What Is a Network Administrator?

A network administrator supports the company's internal servers in the following ways:

- Installs and maintains the network and hardware systems
- Diagnoses and repairs connectivity issues
- Ensures people can only access the files they have permission to
- Monitors the network to maintain speed and availability
- Manages backup systems for the network

What Is NAT?

NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

How Does NAT Work?

Let's say that there is a laptop connected to a home router. Someone uses the laptop to search for directions to their favorite restaurant. The laptop sends this request in a packet to the router, which passes it along to the web. But first, the router changes the outgoing IP address from a private local address to a public address.

If the packet keeps a private address, the receiving server won't know where to send the information back to — this is akin to sending physical mail and requesting return service but providing a return address of anonymous. By using NAT, the information will make it back to the laptop using the router's public address, not the laptop's private one.

NAT Types

There are three different types of NATs. People use them for different reasons, but they all still work as a NAT.

1. Static NAT

When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

2. Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

3. PAT

PAT stands for port address translation. It's a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees' activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

Why Use NAT?

NAT is a straightforward enough process, but what is the point of it? Ultimately, it comes down to conservation and security.

IP Conservation

IP addresses identify each device connected to the internet. The existing IP version 4 (IPv4) uses 32-bit numbered IP addresses, which allows for 4 billion possible IP addresses, which seemed like more than enough when it launched in the 1970s.

However, the internet has exploded, and while not all 7 billion people on the planet access the internet regularly, those that do often have multiple connected devices: phones, personal desktop, work laptop, tablet, TV, even refrigerators.

Therefore, the number of devices accessing the internet far surpasses the number of IP addresses available. Routing all of these devices via one connection using NAT helps to consolidate multiple private IP addresses into one public IP address. This helps to keep more public IP addresses available even while private IP addresses proliferate.

On June 6, 2012, IP version 6 (IPv6) officially launched to accommodate the need for more IP addresses. IPv6 uses 128-bit numbered IP addresses, which allow for exponentially more potential IP addresses. It will take many years before this process finishes; so until then, NAT will be a valuable tool.

NAT Security

Additionally, NAT can provide security and privacy. Because NAT transfers packets of data from public to private addresses, it also prevents anything else from accessing the private device. The router sorts the data to ensure everything goes to the right place, making it more difficult for unwanted data to get by. It’s not foolproof, but it often acts as the first means of defense for your device. If an organization wants to protect its data, they’ll need to go further than just a NAT firewall — they’ll want to hire a cybersecurity professional.

NAT also allows you to display a public IP address while on a local network, helping to keep data and user history private.

All of this might seem complicated in theory, but it’s even more so in the real world. IT professionals use NAT to secure their data and use several devices under the same IP – and everyone is interested in securing their data. Getting the right certification helps IT professionals demonstrate their competence and understanding of these complicated subjects.

DHCP

If Dynamic Host Configuration Protocol (DHCP) didn’t exist, network administrators would have to manually parcel out IP addresses from the available pool, which would be prohibitively time consuming, inefficient, and error prone. Fortunately, DHCP does exist.

What is DHCP and how does it work?

DHCP is an under-the-covers mechanism that automates the assignment of IP addresses to fixed and mobile hosts that are connected wired or wirelessly.

When a device wants access to a network that’s using DHCP, it sends a request for an IP address that is picked up by a DHCP server. The server responds be delivering an IP address to the device, then monitors the use of the address and takes it back after a specified time or when the device shuts down. The IP address is then returned to the pool of addresses managed by the DHCP server to be reassigned to another device as it seeks access to the network.

While the delegation of IP addresses is the central function of the protocol, DHCP also assigns a variety of related networking parameters including subnet mask, default gateway address, and domain name server (DNS). DHCP is an IEEE standard built on top of the older BOOTP (bootstrap protocol), which has become obsolete because it only works on IPv4 networks.

Benefits of DHCP

DHCP provides a range of benefits to network administrators:

Reliable IP address configuration

You can’t have two users with the same IP address because it would create a conflict where one or both devices could not connect to the network. DHCP eliminates human error so that address conflicts, configuration errors, or simple typos are minimized.

Reduced network administration

DHCP provides centralized and automated TCP/IP configuration. By deploying a DHCP relay agent, a DHCP server is not needed on every subnet.

Mobility

DHCP efficiently handles IP address changes for users on portable devices who move to different locations on wired or wireless networks.

IP address optimization

DHCP not only assigns addresses, it automatically takes them back and returns them to the pool when they are no longer being used.

Efficient change management

DHCP makes it simple for an organization to change its IP address scheme from one range of addresses to another. DHCP enables network administrators to make those changes without disrupting end users.

DHCP components

When working with DHCP, it’s important to understand all of its components. Below is a list of them and what they do:

DHCP server

This is a networked device running the DCHP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

DHCP client

This endpoint endpoint software requests and receives configuration information from a DHCP server. This can be installed on a computer, mobile device, IoT endpoint or anything else that requires connectivity to the network. Most are configured to receive DHCP information by default.

IP address pool

The range of IP addresses that are available to DHCP clients is the IP address. Addresses are typically handed out sequentially from lowest to highest.

Subnet

IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.

Lease

The length of time for which a DHCP client holds the IP address information is known as the lease. When a lease expires, the client must renew it.

DHCP relay

A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server is the DHCP relay. The server then sends responses back to the relay agent that passes them along to the client. This can be used to centralize DHCP servers instead of having a server on each subnet.

Assigning IP addresses

The existential question associated with DHCP is how does an end user connect to the network in the first place without having an IP address?

The answer is that there's a complex system of back-and-forth requests and acknowledgments. First, all modern device operating systems include a DHCP client, which is typically enabled by default. In order to request an IP address, the client device sends out a broadcast message—DHCPDISCOVER. The network directs that request to the appropriate DHCP server.

DHCP server functionality is typically assigned to a physical server plus a backup. Other devices can also act as DHCP servers, such as SD-WAN appliances or wireless access points.

The server then determines the appropriate IP address and sends an OFFER packet to the client, which responds with a REQUEST packet. In the final step in the process, the server sends an ACK packet confirming that the client has been given an IP address.

This is all done quickly and automatically and without the need for the end user to take any action. The catch is that the IP address isn't permanent. It's only good for a specified period of time, known as the lease time.

Controlling lease time

If all DHCP did was assign IP addresses permanently, it wouldn't be dynamic, it would be static. Static addresses are appropriate for some devices, such as network printers. However, under the DHCP protocol, every time the DHCP server assigns an address there is an associated lease time. When the lease expires, the client can no longer use the IP address and is essentially kicked off the network.

The protocol is designed so active clients automatically contact the DHCP server halfway through the lease period to renew the lease. If the server doesn't respond immediately, the client continues to ask the DHCP server for a lease renewal until it is approved.

Typically, when a host shuts down, the lease is automatically terminated, in order to free up its IP address so it can be used by another client on the network.

DHCP networking functionality

In addition to providing the client with the ability to connect to network and internet resources through the IP address, the DHCP server assigns additional networking parameters that provide efficiency and security. These include:

Default gateway

This gateway is responsible for transferring data back and forth between the local network and Internet, or between local subnets.

Subnet mask

IP networking uses a subnet mask for separate the host address and the network address portions of an IP address.

DNS server

Translates domain names (networkworld.com) into IP addresses, which are represented by long strings of numbers.

Scopes and user classes of IP addresses

DHCP assigns addresses dynamically, but not randomly. Since DHCP connects hosts to the network and also assigns networking parameters, there are scenarios in which a network administrator might want to assign certain sets of subnet parameters to specific groups of users.

A scope is a consecutive range of IP addresses that a DHCP server can draw on to fulfill an IP address request from a DHCP client. By defining one or more scopes on the DHCP server, the server can manage the distribution and assignment of IP addresses to DHCP clients. Under the DHCP protocol, network admins can set unlimited numbers of scopes, as needed.

A class is a subset of a scope. Classes are useful if the network administrator wants to separate groups of devices to one segment of a larger scope. For example, SD-WAN clients for employees working remotely.

DHCP security concerns

With DHCP, the initial assignment of an IP address is designed to be fast and efficient. The tradeoff is that the DHCP protocol doesn’t require authentication. Of course, enterprises have set up strong authentication requirements for users to access resources once they are on the network, but that still leaves the DHCP server itself as a weak link in the security chain.

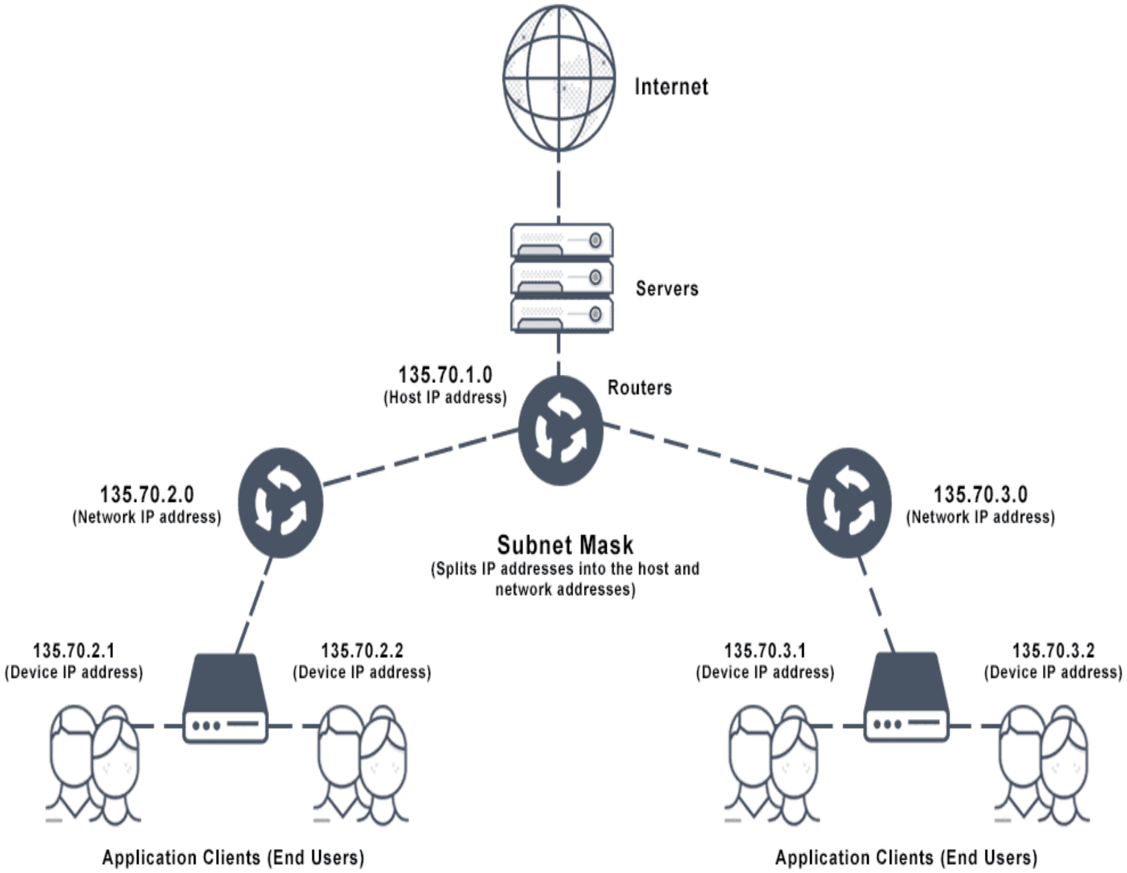
An attacker could take over or spoof the DHCP server and hand out bad information to legitimate end users, sending them to a fake site. Or it could hand out legitimate IP addresses to unauthorized users. This could lead to man-in-the-middle attacks and denial of service attacks.

The DHCP specification does address some of these issues. There is a relay-agent information option that enables network engineers to tag DHCP messages as they arrive. This tag can be used to control network access. In addition, network administrators can use 802.1x authentication (network access control) to help secure DHCP.

Subnet Mask

Every device has an IP address with two pieces: the client or host address and the server or network address. IP addresses are either configured by a DHCP server or manually configured (static IP addresses). The subnet mask splits the IP address into the host and network addresses, thereby defining which part of the IP address belongs to the device and which part belongs to the network.

The device called a gateway or default gateway connects local devices to other networks. This means that when a local device wants to send information to a device at an IP address on another network, it first sends its packets to the gateway, which then forwards the data on to its destination outside of the local network.



What is Subnet Mask?

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address into the network and host addresses.

The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these special purposes.

The IP address, subnet mask and gateway or router comprise an underlying structure—the Internet Protocol—that most networks use to facilitate inter-device communication.

When organizations need additional subnetworking, subnetting divides the host element of the IP address further into a subnet. The goal of subnet masks are simply to enable the subnetting process. The phrase "mask" is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

IP Address and Subnet Mask

A 32-bit IP address uniquely identifies a single device on an IP network. The 32 binary bits are divided into the host and network sections by the subnet mask but they are also broken into four 8-bit octets.

Because binary is challenging, we convert each octet so they are expressed in dot decimal. This results in the characteristic dotted decimal format for IP addresses—for example, 172.16.254.1. The range of values in decimal is 0 to 255 because that represents 00000000 to 11111111 in binary.

IP Address Classes and Subnet Masks

Since the internet must accommodate networks of all sizes, an addressing scheme for a range of networks exists based on how the octets in an IP address are broken down. You can determine based on the three high-order or left-most bits in any given IP address which of the five different classes of networks, A to E, the address falls within.

(Class D networks are reserved for multicasting, and Class E networks not used on the internet because they are reserved for research by the Internet Engineering Task Force IETF.)

A Class A subnet mask reflects the network portion in the first octet and leaves octets 2, 3, and 4 for the network manager to divide into hosts and subnets as needed. Class A is for networks with more than 65,536 hosts.

A Class B subnet mask claims the first two octets for the network, leaving the remaining part of the address, the 16 bits of octets 3 and 4, for the subnet and host part. Class B is for networks with 256 to 65,534 hosts.

In a Class C subnet mask, the network portion is the first three octets with the hosts and subnets in just the remaining 8 bits of octet 4. Class C is for smaller networks with fewer than 254 hosts.

Class A, B, and C networks have natural masks, or default subnet masks:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

You can determine the number and type of IP addresses any given local network requires based on its default subnet mask.

An example of Class A IP address and subnet mask would be the Class A default submask of 255.0.0.0 and an IP address of 10.20.12.2.

How Does Subnetting Work?

Subnetting is the technique for logically partitioning a single physical network into multiple smaller sub-networks or subnets.

Subnetting enables an organization to conceal network complexity and reduce network traffic by adding subnets without a new network number. When a single network number must be used across many segments of a local area network (LAN), subnetting is essential.

The benefits of subnetting include:

- Reducing broadcast volume and thus network traffic
- Enabling work from home
- Allowing organizations to surpass LAN constraints such as maximum number of hosts

Supernetting in Network Layer

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

More specifically,

- When multiple networks are combined to form a bigger network, it is termed super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

- All the Networks should be contiguous.
- The block size of every network should be equal and must be in form of 2^n.
- First Network id should be exactly divisible by whole size of supernet.

Example – Suppose 4 small networks of class C:

200.1.0.0,
200.1.1.0,
200.1.2.0,
200.1.3.0
Build a bigger network that has a single Network Id.

Explanation – Before Supernetting routing table will look like as:

Network Id	Subnet Mask	Interface
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

First, let's check whether three conditions are satisfied or not:

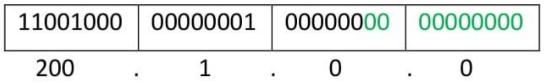
Contiguous: You can easily see that all networks are contiguous all having size 256 hosts.

Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id which is 200.1.1.0. Similarly, check that all network are contiguous.

Equal size of all network: As all networks are of class C, so all of them have a size of 256 which is in turn equal to 2^8.

First IP address exactly divisible by total size: When a binary number is divided by 2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits are 0 or not.

In the given example first IP is 200.1.0.0 and whole size of supernet is 4*^{28} = 2^{10}. If last 10 bits of first IP address are zero then IP will be divisible.



11001000	00000001	00000000	00000000
200 .	1 .	0 .	0

Last 10 bits of first IP address are zero (highlighted by green color). So, 3rd condition is also satisfied.

1. Control and reduce network traffic

2. Helpful to solve the problem of lacking IP addresses
3. Minimizes the routing table
    - It cannot cover a different area of the network when combined
    - All the networks should be in the same class and all IP should be contiguous

Network Addressing

The standard modern network prefix, used for both IPv6 and IPv4, is Classless Inter-Domain Routing (CIDR) notation. IPv4 addresses represented in CIDR notation are called network masks, and they specify the number of bits in the prefix to the address after a forward slash (/) separator. This is the sole standards-based format in IPv6 to denote routing or network prefixes.

To assign an IP address to a network interface since the advent of CIDR, there are two parameters: a subnet mask and the address. Subnetting increases routing complexity, because there must be a separate entry in each connected router's tables to represent each locally connected subnet.

What Is a Subnet Mask Calculator?

Some know how to calculate subnet masks by hand, but most use subnet mask calculators. There are several types of network subnet calculators. Some cover a wider range of functions and have greater scope, while others have specific utilities. These tools may provide information such as IP range, IP address, subnet mask, and network address.

Here are some of the most common varieties of IP subnet mask calculator:

- A IPv6 IP Subnet Calculator maps hierarchical subnets.
- An IPv4/IPv6 Calculator/Converter is an IP mask calculator that supports IPv6 alternative and condensed formats. This network subnet calculator may also allow you to convert IP numbers from IPv4 to IPv6.
- An IPv4 CIDR Calculator is a subnet mask adjustment and Hex conversion tool.
- An IPv4 Wildcard Calculator reveals which portions of an IP address are available for examination by calculating the IP address wildcard mask.
- Use a HEX Subnet Calculator to calculate the first and last subnet addresses, including the hexadecimal notations of multicast addresses.
- A simple IP Subnet Mask Calculator determines the smallest available corresponding subnet and subnet mask.
- A Subnet Range/Address Range Calculator provides start and end addresses.

What Does IP Mask Mean?

Typically, although the phrase “subnet mask” is preferred, you might use “IP/Mask” as a shorthand to define both the IP address and submask at once. In this situation, the IP address is followed by the number of bits in the mask. For example:

10.0.1.1/24
216.202.192.66/22
These are equivalent to
IP address: 10.0.1.1 with subnet mask of 255.255.255.0
IP address: 216.202.196.66 with a subnet mask example of 255.255.252.0
However, you do not mask the IP address, you mask the subnet.

Subnet Masks Reference Table

Subnetting is the process of dividing one network into smaller networks. Collectively, the smaller networks are referred to as subnetworks (or subnets), and the singular subdivision is a subnetwork (more commonly referred to as a subnet). Every single computer that is connected to a subnet shares an identical portion of the IP address. This shared information is known as a routing prefix, and in IPV4 (Internet Protocol Version 4), the routing prefix is called a subnet mask. The subnet mask is a "quad-dotted decimal representation".

This IPv4 Subnet Chart can assist you in looking up how a network is broken up into subnets.

Class address ranges:

Class A = 1.0.0.0 to 126.0.0.0
Class B = 128.0.0.0 to 191.255.0.0
Class C = 192.0.1.0 to 223.255.255.0

Reserved address ranges for private (non-routed) use:

10.0.0.0 -> 10.255.255.255
172.16.0.0 -> 172.31.255.255
192.168.0.0 -> 192.168.255.255

Other reserved addresses:

127.0.0.0 is reserved for loopback and IPC on the local host
224.0.0.0 -> 239.255.255.255 is reserved for multicast addresses

Chart notes:

Number of Subnets - "( )" Refers to the number of effective subnets, since the use of subnet numbers of all 0s or all 1s is highly frowned upon and RFC non-compliant.
Number of Hosts - Refers to the number of effective hosts, excluding the network and broadcast address.

Class A

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/8	255.0.0.0	0	16777214
/9	255.128.0.0	2 (0)	8388606
/10	255.192.0.0	4 (2)	4194302
/11	255.224.0.0	8 (6)	2097150
/12	255.240.0.0	16 (14)	1048574
/13	255.248.0.0	32 (30)	524286
/14	255.252.0.0	64 (62)	262142
/15	255.254.0.0	128 (126)	131070
/16	255.255.0.0	256 (254)	65534
/17	255.255.128.0	512 (510)	32766
/18	255.255.192.0	1024 (1022)	16382
/19	255.255.224.0	2048 (2046)	8190
/20	255.255.240.0	4096 (4094)	4094
/21	255.255.248.0	8192 (8190)	2046
/22	255.255.252.0	16384 (16382)	1022
/23	255.255.254.0	32768 (32766)	510
/24	255.255.255.0	65536 (65534)	254
/25	255.255.255.128	131072 (131070)	126
/26	255.255.255.192	262144 (262142)	62
/27	255.255.255.224	524288 (524286)	30
/28	255.255.255.240	1048576 (1048574)	14
/29	255.255.255.248	2097152 (2097150)	6
/30	255.255.255.252	4194304 (4194302)	2

Class B

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/16	255.255.0.0	0	65534
/17	255.255.128.0	2 (0)	32766
/18	255.255.192.0	4 (2)	16382
/19	255.255.224.0	8 (6)	8190
/20	255.255.240.0	16 (14)	4094
/21	255.255.248.0	32 (30)	2046
/22	255.255.252.0	64 (62)	1022
/23	255.255.254.0	128 (126)	510
/24	255.255.255.0	256 (254)	254
/25	255.255.255.128	512 (510)	126
/26	255.255.255.192	1024 (1022)	62
/27	255.255.255.224	2048 (2046)	30
/28	255.255.255.240	4096 (4094)	14
/29	255.255.255.248	8192 (8190)	6
/30	255.255.255.252	16384 (16382)	2

Class C

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/24	255.255.255.0	0	254
/25	255.255.255.128	2 (0)	126
/26	255.255.255.192	4 (2)	62
/27	255.255.255.224	8 (6)	30
/28	255.255.255.240	16 (14)	14
/29	255.255.255.248	32 (30)	6
/30	255.255.255.252	64 (62)	2

Class D

CIDR Block	Supernet Mask	Number of Class C Addresses	Number of Hosts
/14	255.252.0.0	1024	262144
/15	255.254.0.0	512	131072
/16	255.255.0.0	256	65536
/17	255.255.128.0	128	32768
/18	255.255.192.0	64	16384
/19	255.255.224.0	32	8192
/20	255.255.240.0	16	4096
/21	255.255.248.0	8	2048
/22	255.255.252.0	4	1024
/23	255.255.254.0	2	512