is why this device is called modem. Modem is a combination of the words **mo** dulator and **dem** odulator. You will usually receive a modem from your ISP when you sign up for an Internet package. Signal conversion is a specialized function of the modem, while coordinating the signals is the router's job.

Pictures of Routers

To better visualize, you can see the illustrations in Figures A and B. Figure A is the front of a TP-Link Archer C7 AC1750 broadband router, and Figure B is its back.

Figure A : Front view of TP-Link's Archer C7 AC1750 router

Figure B : The back of TP-Link's Archer C7 AC1750 router includes a set of RJ-45 ports like a hub or switch

Figure A is the front of the router, including the beacons, from left to right: power beacon, wifi beacon (2.4GHz), wifi beacon (5GHz), 4 Ethernet beacons, internet beacon, system beacon .

Looking at Figure B you will see there are three sets of ports on the back of the router. The leftmost port is where the power source is connected to the router. Blue RJ-45 port to plug in network cable from cable modem or DSL modem.

4 yellow RJ-45 ports are used to connect network cables to computers on the network, thereby providing network connections for them.

Router applications

Here are the important applications of routers:

1. Create .
2. Allows you to split your Internet connection to all devices.
3. Connect different media/devices together
4. Run .
5. Routers determine where information is sent from one computer to another
6. Packet filtering and forwarding.
7. The router also ensures that the information reaches its intended destination.
8. Connect to VPN

Advantages and disadvantages of routers

Advantage

1. Routers help share network connections with multiple computers, helping to increase work efficiency.
2. Routers allow data packets to be distributed in an organized way, helping to reduce data load.
3. Routers provide stable and reliable connections between network hosts.
4. Routers use replacement parts in case the main part fails to deliver data packets.

Defect

1. The connection may become slow when many computers are using the network. This situation is described as waiting for a connection.
2. Routers help multiple computers share the same network, which can reduce the speed of the network connection.

Types of routers

Core router

Core routers are typically used by service providers (i.e. AT&T, Verizon, Vodafone) or cloud providers (i.e. Google, Amazon, Microsoft). These companies provide maximum bandwidth for connecting additional routers or switches. Most small businesses will not need a core router. But very large businesses with many employees

working in different buildings or locations may use core routers as part of the network architecture.

Edge routers

Edge router, also known as gateway router or gateway, is the outermost connection point of the network to external networks, including the Internet.

Edge routers are optimized for bandwidth and designed to connect to other routers to distribute data to end users. Edge routers typically do not provide WiFi or full local network management capabilities. They usually only have Ethernet ports - one input to connect to the Internet and several outputs to connect additional routers.

Edge router and edge modem are interchangeable terms, although the word edge modem is no longer commonly used by manufacturers or IT professionals when referring to edge routers.

Distribution router

A distribution router, or interior router, receives data from the edge router (or gateway) via a wired connection and sends that data to the end user, usually via WiFi, although the router often includes physical connections as well. (Ethernet) to connect users or additional routers.

Wireless router (wireless router)

Wireless routers combine the functions of edge routers and distribution routers. These are popular routers for home networks and Internet access.

Most service providers offer full-featured wireless routers as standard equipment. But even if you have the option of using an ISP's wireless router in your small business, you may still want to use a business-class router to take advantage of better wireless performance, with more connection control features. more connected and secure.

Virtual router

A virtual router is software that allows some router functions to be virtualized in the cloud and delivered as a service. These routers are ideal for large businesses with complex network needs. They provide flexibility, easy scalability, and lower entry costs. Another benefit of virtual routers is that they reduce the workload of managing local network hardware.

Router routing process

To understand how routing is done, you must first know a little about how the TCP/IP protocol works.

Every device connected to a TCP/IP network has a unique IP address limited to its network interface. An IP address is a series of four unique numbers separated by dots. For example, a typical IP address has the form: 192.168.0.1.

The easiest example to understand when talking about IP is the home address. A normal home address always has a house number and street name. The house number determines the specific location of the house on that street. IP addresses work similarly. It includes the network address code and device code. Comparing with the

home address, you will see that the network address is like the street name and the device code is like the house number. The network address refers to the specific network the device is participating in, and the device ID provides the device with an identity on the network.

So where does the network address end and the device ID begin? This is the job of a subnet mask. The subnet mask will 'tell' the computer the last position of the network address and the first position of the device number in the IP address. Subnet operations can sometimes be very complicated. You can refer to more details in another article that we will introduce later. Now let's take care of the simplest things, consider a very basic subnet mask.

The subnet mask at first glance is very similar to the IP address because it also has 4 numbers in a format separated by dots. A typical subnet mask has the form: 255.255.255.0.

In this particular example, the first three numbers (called octets) are all 255, the last number is 0. The number 255 indicates that all the bits in the corresponding position of the IP address are part of the code. fate. The final 0 indicates that no bit in the corresponding position of the IP address is part of the network address. Therefore they belong to the device code.

It sounds quite confusing, you will understand better with the following example. Imagine you have a computer with an IP address of 192.168.1.1 and a subnet mask of: 255.255.255.0. In this case, the first three octets of the subnet mask are all 255. This means that the first three octets of the IP address all belong to the network code. Therefore, the network code location of this IP address is 192.168.1.x.

This is very important because the router's job is to transfer data packets from one network to another. All devices on the network (or specifically on a network segment) share a common network number. For example, if 192.168.1.x is the network number associated with the computers connected to the router in Figure B, then the IP addresses for the four computers might be:

1.
2.
3. 192.168.1.3
4. 192.168.1.4

As you can see, each computer on the local network shares the same network address, but the device ID is different. When one computer needs to communicate with another computer, it does so by referring to that computer's IP address. For example, in this particular case, the computer with address 192.168.1.1 can easily send data packets to the computer with address 192.168.1.3 because both of them are part of the same physical network. physical.

If a machine needs to access a machine located on another network, things are a little different. Suppose that one of the users on the local network wants to visit the website TipsMake.com, a website located on a server. Like any other computer, each Web server has a unique IP address. The IP address for this website is 24.235.10.4.

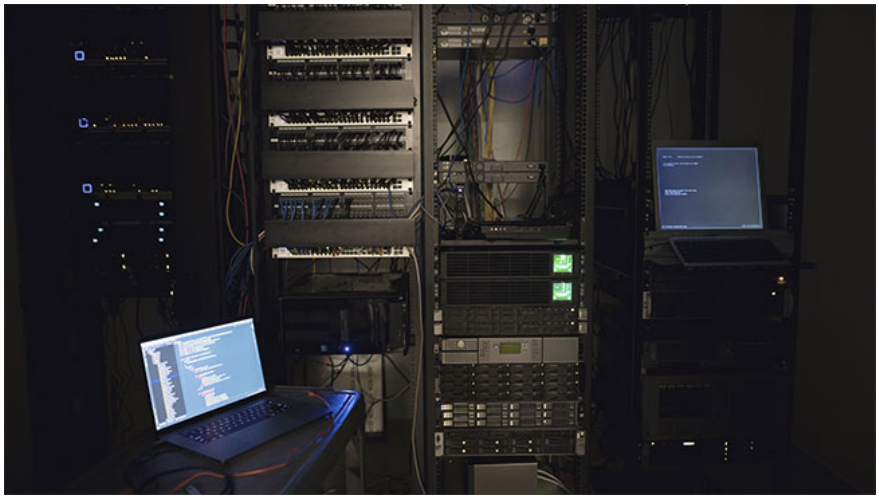
You can easily see that the website's IP address is not on the 192.168.1.x network. In this case, the computer trying to reach the website cannot send data packets out over the local network, because the Web server is not part of the local network. Instead, the computer that needs to send the data packet will consider the default gateway address.

The default gateway is part of the TCP/IP configuration of a computer. That's basically telling the computer that if it doesn't know where to send a data packet, it should send it to the default gateway address it has assigned.

The default gateway address is the IP address of a router. In this case, the router's IP address is chosen as 192.168.1.0

Note that the router's IP address shares the same network address as other machines on the local network. This is so that it can access machines on the same network. Each router has at least two IP addresses. One uses the same network address of the local network, while the other is specified by your ISP. This IP address uses the same network address of the ISP network. The router's job is then to transfer data packets from the local network to the ISP network. Your ISP has its own routers that work just like any other router, but route data packets to other parts of the Internet.

Router protocols



Routing protocols determine how a router identifies other routers on the network, keeps track of all possible destinations, and makes decisions about where to send each network message. Common protocols include:

- **Open Shortest Path First (OSPF)** - used to find the best path for packets, as they traverse a set of connected networks. OSPF is specified by the Internet Engineering Task Force (IETF) - one of the Interior Gateway Protocols (IGP).

- **Border Gateway Protocol (BGP)** - manages how packets are routed across the Internet through the exchange of information between edge routers. BGP provides network stability, ensuring the router can quickly adapt to send packets through another reconnection, if one Internet path goes down.

- **Interior Gateway Routing Protocol (IGRP)** - defines how routing information between gateways will be exchanged within an autonomous network. The routing information can then be used by other network protocols to specify how the transport should be routed.

- **Enhanced Interior Gateway Routing Protocol (EIGRP)** - developed from IGRP. If a router cannot find a route to a destination in one of these tables, it will query the neighbor tables in turn until a new route is found. When an entry in the routing table changes at one of the routers, it notifies its neighbors of the change instead of sending the entire table.

- **Exterior Gateway Protocol (EGP)** - defines how routing information between two neighbor gateway hosts (each with its own router) is exchanged. EGP is commonly used between hosts on the Internet to exchange

routing table information.

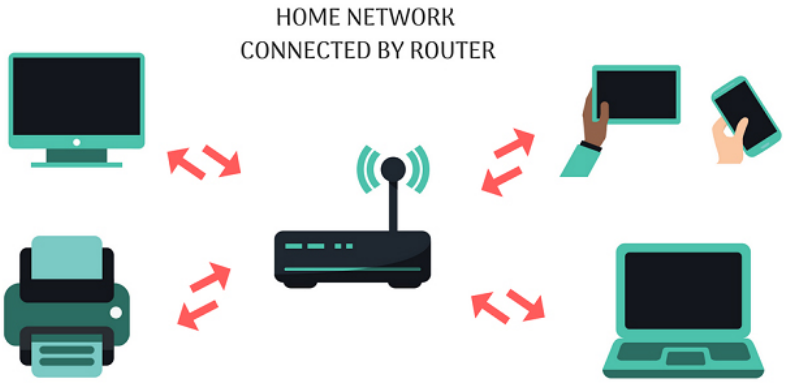
- **Routing Information Protocol (RIP)** - original protocol for defining how routers should share information when moving traffic between a group of interconnected local networks. The maximum number of hops allowed for RIP is 15, which limits the size of the network that RIP can support.

When do you need a router?

Technically, if you only want to connect to the Internet for one device, you only need to use a modem. Although for security and portability reasons, it's best to use a router even when there's only one device on your network.

But when you need to provide Internet for many devices such as mobile phones and smart TVs, the router is an indispensable device. Remember the example of street names and house numbers. If there is only one house on a street, you don't need a house number because it only has one location. But when there are many houses on that street, you need a specific address.

Users need routers not only to connect to multiple network devices but also to connect multiple devices to each other. If there is no Internet, you can still create a local network of computers and other devices. This allows you to transfer and share files with specific devices on a network such as printers, scanners and game consoles.



Without a router, data will not be sent to the correct device. A command to print a document becomes useless when it is sent to a smartphone or Google Home speaker instead of a printer.

Speaking of Google Home, a router is even more necessary if you need to connect to a Smart home. Because Smart home is also a local network of devices, without a router they cannot communicate with each other. You can still use a local network without the Internet or a modem, but not without a router.

Difference between wired and wireless routers

The difference between a wired router and a wireless router is the type of connection each device uses. Wired routers only have LAN cable ports while wireless routers (also known as Wifi routers) have antennas and wireless adapters, allowing devices to connect without cables. Most routers and modems today have LAN ports and antennas. There are a few things you need to remember when choosing a Wifi router to make sure you choose the right type you need.

As you can see, routers are extremely important network components. Without a router, connectivity between networks (such as the Internet) is impossible.

.

Some security challenges related to routers

Exploiting security vulnerabilities

All hardware-based routers come with automatically installed software called firmware that helps the router perform its functions. Like any other software, router firmware often contains vulnerabilities that cyber attackers can exploit, and router manufacturers periodically release updates to patch these vulnerabilities. For this reason, router firmware needs to be updated regularly. Unpatched routers can be compromised by attackers, allowing them to monitor traffic or use the router as part of a botnet.

DDoS attack

Organizations large and small are often the target of distributed denial of service (DDoS) attacks targeting their network infrastructure. Unregulated network layer DDoS attacks can overwhelm routers or cause them to crash, leading to network downtime. Cloudflare Magic Transit is a solution to protect routers and networks from various types of DDoS attacks.

Admin login information

All routers come with a set of admin credentials to perform administrative functions. These credentials are set to default values, such as "admin" as the username and password. Usernames and passwords should be reset to something more secure as soon as possible: Attackers know the common defaults for these credentials and can use them to gain authority. control the router remotely if they are not reset.

What makes business routers so expensive?

Let's take a look at the basic functions of a router used in businesses and large organizations. Below you will understand why:

1. Business routers often take the form of a device that integrates many additional services, for example, in addition to providing network services, there are also applications and security.
2. Hardware-based VPN integration for remote access by customers and employees.
3. Highly configurable, providing advanced options for managing connected devices, such as quality of service (QoS) control for specific devices, ports, and traffic types.
4. High-end business routers, such as those developed by Cisco, will require separate devices to create wireless access points and will use external switches to connect wired devices to the router.
5. Business routers often use high-quality components that perform well continuously for many years.

As you can see, a business router is more complex, it also omits some of the features that a home router has. Business routers are designed to be the single high-performance device in a larger and more complex network, while home routers are designed to be all-in-one solutions that are easy to connect and access. .