What is DHCP or dynamic host configuration protocol?

DHCP (Dynamic Host Configuration Protocol or Dynamic Host Configuration Protocol) is a protocol used to provide fast, automated and centralized management for IP address distribution in the network.

DHCP (Dynamic Host Configuration Protocol or Dynamic Host Configuration Protocol) is a protocol used to provide fast, automated and centralized management for IP address distribution in the network. DHCP is also used to properly configure the subnet mask, the default gateway and information about the DNS server on the device.

Learn about DHCP - Dynamic host configuration protocol

1. How DHCP works
2. Components of DHCP
3. Pros and cons when using DHCP
4. More information about DHCP
5. Security risks of DHCP

How DHCP works

The DHCP server is used to issue unique IP addresses and automatically configure other network information. In most families and small businesses, routers work as DHCP servers. In large networks, a single computer can act as a DHCP server.

In summary, this process takes place as follows: A device (client) requests an IP address from a router (server), then the host will assign an available IP address to allow the client to communicate with network.

When a device is turned on and connected to a network that has a DHCP server, it sends a request to this server, called DHCPDISCOVER request. After the DISCOVER packet arrives at the DHCP server, the server will try to keep an IP address that the device can use, and then provide the client with this DHCPOFFER packet.

After providing the selected IP address, the device responds to the DHCP server with a DHCPREQUEST packet to accept it, then the server sending the ACK is used to confirm that the device has that specific IP address and to determine the time period in which the device can use the address before taking a new address. If the server decides that the device does not have an IP address, it sends a NACK. Of course this happens very quickly and you don't need to know any kind of technique used to get the IP address from the DHCP server.

Components of DHCP

When working with DHCP, you need to understand all of its components. Below is a list of components of DHCP.

1. **DHCP server:** A network device runs a DHCP service containing the IP address and related configuration information. This is usually a server or router but can be anything that acts as a server such as an SD-WAN device.
2. **DHCP client** : The device receives configuration information from the DHCP server. This can be a computer, mobile device, IoT device (Internet of Things) or any other device that requires a network connection. Most of these devices are configured to receive DHCP information by default.
3. **IP address pool** : **Address ranges** are available for DHCP clients. These addresses are usually transmitted from lowest to highest.
4. **Subnet** : IP networks can be classified into segments called subnets. Subnets make network management easier.
5. **Lease** : The length of time the DHCP client holds IP address information. When this time period expires, the client must refresh it.
6. **DHCP relay** : Router or server listens for messages that are broadcast on that network and then transfers them to a configured server. This server then responds to the relay agent to transmit them to the client. It is

used to focus DHCP servers instead of to servers on each subnet.

Pros and cons when using DHCP

The computer or any other device connected to the network (local or Internet) must be properly configured to communicate on that network. Because DHCP allows automatic configuration, it is used in almost any device connected to the network including computers, switches, smartphones, game consoles, etc.

Due to the dynamic IP address assignment, it is very unlikely that two devices have the same IP address, which is very likely to happen when manually assigning a static IP address.

Using DHCP also makes network management easier. From an administrative point of view, all devices on the network can receive IP addresses without installing anything other than the default network settings, which are set to automatically obtain addresses. The only alternative is to manually assign the address to each device on the network.

Because these devices can automatically receive IP addresses, they can move freely from one network to another (assuming they are all set up with DHCP) and receive automatic IP addresses, this is very useful with mobile devices.

In most cases, when a device has an IP address assigned by a DHCP server, that IP address changes every time the device joins the network. If the IP address is manually assigned, it means that the administrator not only provides a specific address for each new client, but that the existing assigned addresses must be manually assigned to other devices. use the same address. This not only takes time, but manually configuring each device also causes a higher human error to occur.

1. Here's how to check if your IP address is static or dynamic

Although using DHCP has many advantages, it also has some disadvantages. Don't use dynamic IP addresses for fixed devices and need constant access, such as printers and file servers. Although such devices are used primarily in an office environment, they are not practical when assigning them to ever-changing IP addresses. For example, if the network printer has an IP address that changes, all computers connected to that printer will have to regularly update the settings so that their computer understands how to contact the printer.

This type of setup is extremely unnecessary and can be avoided by not using DHCP for these types of devices and instead assigning a static IP address to them. The same way should be applied when you need remote access to a computer on your home network regularly. If DHCP is enabled, this computer will receive a new IP address at different times. That means the computer has recorded what it has and will not be accurate for a long time. If you use remote access software using the IP address to access, you need to use a static IP address for that device.

More information about DHCP

The DHCP server determines the range of IP addresses it uses to distribute addressable devices. This group of addresses is the only way that a device can receive a valid network connection.

This is another reason DHCP is very useful, because it allows multiple devices to connect to the network for a period of time without the need for a large number of available addresses. For example, even if only 20

addresses are identified by the DHCP server, 30, 50, or even 200 (or more) devices can connect to the network, as long as no more than 20 devices are used. Use one of these available IP addresses at the same time.

Because DHCP assigns IP addresses in a specific time period (rental period), using commands like ipconfig to find the IP address of your computer will yield different results over time.

1. Instructions on how to determine the IP address on the computer

Although DHCP is used to provide dynamic IP addresses to its clients, it does not mean that static IP addresses cannot be used at the same time. Many different devices receive dynamic addresses and can also receive IP addresses manually and exist on the same network.

Even if your service provider uses DHCP to assign an IP address, you can still know this when determining a public IP address. And these addresses will change over time unless your home network uses static IP addresses.

In Windows, APIPA specifies a temporary IP address especially when the DHCP server does not provide an address for a device and uses this address until it can receive an active address.

Security risks of DHCP

DHCP protocol does not require authentication so any client can join the network quickly. Therefore, it has many security issues such as unauthorized server giving bad information to the client, unauthorized client is granted IP address, etc.

Because the client has no way to validate the DHCP server's validity, the server can provide incorrect network information. This can cause denial-of-service attacks or man-in-the-middle attacks using a fake server to block data that can be used for malicious purposes. . Conversely, because the DHCP server does not authenticate the client, it will broadcast IP address information to any device that requires it. Someone can configure the client to constantly change login information and quickly exhaust the available IP address within range, preventing devices from accessing the network.

1. Summary of popular network attacks today

DHCP parameters can solve some of the problems mentioned above. The Relay Agent Information Option option allows network engineers to tag DHCP messages when they reach the network. This card is used to control network access. In addition, there is a provision to authenticate DHCP messages. The use of 802.1x authentication also known as network access control (NAC) is used to secure DHCP. Most leading network providers support NAC.

See more:

1. Configuration, static DHCP settings on DD-WRT router
2. Configure TCP / IP to use DHCP and static IP address at the same time
3. Add DHCP server from the command line in Windows Server 2008