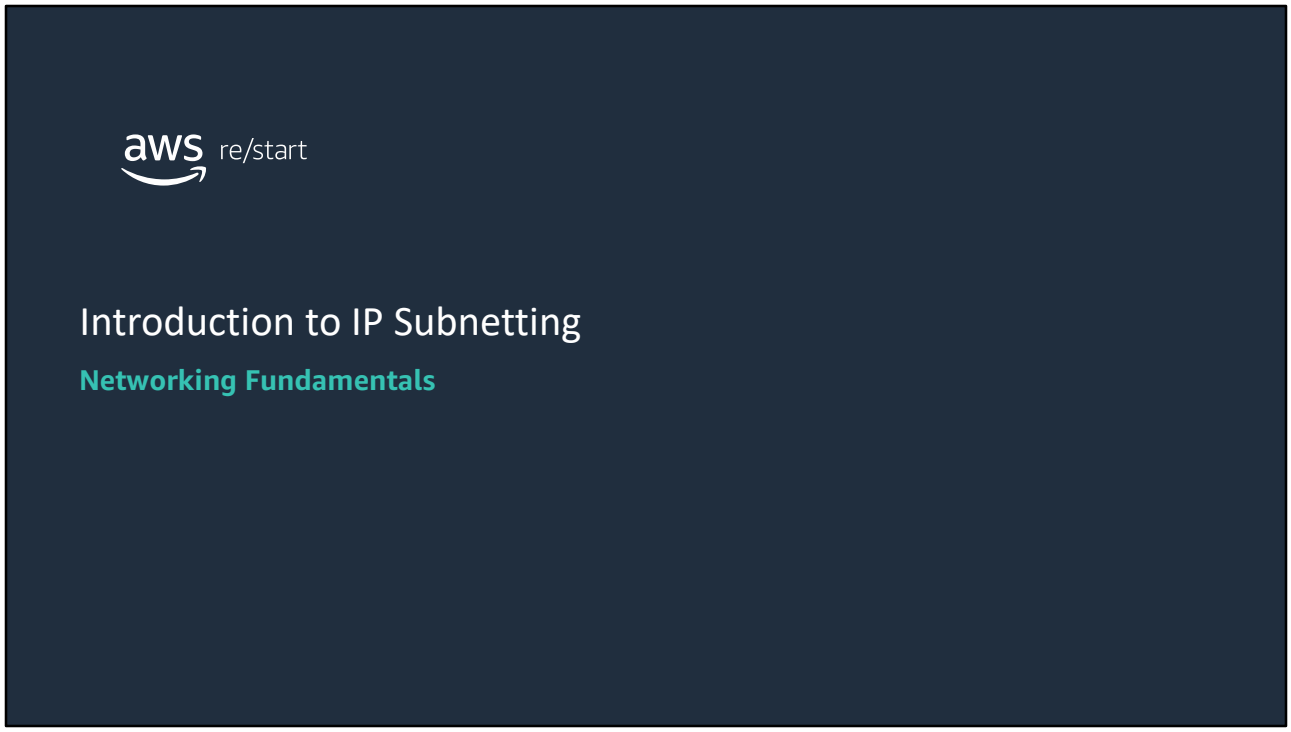


Welcome to Introduction to IP Subnetting.

What you will learn

At the core of the lesson

You will learn how to:

- Define a subnet, its parts, and its purpose
- Describe the purpose of IP subnetting
- Use the Classless Inter-Domain Routing (CIDR) notation to specify subnet address ranges
- Describe the use of subnet masks

aws re/start

In this lesson, you will learn how to:

- Define a subnet, its parts, and its purpose
- Describe the purpose of IP subnetting
- Use the Classless Inter-Domain Routing (CIDR) notation to specify subnet address ranges
- Describe the use of subnet masks

What is an IP address, and how can you find yours?

Take a moment to recall: What is an IP address, and how can you find yours?

What is an IP address?

Networking is how you connect computers and other devices around the world so that they can communicate with one another. Each one has an IP address so that traffic (data packets) can be directed to and from each device.

Think about IP addresses as similar to your home and work addresses. The internet uses these addresses to deliver packets of information to each address that it is routed to. This process is like using an email address to direct traffic to one or several recipients.

aws re/start

What is an IP address?

Networking is how you connect computers and other devices around the world so that they can communicate with one another. Each one has an IP address so that traffic (data packets) can be directed to and from each device.

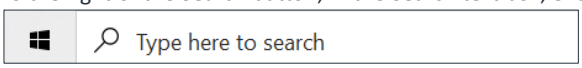
Think about IP addresses as similar to your home and work addresses. The internet uses these addresses to deliver a packet of information to each address it is routed to. This process is like using an email address to direct traffic to one or several recipients.

How to find your own IP address

You should always be able to find the IP address for a device. The best way to do it is to search online for the instructions for the device that you are using.

The following are the instructions for finding your local IP address on a Windows PC:

1. To the right of the Search button, in the Search text box, enter **command prompt,** and press Enter.



2. In the command prompt box, enter **ipconfig,** and press Enter.
3. Scroll to see a list of Wireless Lan Adapter Wi-Fi information, including IP addresses.

aws re/start

You should always be able to find the IP address for a device. The best way to do it is to search online for the instructions for the device that you are using.

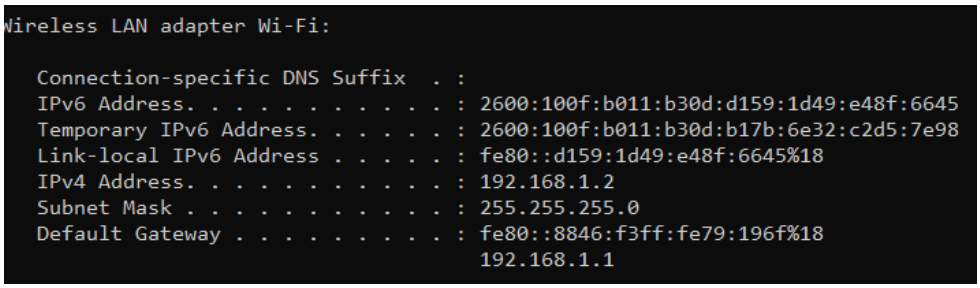
The following are the instructions for finding your local IP address on a Windows PC:

1. To the right of the Search button, in the Search text box, enter **command prompt,** and press Enter.
2. In the Command Prompt box, enter **ipconfig,** and press Enter.
3. Scroll down to see a list of Wireless Lan Adapter Wi-Fi information, including IP addresses.

How to find your own IP address, continued

The image contains an example of what you'll see after scrolling through the results of your ipconfig search. As soon as your ipconfig results display, the following are a few of the many things that are displayed:

- IPv4 Address (192.168.1.2)
- IPv6 Address (2600:100f:b011:b30d:b17b:6e32:c2d5:7e98)
- Subnet Mask (255.255.255.0)



aws re/start

This slide shows an example of what you'll see after scrolling through the results of your ipconfig search.

Notice that you can see:

- IPv4 address (192.168.1.2)
- IPv6 address (2600:100f:b011:b30d:b17b:6e32:c2d5:7e98)
- Subnet (255.255.255.0)

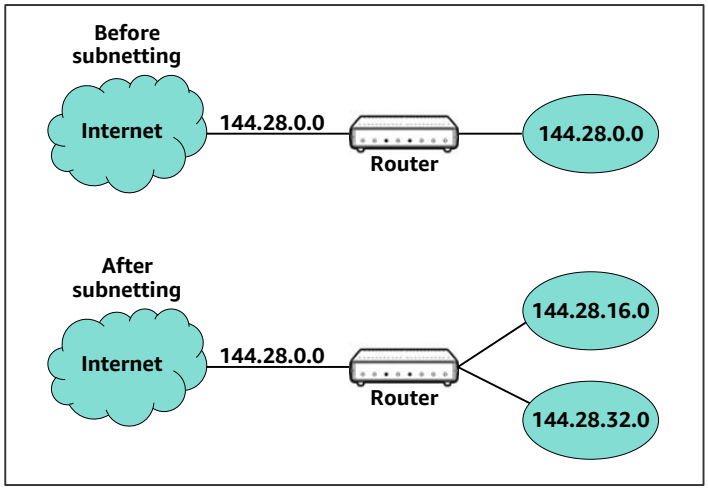
Subnetting

In this section, you'll learn what a subnet is.

What are subnets?

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

- An organization can use subnetting to conceal network complexity and reduce network traffic by adding subnets without a new network number.
- Organizations use subnets to subdivide large networks into smaller, more efficient subnetworks.
- Subnets split larger networks into a groupings of smaller, interconnected networks to help minimize traffic.



aws re/start

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

An organization can use subnetting 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.

- A subnet is used to split a network into two or more smaller, more efficien networks.
- A subnet is a segmented piece of a larger network and is often thought of as a subnetwork.
- Subnets split larger networks into a groupings of smaller, interconnected networks to help minimize traffic.

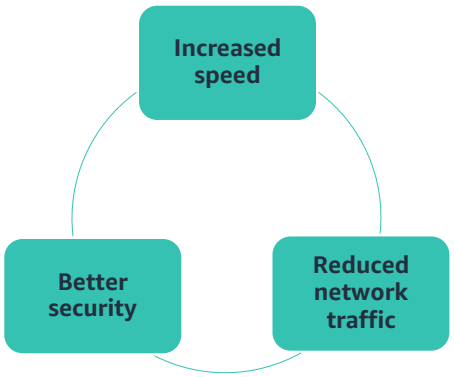
In the example shown, after submitting, the IP address has been changed from 144.28.0.0 (external) to 144.28.**16**.0 and 144.28.**32**.0. The changed numbers are multiples of 16.

Why do organizations use subnets?

Organizations use subnets to:

- Minimize traffic
- Maximize the efficiency of IP addressing
- Reduce network traffic by eliminating collision and broadcast traffic
- Provide the efficient application of network security policies at the interconnection between subnets
- Facilitate spanning of large geographical distances
- Prevent the allocation of large numbers of unused IP network addresses

Top reasons for using subnets



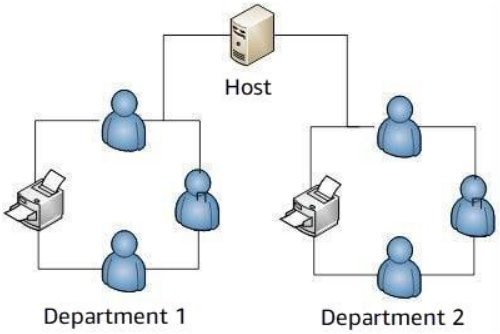
aws re/start

Why do organizations use subnets?

Organizations use subnets to:

- Minimize traffic. Using subnets, traffic takes the most efficient routes, increasing network speeds.
- Maximize the efficiency of IP addressing.
- Reduce network traffic by eliminating collision and broadcast traffic.
- Provide the efficient application of network security policies at the interconnection between subnets.
- Facilitate spanning of large geographical distances (especially for the needs of AWS).
- Prevent the allocation of large numbers of unused IP network addresses.

A simple subnet example



In this example, the subnets bring an organization the following benefits:

- Splitting the network in two produces less printer traffic on each printer.
- Jobs print faster, increasing personnel productivity.

aws re/start

This slide shows a simple subnet example.

In this example, the subnets bring an organization the following benefits:

- Splitting the network into two produces less printer traffic on each printer.
- Jobs print faster, increasing personnel productivity.

If this organization had not created subnets and added two printers, six people could be standing in line waiting for their 100-page reports to print. That arrangement would cost a company a loss of productivity, efficiency, and more.

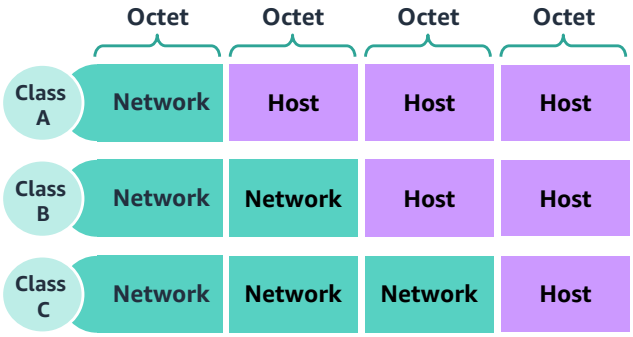
How subnetting works with classes

IP subnetting is a method for dividing a single, physical network into smaller subnetworks (subnets).

Subnetting in an IPv4 address gives you 32 bits to divide into two parts:

- A network ID
- A host ID

Depending on the number of bits that you assign to the network ID, subnetting offers either a greater number of total subnetworks or more hosts (devices that can be part of each subnet).



aws re/start

IP subnetting is a method for dividing a single, physical network into smaller subnetworks (subnets). Subnetting in an IPv4 address gives you 32 bits to divide into two parts: a network ID and a host ID.

Depending on the number of bits you assign to the network ID, subnetting provides either a greater number of total subnetworks or more hosts. (Hosts are devices that can be part of each subnet.)

Classes that you can or cannot use in a subnet

One more aspect of an IP address is important to understand: the concept of a class. Each IP address belongs to a class of IP addresses depending on the number in the first octet.

The following are these classes:

First octet value	Class	Example IP address	IPv4 bits for network ID sizes
0–126	Class A	34.126.35.125	8
128–191	Class B	134.23.45.123	16
192–223	Class C	212.11.123.3	24
224–239	Class D	225.2.3.40	Used for multicast and cannot be used for regular internet traffic
240–255	Class E	245.192.1.123	Reserved and cannot be used on the public internet

aws re/start

Classes are important to know about in regard to subnetting.

Each IP address belongs to a class of IP addresses depending on the number in the first octet.

Standard IPv4 address classes have three network ID sizes: 8 bits for Class A (which allows for more hosts), 16 bits for Class B, and 24 bits for Class C (which can have more subnetworks). However, in many cases, standard sizes do not fit all. With subnetting, you can have more control over the length of the network ID portion of an IP address. Your options go beyond the bounds of the standard 8-bit, 16-bit, or 24-bit lengths. Therefore, you can create more Host IDs for host devices per subnetwork.

The opposite of subnetting is supernetting, where you combine two or more subnets to create a single supernet. You can refer to this supernet by using a CIDR prefix.

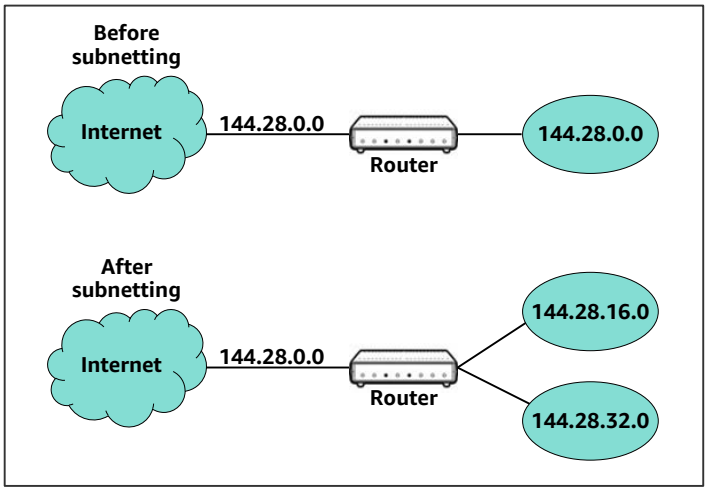
What is the use of Class D and Class E IP addresses?

Class D and Class E IP addresses are mostly reserved for experimental purposes. For example, a Class D IP address is almost exclusively reserved for multicasting applications. (Multicasting is a method of routing data on a computer network by which a single or group of senders can communicate with a group of receivers.) Unlike Classes A, B, and C, Class D is not available for use in normal networking

operations. They don’t have subnet potential because Class D has no host bits within its address space.

Class E is often cited as having been created for future use, research, and development. Although these IP addresses are reserved, their actual use has never developed. As a result, most network implementations disregard this class altogether. In fact, Class E is sometimes classified as illegal or undefined. The one exception is IP address 255.255.255.255, which can be used as a broadcast address. (A broadcast address is a network address in which devices connect to a multiple-access communications network).

More about after subnetting



What do you notice when you look at the IP addresses after the subnetting has been applied?

The first two sections of network are the network identifier (144.28.0.0), and the subnets are identified as 144.28.16.0 and 144.28.32.0. But to the outside world, the IP address is seen only as 144.28.0.0. (See purple colored text to see the subnets.)

You can use up to three of the four octets for subnets, depending on the class, which will be explained in an upcoming section.

aws re/start

What do you notice when you look at the IP addresses after the subnetting has been applied?

The first two sections of network are the network identifier (144.28.0.0), and the subnets are identified as 144.28.16.0 and 144.28.32.0. But to the outside world, the IP address is seen only as 144.28.0.0. (See purple colored text to see the subnets.)

You can use up to three of the four octets for subnets, depending on the class, which an upcoming section will explain further.

What are the parts of a subnet?

A 32-bit IP address uniquely identifies a single device on an IP network. The subnet mask divides the 32 binary bits into the host and network sections, but they are also broken into four 8-bit octets. Each subnet is a network inside a network and contains the following parts:

- **Network ID:** This portion of the IP address identifies the network and makes it unique.
- **Subnet mask:** A subnet mask defines the range of IP addresses that can be used within a network or subnet. It also separates an IP address into two parts: network bits and host bits.
- **Host ID range:** This range consists of all of the IP addresses between the subnet address and the broadcast address. To calculate, take the number of usable host IP addresses within the subnet minus the first and last.
- **Number of usable host IDs:** This number depends on the class and prefix of subnet. Depending on the CIDR, it can run between 30 and 254. It is always minus the broadcast ID and the first character of the IP address (minus 2).
- **Broadcast ID:** This IP address is used to target all systems on a specific subnet instead of a single host. It permits traffic to be sent to all devices on a specific subnet rather than a specific host.

A 32-bit IP address uniquely identifies a single device on an IP network. The subnet mask divides the 32 binary bits into the host and network sections, but they are also broken into four 8-bit octets. Each subnet is a network inside a network and contains the following parts:

- **Network ID:** This portion of the IP address identifies the network and makes it unique.
- **Subnet mask:** A subnet mask defines the range of IP addresses that can be used within a network or subnet. It also separates an IP address into two parts: network bits and host bits.
- **Host ID range:** This range consists of all of the IP addresses between the subnet address and the broadcast address. To calculate, take the number of usable host IP addresses within the subnet minus the first and last.
- **Number of usable host IDs:** This number depends on the class and prefix of subnet. Depending on the CIDR (covered in the last section of this module), it can run between 30 and 254. It is always minus the broadcast ID and the first character of the IP address (minus 2).
- **Broadcast ID:** This IP address is used to target all systems on a specific subnet instead of a single host. It permits traffic to be sent to all devices on a specific subnet rather than a specific host.

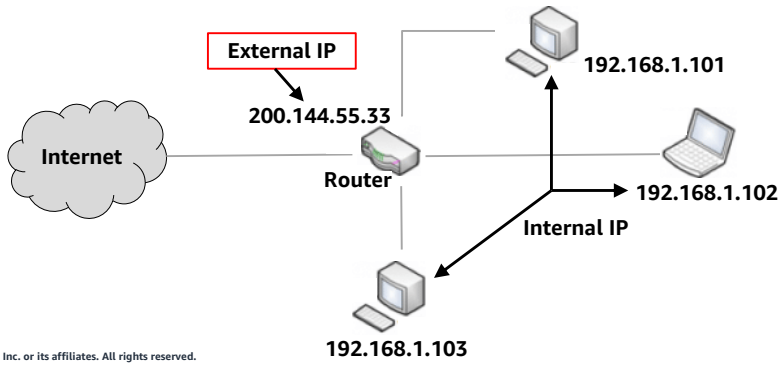
Understanding subnet masks

This section discusses subnet masks.

What is a subnet mask?

The IP address, subnet mask, and gateway or router create an underlying structure called the Internet Protocol. Most networks use it to facilitate inter-device communication.

As an organization's need for devices grows, subnetting divides the host element of the IP address to further increase the number of available subnets. The goal of a subnet mask is to create more subnets. The term *mask* is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.



aws re/start

The IP address, subnet mask, and gateway or router together create an underlying structure, which is called the Internet Protocol. Most networks use it to facilitate inter-device communication.

As an organization's need for devices grows, subnetting divides the host element of the IP address to further increase the number of available subnets. The goal of a subnet mask is to create more subnets. The term *mask* is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

What is a subnet mask? (continued)

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 one can be assigned to hosts because they are reserved for these special purposes.

Class A subnet mask	**Network**	**Host**	**Host**	**Host**
	255	**0**	**0**	**0**
Class B subnet mask	**Network**	**Network**	**Host**	**Host**
	255	**255**	**0**	**0**
Class C subnet mask	**Network**	**Network**	**Network**	**Host**
	255	**255**	**255**	**0**

aws re/start

What is a 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 one can be assigned to hosts because they are reserved for these special purposes.

Why are subnet masks used?

Subnet masks:

- Determine which hosts are on the local network and which ones are outside of the network. Hosts can talk directly to hosts on the same network, but they must communicate with a router to talk to hosts on external networks.
- Hide network size information for IPv4 addresses.
- Are used for special purposes:
  - Class D IPv4 addresses are used for multicast addressing.
  - In computer networking, multicast refers to group communication where information is addressed to a group of destination computers simultaneously. For example, multicast addressing is used in internet television and multipoint video conferences.
  - The class E IPv4 addresses cannot be used in real applications because they are used only in experimental ways.

Why are subnet masks used?

A subnet mask uses its own 32-bit number to mask the IP address and further enable the subnetting process. Subnet masks:

- Determine which hosts are on the local network and which hosts are outside the network. Hosts can talk directly to hosts on the same network, but they must communicate with a router to talk to hosts on external networks.
- Hide network size information for IPv4 addresses.
- Are used for special purposes:
  - Class D IPv4 addresses are used for multicast addressing.
  - In computer networking, multicast refers to group communication where information is addressed to a group of destination computers simultaneously. For example, multicast addressing is used in internet television and multipoint video conferences.
  - Class E IPv4 addresses cannot be used in real applications because they are used only in experimental ways.

CIDR notation

In this section, you will discuss CIDR notation.

What is CIDR?

An IP addressing scheme that improves the allocation of IP addresses

The general rule is that subnets are used at the organizational level, but CIDRs are used at the internet service provider (ISP) level and higher.

- **Subnets**: When you place a mask over the subnet, you instantly create an entire subnetwork that is a subordinate network of the internet. The subnet mask signals to the router which part of the IP address is assigned to the hosts (individual participants of the network). It also signals which address determines the network.
- **CIDRs**: This scheme adds suffixes and then integrates them directly into the IP address. Using CIDRs, you can create not only subnets but also supernets. In addition, you can use CIDR to subdivide a network into several networks.

CIDR is an IP addressing scheme that improves the allocation of IP addresses.

The general rule is that subnets are used at the organizational level, but CIDRs are used at the ISP level and higher.

- **Subnets**: When you place a mask over the subnet, you instantly create an entire subnetwork that is a subordinate network of the internet. The subnet mask signals to the router which part of the IP address is assigned to the hosts (individual participants of the network). It also signals which address determines the network.
- **CIDRs**: This scheme adds suffixes and then integrates them directly into the IP address. Using CIDRs, you can create not only subnets but also supernets. In addition, you can use CIDR to subdivide a network into several networks.

CIDR notations

Previously, you looked at a single IP address. What if you want to send data to a range of IP addresses as in the example of 192.168.1.0 and 192.168.1.255? How can you do that?

CIDR notation is a compressed method of specifying a range of IP addresses. This method determines how many IP addresses are available to you. The following is an example of how to use a range of IP addresses.

192.168.1.0/24

When you add a slash after the fourth integer and then add another number, it specifies how many bits in the IP address are fixed.

Earlier, you saw the /26 when you set up three subnets. This notation is another way of showing the range.

aws re/start

Previously, you looked at a single IP address. What if you want to send data to a range of IP addresses as in the example of 192.168.1.0 and 192.168.1.255? How can you do that?

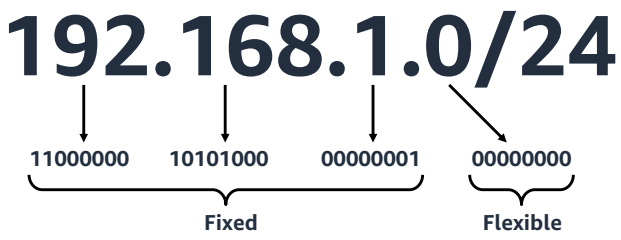
CIDR notation is a compressed method of specifying a range of IP addresses. This method determines how many IP addresses are available to you. This example shows how to use a range of IP addresses.

When you add a slash after the fourth integer and then add another number, it specifies how many bits in the IP address are fixed.

Earlier, you saw the /26 when you set up three subnets. This notation is another way of showing the range.

CIDR notations (continued)

In this example, the first 24 bits of the IP address are fixed. The rest are flexible.

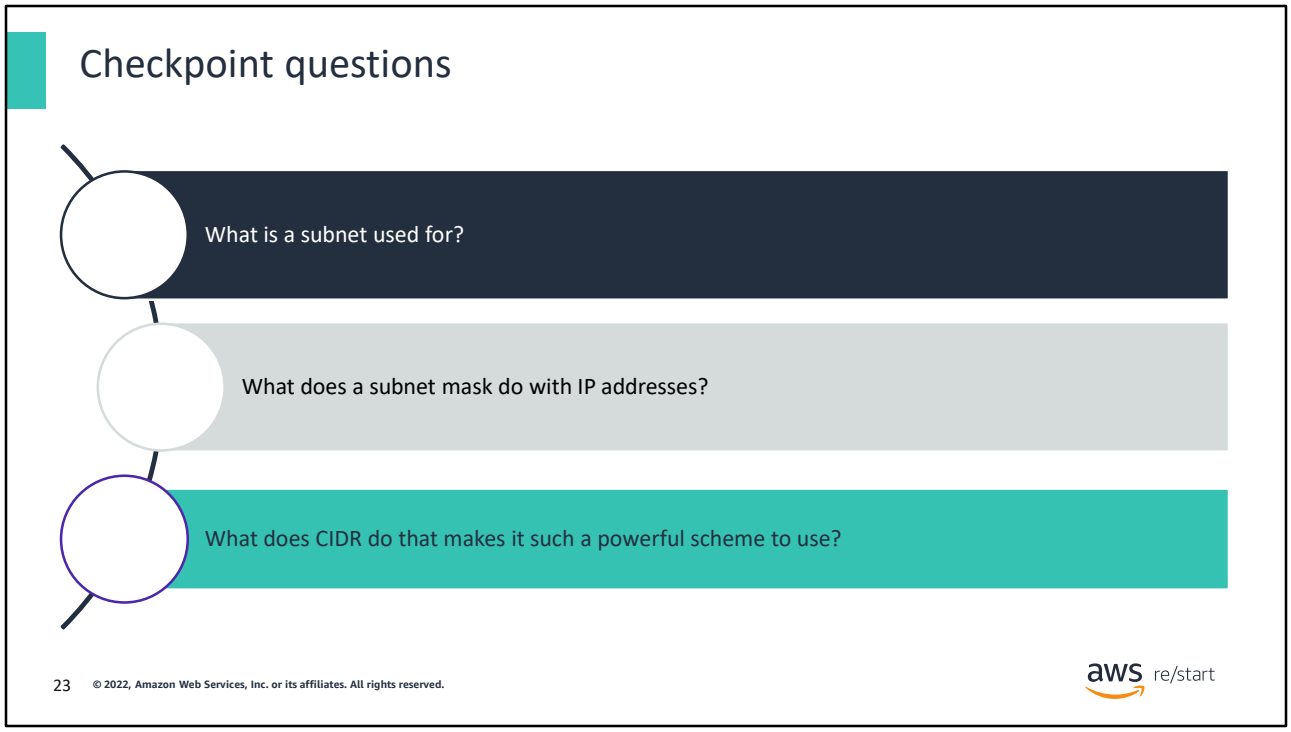


Here, 32 total bits minus 24 fixed bits leaves 8 flexible bits. Each of these flexible bits can be either 0 or 1 because they are binary. Therefore, you have two choices for each of the 8 bits, which provides 256 IP addresses in that IP range.

aws re/start

In this example, the first 24 bits of the IP address are fixed. The rest are flexible.

Here, 32 total bits minus 24 fixed bits leaves 8 flexible bits. Each of these flexible bits can be either 0 or 1 because they are binary. Therefore, you have two choices for each of the 8 bits, which provides 256 IP addresses in that IP range.



Q1: What is a subnet used for?

Organizations use subnets to:

- Minimize traffic. Using subnets, traffic takes the most efficient routes, which increases network speeds.
- Maximize the efficiency of IP addressing.
- Extend the life of IPv4 because of its scarcity.
- Reduce network traffic by eliminating collision and broadcast traffic.
- Apply network security policies efficiently at the interconnection between subnets.

Q2. What does a subnet mask do with IP addresses?

The subnet mask splits the IP address into the host and network addresses. In this way, it defines which part of the IP address belongs to the device and which part belongs to the network. It also covers up the subnet so that it isn't seen outside of allowed traffic.

Q3. What does CIDR do that makes it such a powerful scheme to use?

This scheme adds suffixes to integrate them directly into the IP address. Using CIDRs, you can create not only subnets but also supernets. You can also use it to subdivide a

network into several networks.

Key takeaways

- **IP addresses**: IP addresses are used for individual devices and small networks.
- **Subnets**: Organizations use subnets to divide large networks into smaller, more interconnected networks to increase speed, minimize security threats, and reduce network traffic.
- **Subnet masks**: Subnet masks split IP addresses into host and network sections based on four 8-bit octets.
- **Subnet communication rules**: Systems within the same subnet can communicate directly with each other, but systems on different subnets must communicate through a router.
- **CIDR**: This scheme adds suffixes to integrate them directly into the IP address. Using CIDRs, you can create not only subnets but also supernets.

aws re/start

- **IP addresses**: IP addresses are used for individual devices and small networks.
- **Subnets**: Organizations use subnets to divide large networks into smaller, more interconnected networks to increase speed, minimize security threats, and reduce network traffic.
- **Subnet masks**: Subnet masks split IP addresses into host and network sections based on four 8-bit octets.
- **Subnet communication rules**: Systems within the same subnet can communicate directly with each other, but systems on different subnets must communicate through a router.
- **CIDR**: This scheme adds suffixes to integrate them directly into the IP address. Using CIDRs, you can create not only subnets but also supernets.

Thank you

Thank you for completing this module.