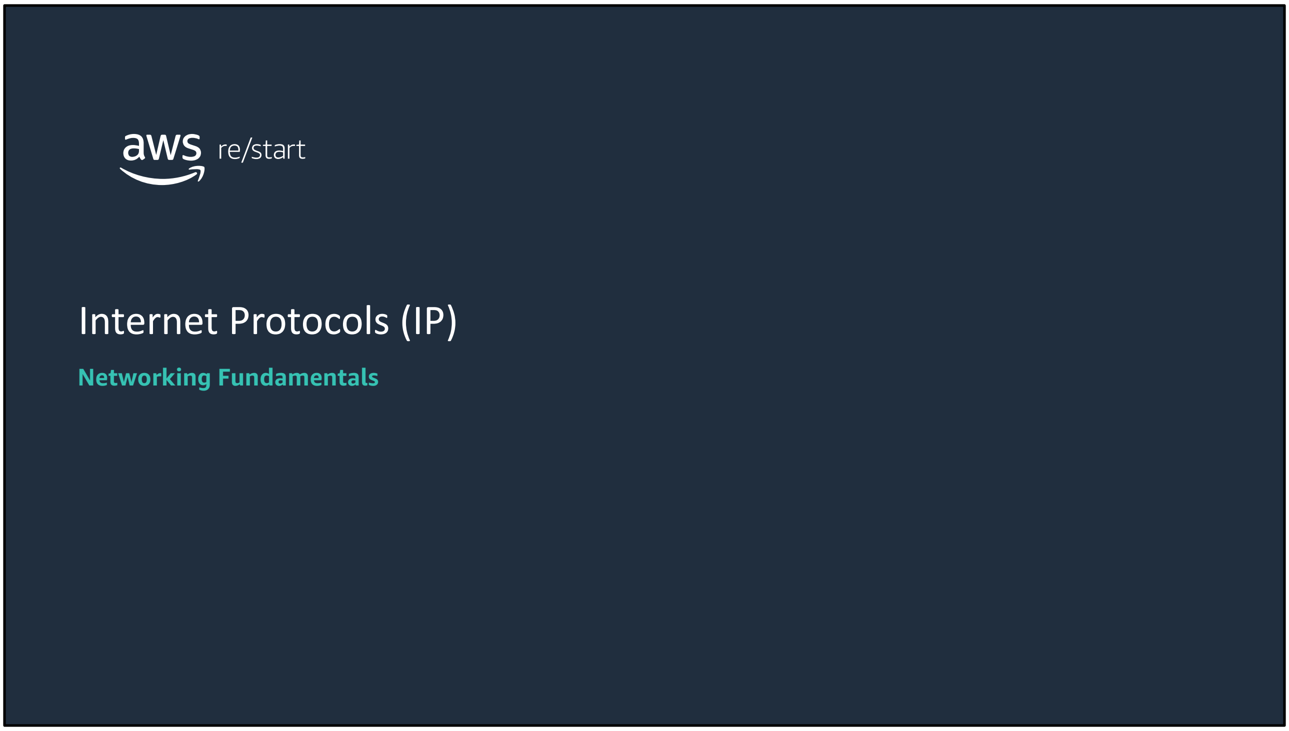
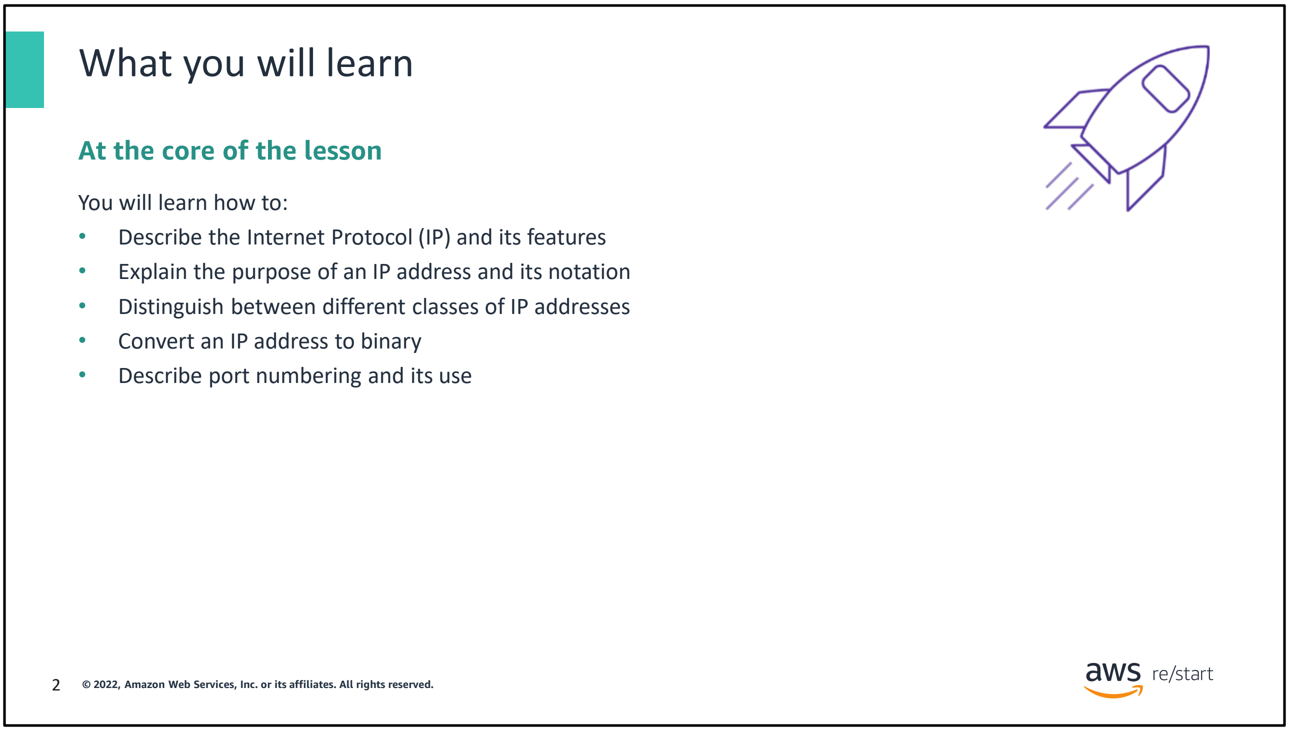


aws re/start

Internet Protocols (IP)

Networking Fundamentals

Welcome to Internet Protocols (IP)!



What you will learn

At the core of the lesson

You will learn how to:

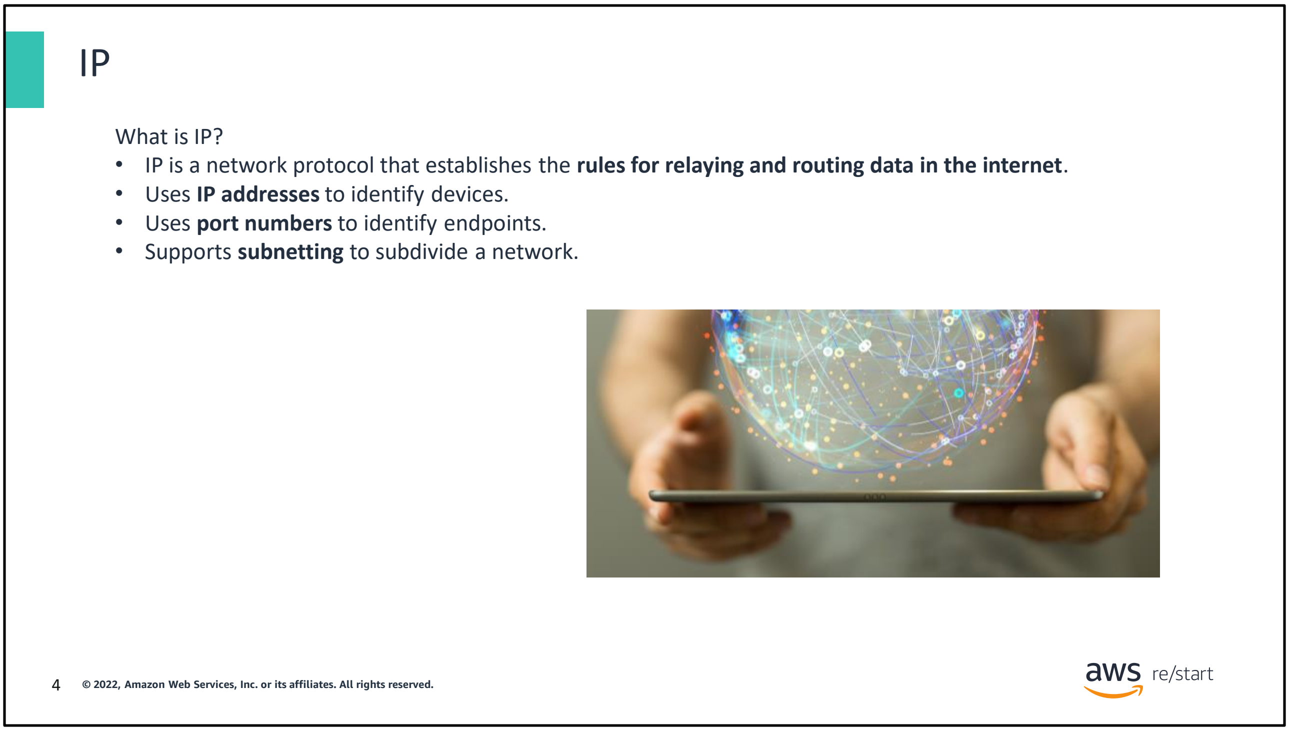
- Describe the Internet Protocol (IP) and its features
- Explain the purpose of an IP address and its notation
- Distinguish between different classes of IP addresses
- Convert an IP address to binary
- Describe port numbering and its use

You will learn how to:

- Describe the Internet Protocol (IP) and its features
- Explain the purpose of an IP address and its notation
- Distinguish between different classes of IP addresses
- Convert an IP address to binary
- Describe port numbering and its use

What is IP?

In this section, you will understand what an IP is.



IP

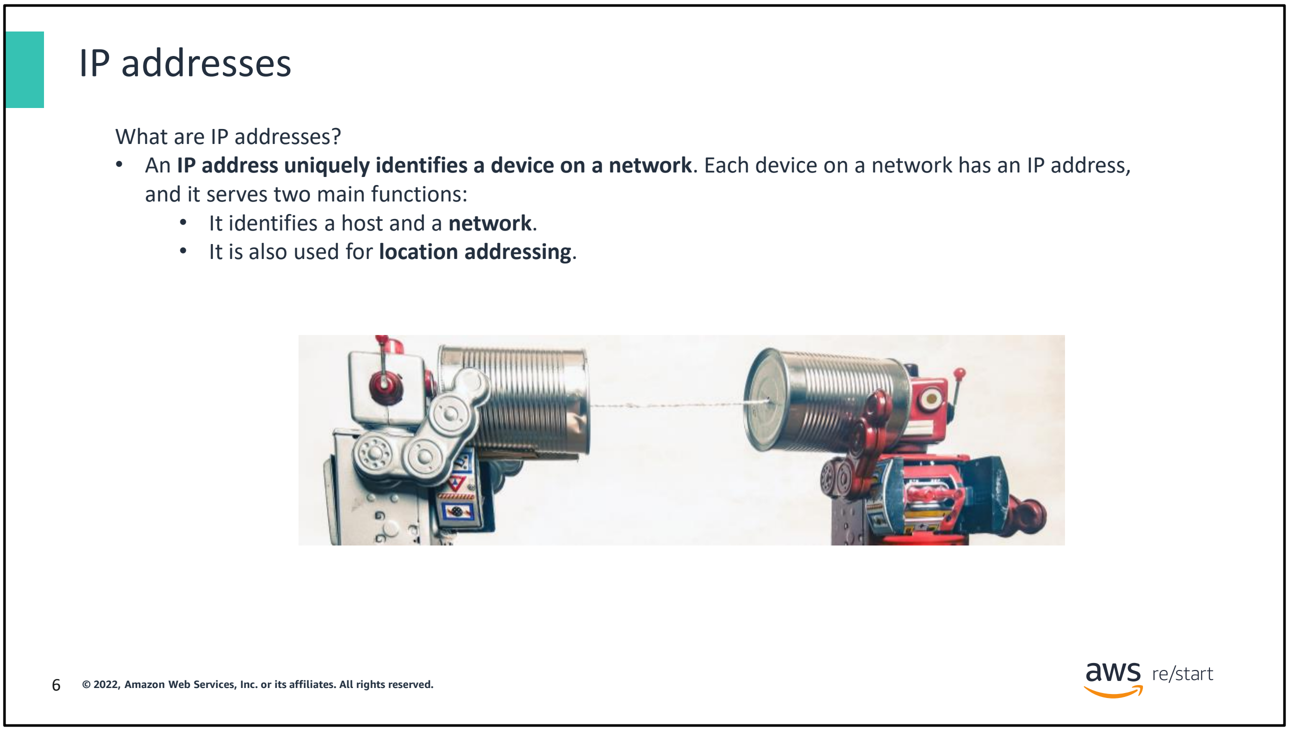
What is IP?

- IP is a network protocol that establishes the **rules for relaying and routing data in the internet**.
- Uses **IP addresses** to identify devices.
- Uses **port numbers** to identify endpoints.
- Supports **subnetting** to subdivide a network.

IP is a critical standard within the larger TCP/IP protocol suite when it is combined with the connection-oriented Transmission Control Protocol (TCP). TCP/IP implements the set of protocols that provides a crucial service for the internet because it enables the successful routing of network traffic among devices on a network.

IP addresses

In this section, we will define IP addresses.



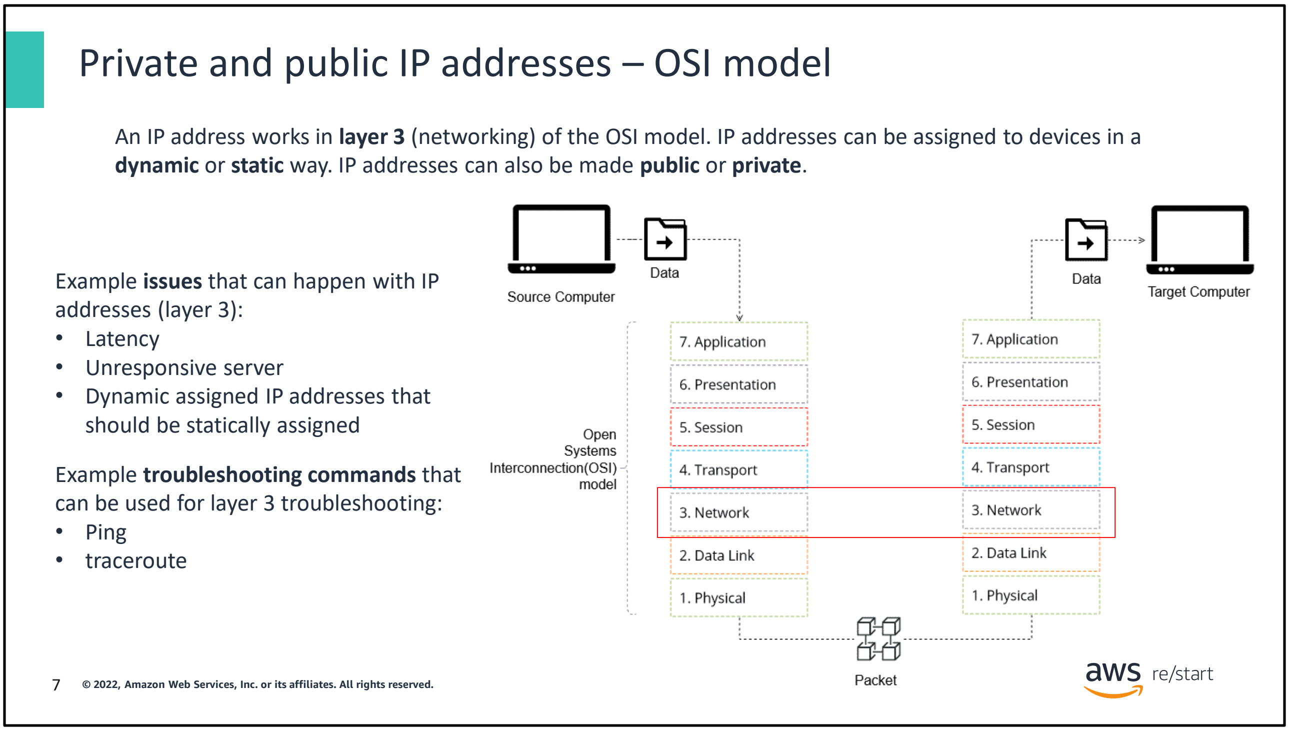
IP addresses

What are IP addresses?

- An **IP address uniquely identifies a device on a network**. Each device on a network has an IP address, and it serves two main functions:
  - It identifies a host and a **network**.
  - It is also used for **location addressing**.

IP addresses:

- Work at layer 3 of the OSI model and are used to identify a host and a network.
- Can be assigned in a dynamic or static way:
  - Dynamic is when an assigned IP address can change.
  - Static is when an assigned IP address does not change.
- Can be made public or private:
  - A public IP address can be accessed over the internet.
  - A private IP address cannot be accessed over the internet.



Private and public IP addresses – OSI model

An IP address works in **layer 3** (networking) of the OSI model. IP addresses can be assigned to devices in a **dynamic** or **static** way. IP addresses can also be made **public** or **private**.

Example **issues** that can happen with IP addresses (layer 3):

- Latency
- Unresponsive server
- Dynamic assigned IP addresses that should be statically assigned

Example **troubleshooting commands** that can be used for layer 3 troubleshooting:

- Ping
- traceroute

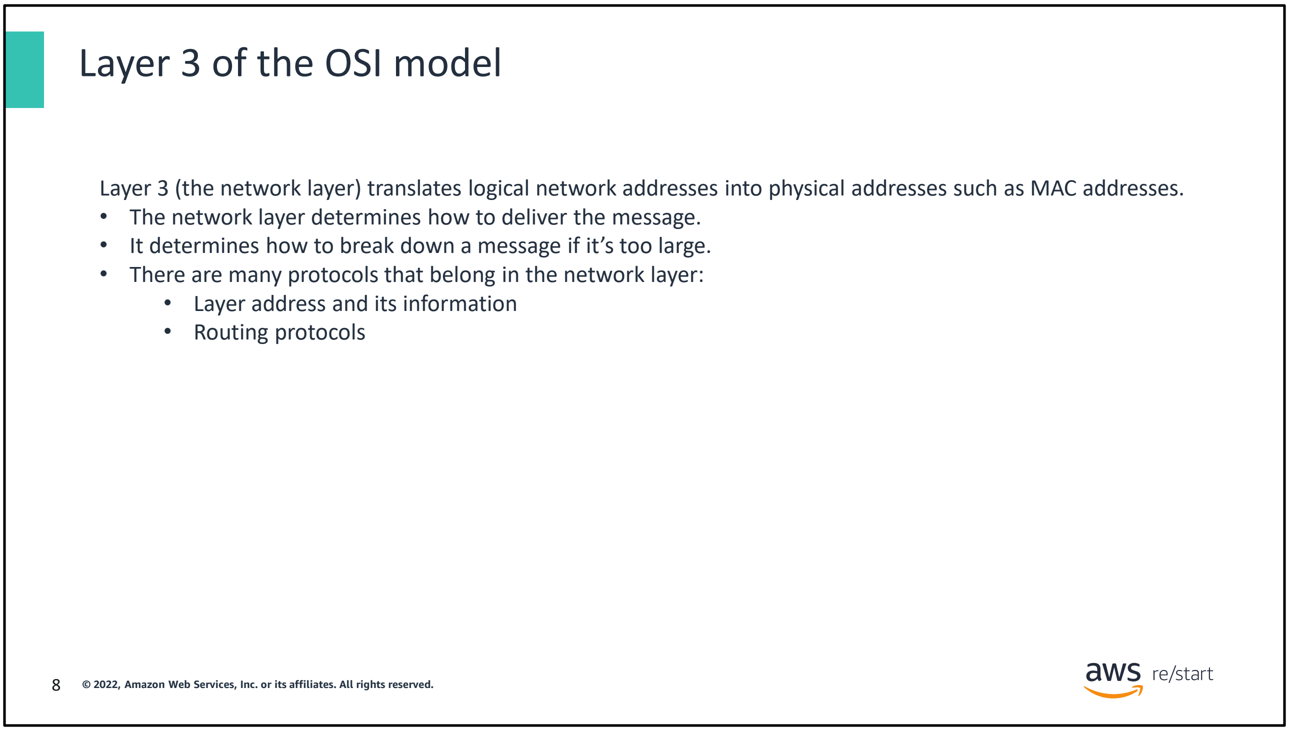
aws re/start

IP addresses:

- Work at layer 3 of the OSI model and is used to identify a host and a network.
- RFC 1918 provides a guide to private address space (https://datatracker.ietf.org/doc/html/rfc1918):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- **Why is this important for issues and troubleshooting?**
  - You might have experience **latency**, where a site or application is taking a long time to load, possibly to the point that it times out. In corporate settings, latency is a big deal, and finding out exactly where and what is causing it can save time and money. When troubleshooting latency, at layer 3, there is a command called **traceroute** where it provides a report on the path the packet takes from source to destination, each server is called a hop, and it checks for packet loss as well. This will be covered more in detail in a later module.
  - You might come across an issue where a server is **not responding to requests**, could it be layer 3 related? Or layer 4? Starting at the bottom and working your way up will assist in a solid troubleshooting method. Checking the Physical aspects first at layer 1 if possible, understanding what operates at layer 2, and working your way up to layer 3 IP addresses. An example of this is a server may not be responding because

it was assigned a dynamic IP address, even though layer 1 and layer 2 are fine, however, you will not be able to get past layer 3 because of a troubleshooting command called **ping**. This will be discussed in further detail in another module.

- Understanding how, where, and what works at each layer will assist you in troubleshooting basic networking issues.

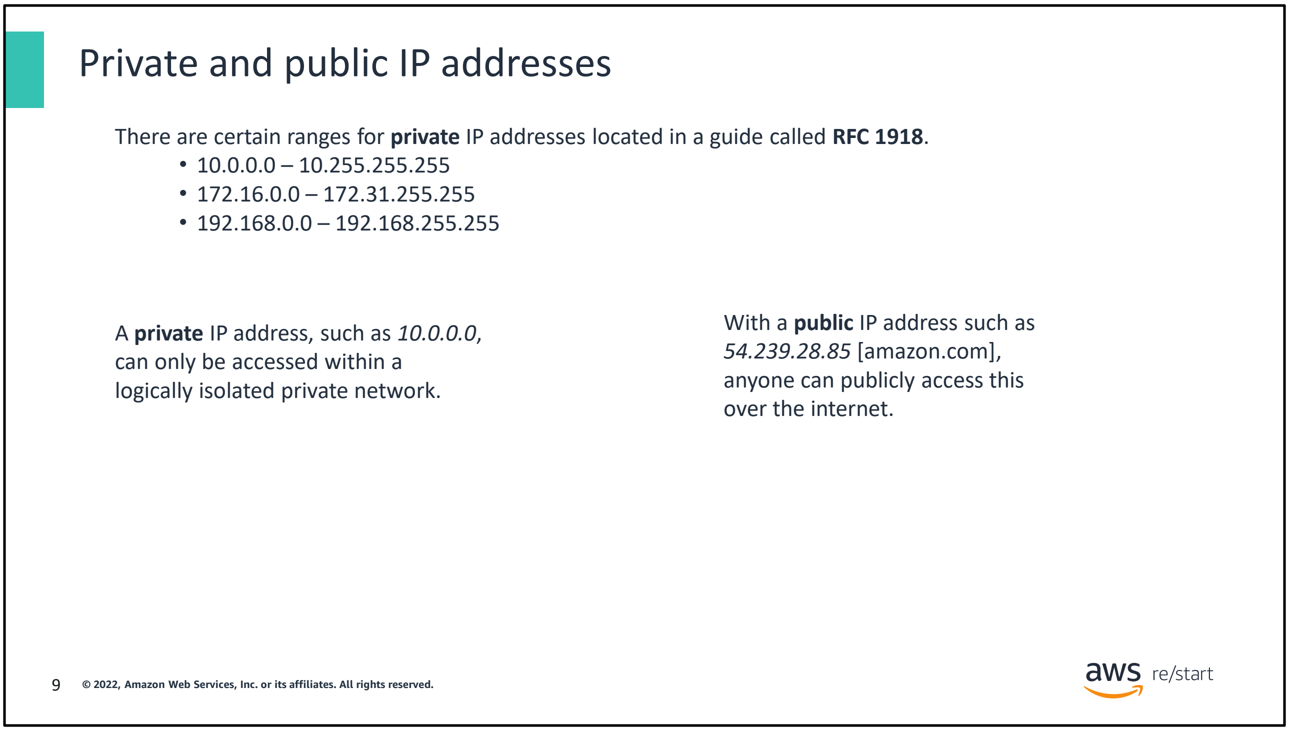


Layer 3 of the OSI model

Layer 3 (the network layer) translates logical network addresses into physical addresses such as MAC addresses.

- The network layer determines how to deliver the message.
- It determines how to break down a message if it’s too large.
- There are many protocols that belong in the network layer:
    - Layer address and its information
    - Routing protocols

- Why is it important?
    - Layer 2 (data link) establishes the connection between two nodes. These nodes have the physical components that use a MAC address. This needs to be translated to a logical address. At layer 3 (network), this translation between logical and physical takes place.
    - This is important to understand the differences of where MAC and IP addresses live and work when troubleshooting issues in the future.



Private and public IP addresses

There are certain ranges for **private** IP addresses located in a guide called **RFC 1918**.

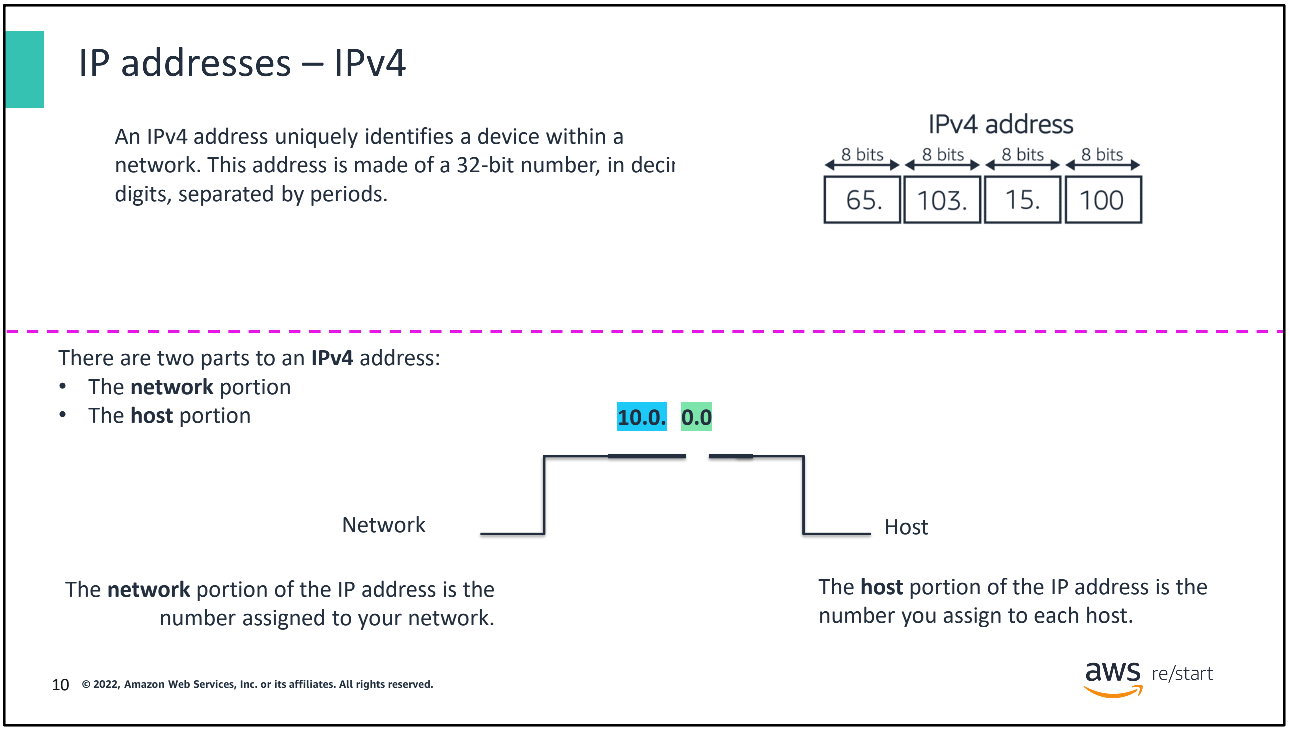
- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

A **private** IP address, such as *10.0.0.0*, can only be accessed within a logically isolated private network.

With a **public** IP address such as *54.239.28.85* [amazon.com], anyone can publicly access this over the internet.

IP addresses:

- Work at layer 3 of the OSI model and is used to identify a host and a network.
- RFC 1918 provides a guide to private address space (https://datatracker.ietf.org/doc/html/rfc1918):
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255



IP addresses – IPv4

An IPv4 address uniquely identifies a device within a network. This address is made of a 32-bit number, in deci digits, separated by periods.

IPv4 address

8 bits 8 bits 8 bits 8 bits

65. 103. 15. 100

There are two parts to an **IPv4** address:

- The **network** portion
- The **host** portion

10.0. 0.0

Network

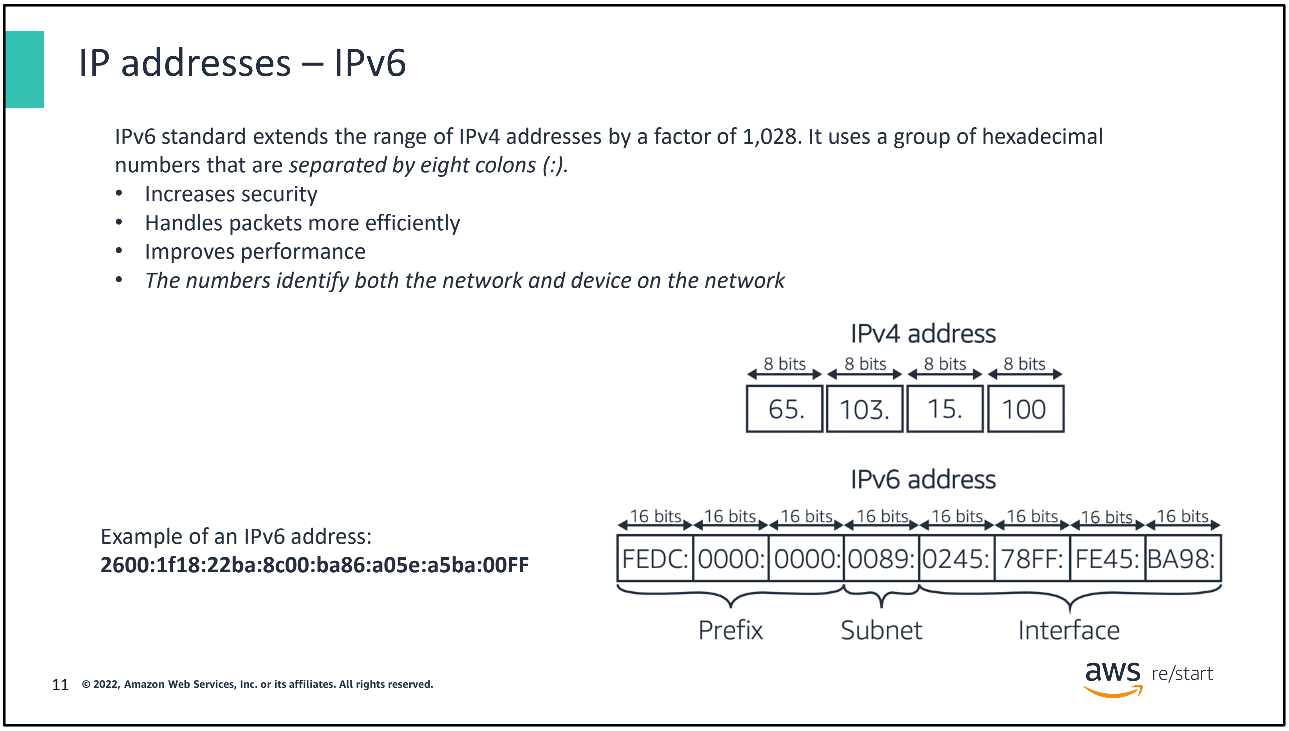
Host

The **network** portion of the IP address is the number assigned to your network.

The **host** portion of the IP address is the number you assign to each host.

IPv4 addresses:

- An IP address consists of *four numbers from 0 to 255 separated by a period*, which is also known as a *dotted quad* (for example, 10.15.200.0). This format follows the *IPv4 standard*. It is important to note that the numbers in the IP address *identify both the network and the device on the network*.
- An IP address is made of a 32-bit number, where each of the numbers between the dots is an 8-bit binary number. Thus, the entire address is a 32-bit binary number. For example:
    - An IP address of 10.100.20.5, the 10 is 8-bits, the 100 is 8-bits, the 20 is 8-bits, and the 5 is 8-bits totaling 32-bits (8x4).
    - Each *binary digit* or bit, has the value of *zero or one*. And has a separate decimal value.
- The network portion of the IP address is the number assigned to your network.
- The host portion of the IP address is the number you assign to each host.



IP addresses – IPv6

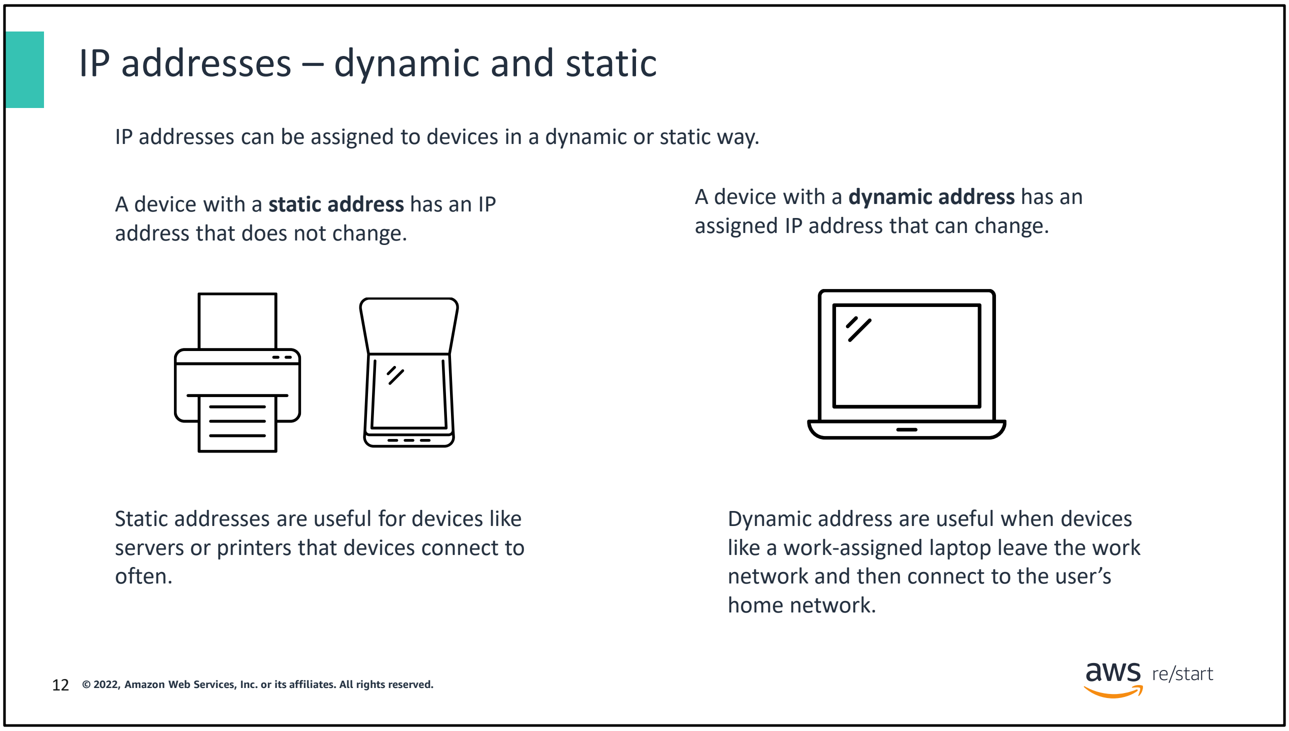
IPv6 standard extends the range of IPv4 addresses by a factor of 1,028. It uses a group of hexadecimal numbers that are *separated by eight colons (:).*

- Increases security
- Handles packets more efficiently
- Improves performance
- *The numbers identify both the network and device on the network*

Example of an IPv6 address:
2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

IPv6 addresses:

- The extra digits in IPv6 allow an expanded number of available addresses.
- Each decimal value now allows for 16 bits instead of the 8 bits that IPv4 provided.
- IPv4 provided an estimated 4.2 billion addresses, IPv6 provides around 340 trillion, trillion, trillion addresses to keep up with today’s growing list of internet of things (IoT) devices.



IP addresses – dynamic and static

IP addresses can be assigned to devices in a dynamic or static way.

A device with a **static address** has an IP address that does not change.

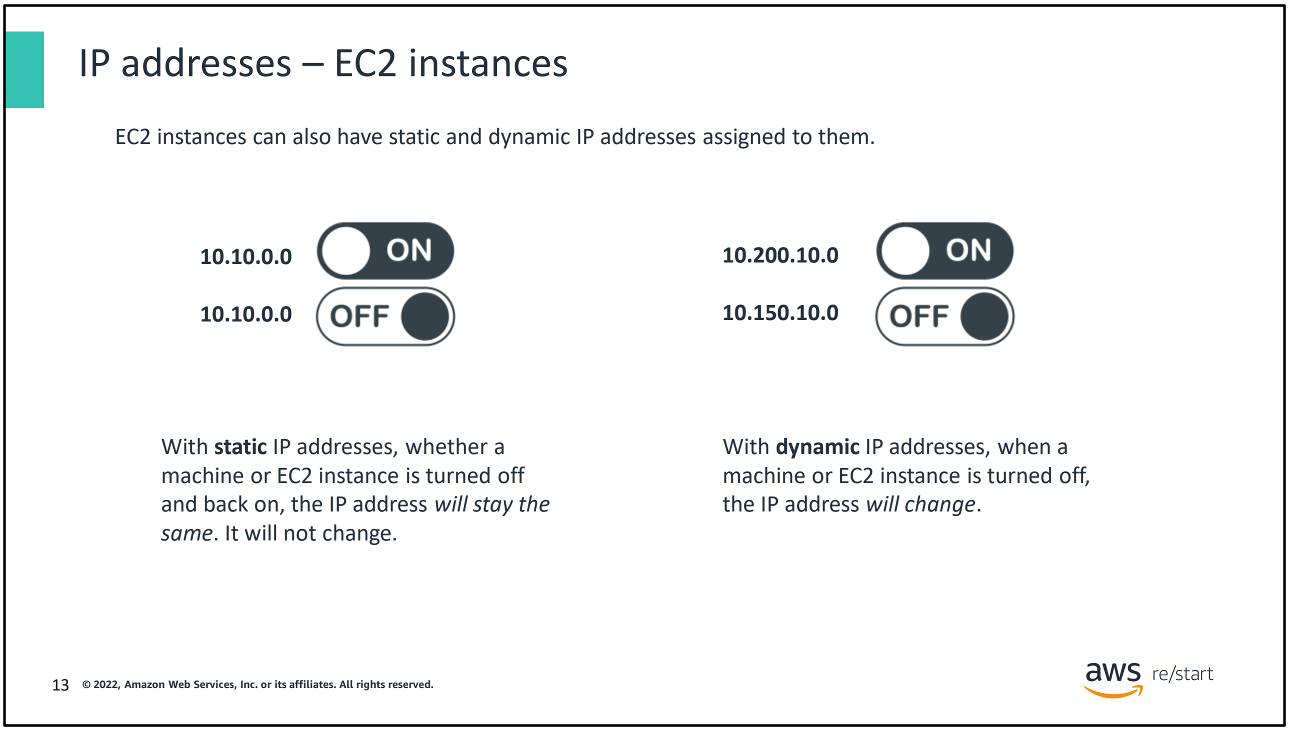
A device with a **dynamic address** has an assigned IP address that can change.

Static addresses are useful for devices like servers or printers that devices connect to often.

Dynamic address are useful when devices like a work-assigned laptop leave the work network and then connect to the user’s home network.

Dynamic and static IP addresses:

- Dynamic IP addresses can change. Useful for devices that leave and come back to a network.
- Static IP addresses cannot change. Useful for devices that are connected to often, like printers.



IP addresses – EC2 instances

EC2 instances can also have static and dynamic IP addresses assigned to them.

10.10.0.0 ON

10.10.0.0 OFF

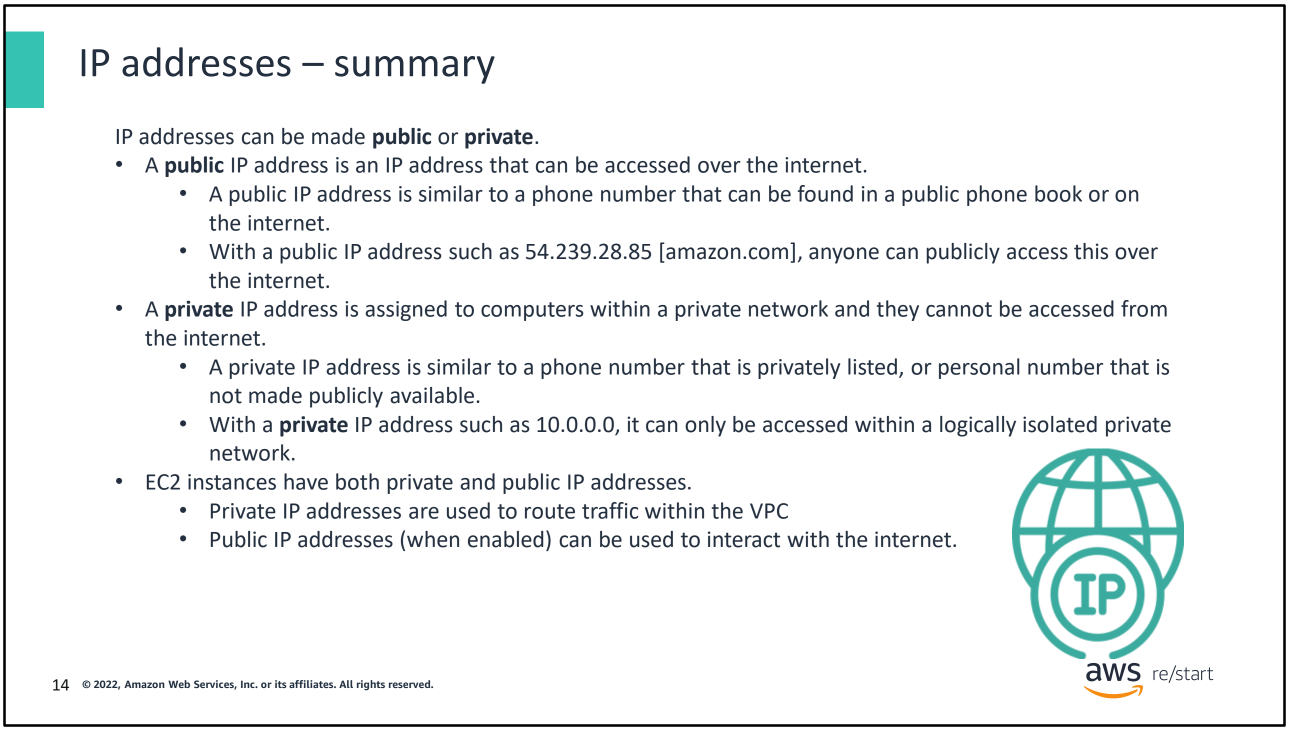
With **static** IP addresses, whether a machine or EC2 instance is turned off and back on, the IP address *will stay the same*. It will not change.

10.200.10.0 ON

10.150.10.0 OFF

With **dynamic** IP addresses, when a machine or EC2 instance is turned off, the IP address *will change*.

EC2 instances can be assigned a static or dynamic IP address depending on the use case. If the instance is used as a server, the best address to assign it is a static IP address, also known as an *Elastic IP address (EIP*). Otherwise, it will be assigned a dynamic IP address, when the instance is stopped and restarted, the IP address will change.



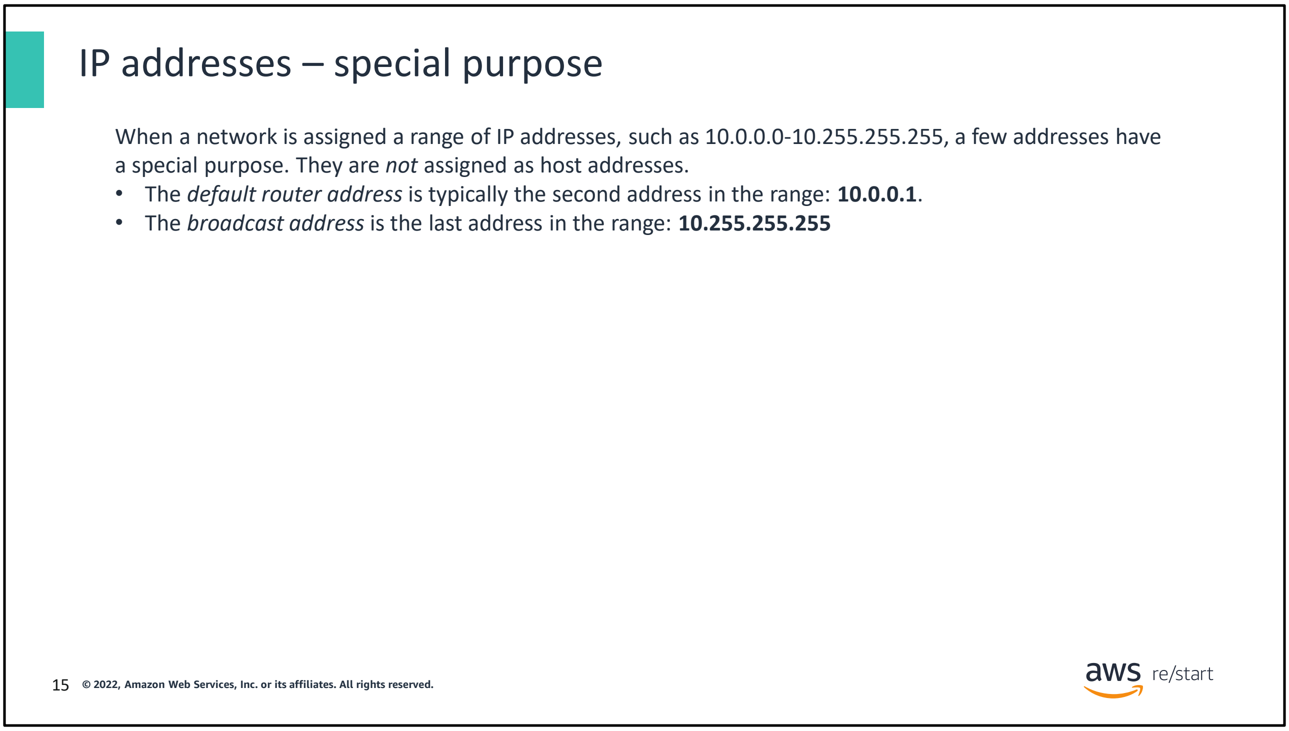
IP addresses – summary

IP addresses can be made **public** or **private**.

- A **public** IP address is an IP address that can be accessed over the internet.
  - A public IP address is similar to a phone number that can be found in a public phone book or on the internet.
  - With a public IP address such as 54.239.28.85 [amazon.com], anyone can publicly access this over the internet.
- A **private** IP address is assigned to computers within a private network and they cannot be accessed from the internet.
  - A private IP address is similar to a phone number that is privately listed, or personal number that is not made publicly available.
  - With a **private** IP address such as 10.0.0.0, it can only be accessed within a logically isolated private network.
- EC2 instances have both private and public IP addresses.
  - Private IP addresses are used to route traffic within the VPC
  - Public IP addresses (when enabled) can be used to interact with the internet.

Public or private IP addresses:

- Public IP address can be accessed over the internet. Its globally unique IP address that is assigned to a computing device that must access the internet.
- Private IP address cannot be accessed from the internet. Example: the application and database servers in your data center are assigned private IP addresses because you might not want other devices to know about these servers.



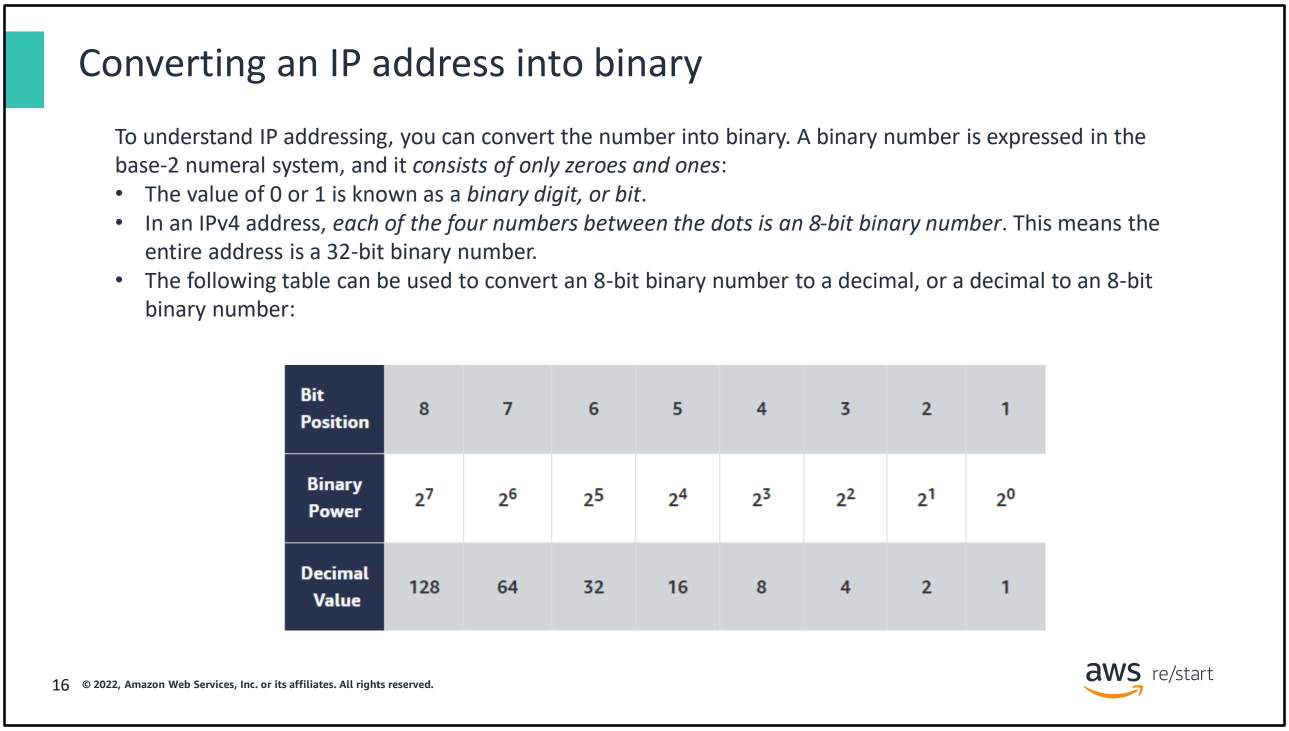
IP addresses – special purpose

When a network is assigned a range of IP addresses, such as 10.0.0.0-10.255.255.255, a few addresses have a special purpose. They are *not* assigned as host addresses.

- The *default router address* is typically the second address in the range: **10.0.0.1**.
- The *broadcast address* is the last address in the range: **10.255.255.255**

Special purpose IP addresses:

- The *default router address* is typically the second address, for example in the range of 10.0.0.0-10.255.255.255, *10.0.0.1* is the default router address.
    - Its also known as the *gateway address*
    - It's the IP address of the network router
- The *broadcast address* is the last address in the range: 10.255.255.255.
    - The broadcast address is used to transmit messages to all devices that are connected to a network. If a message is sent to a broadcast address, then all nodes on the network can receive it.



Converting an IP address into binary

To understand IP addressing, you can convert the number into binary. A binary number is expressed in the base-2 numeral system, and it *consists of only zeroes and ones*:

- The value of 0 or 1 is known as a *binary digit, or bit*.
- In an IPv4 address, *each of the four numbers between the dots is an 8-bit binary number*. This means the entire address is a 32-bit binary number.
- The following table can be used to convert an 8-bit binary number to a decimal, or a decimal to an 8-bit binary number:

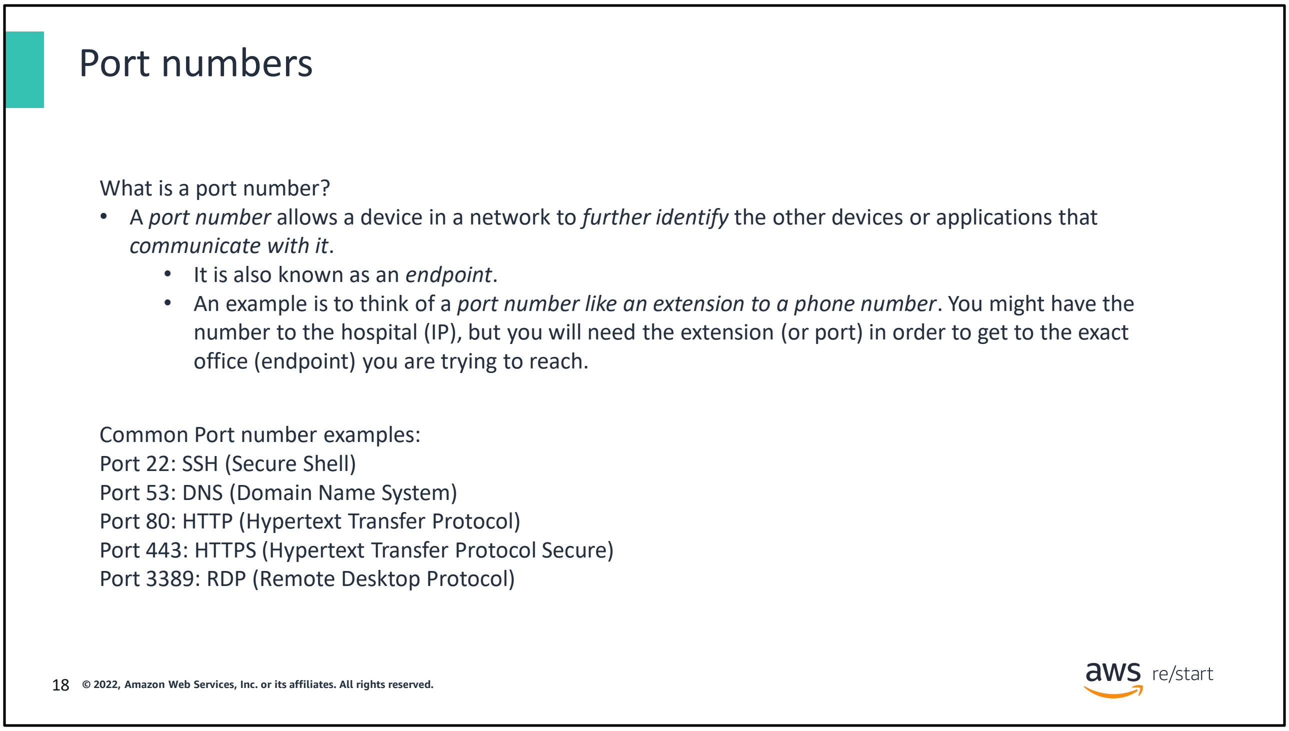
Bit Position	8	7	6	5	4	3	2	1
Binary Power	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Value	128	64	32	16	8	4	2	1

IPv4 addresses:

- An IP address consists of *four numbers from 0 to 255 separated by a period*, which is also known as a *dotted quad* (for example, 10.15.200.0). This format follows the *IPv4 standard*. It is important to note that the numbers in the IP address *identify both the network and the device on the network*.
- IP address identifies both the network and the device on the network
- The value of 0 or 1 is known as a binary digit or bit
- Each of the four numbers between the dots are 8-bit binary numbers, equaling 32-bits.
- This is the traditional theory to do so, however, **there are many webtools available to use in order to convert IP to binary and vice versa**. Many professionals use webtools today, but it is important to understand the basic theory as well. In your free time, explore the available webtools that can be found on the internet.

Port numbers

In this section, you will understand port numbers and their role in internet protocols.



Port numbers

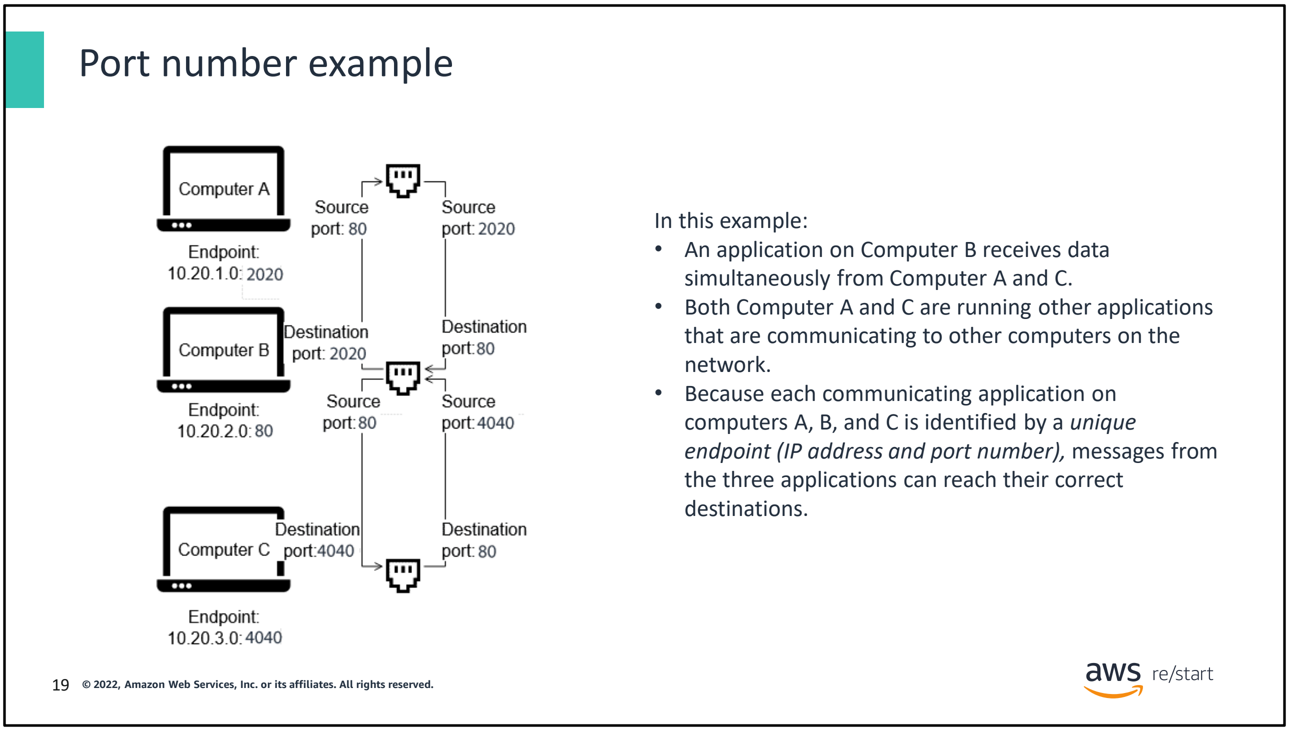
What is a port number?

- A *port number* allows a device in a network to *further identify* the other devices or applications that *communicate with it*.
  - It is also known as an *endpoint*.
  - An example is to think of a *port number like an extension to a phone number*. You might have the number to the hospital (IP), but you will need the extension (or port) in order to get to the exact office (endpoint) you are trying to reach.

Common Port number examples:
Port 22: SSH (Secure Shell)
Port 53: DNS (Domain Name System)
Port 80: HTTP (Hypertext Transfer Protocol)
Port 443: HTTPS (Hypertext Transfer Protocol Secure)
Port 3389: RDP (Remote Desktop Protocol)

Port numbers:

- A device might send or receive data from multiple devices at the same time. A port number, in combination with an IP address, enables the device to determine the exact source or destination of the data, which is also known as the *endpoint*.
- A computer can receive and send information in a similar way to the earlier phone example. It can enable multiple types of data to be sent to the same IP address, and still be parsed and acted on in separate and unique ways. This functionality enables a computer download a file over File Transfer Protocol (FTP) from an Amazon Simple Storage Service (Amazon S3) bucket, stream a live video from Twitch, and receive email messages – all at the same time.
- Common Port number examples:
  - Port 22: SSH – used to create a secure network connection
  - Port 53: DNS – used for the modern internet and Amazon uses it as a service Route53
  - Port 80: HTTP – protocol used to connect to a page like http://www.amazon.com
  - Port 443: HTTPS – A secure version of HTTP, used more for purchases and the need for secure sites. Such as https://www.amazon.com
  - Port 3389: RDP – With this protocol users can remotely connect to their desktop from another computer.

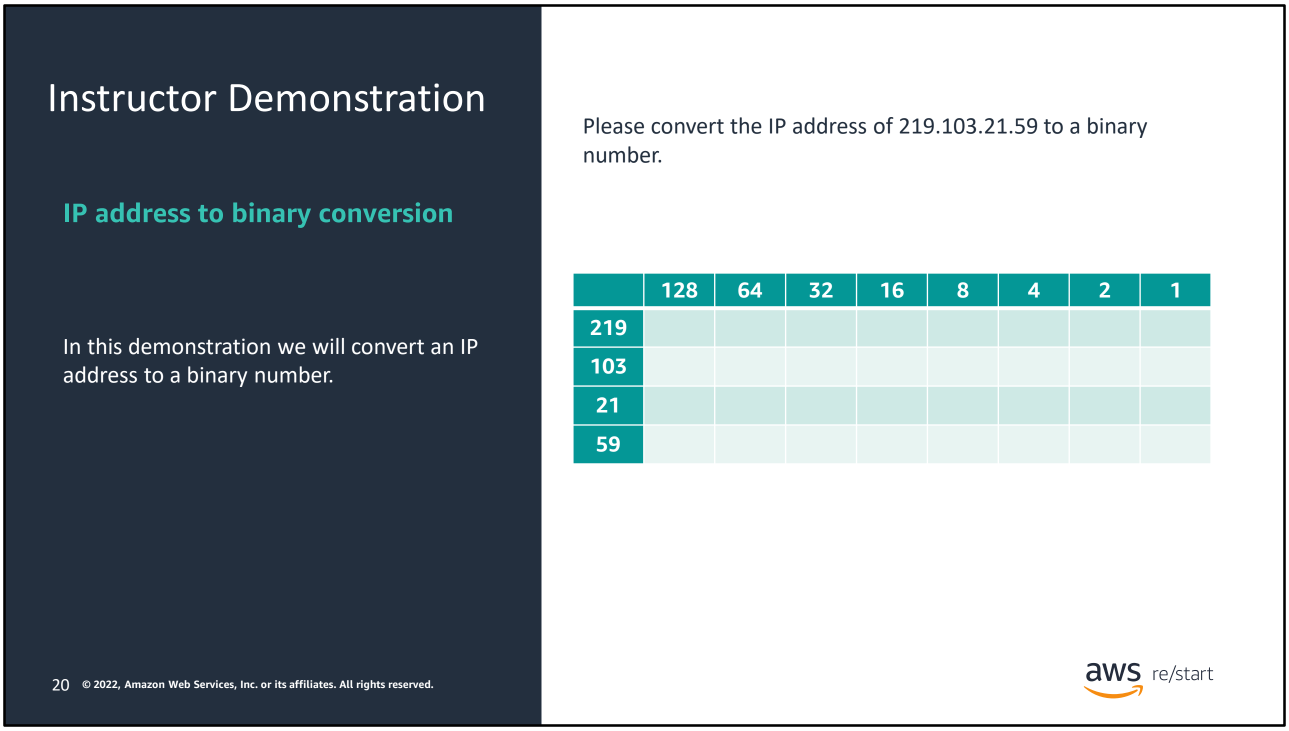


Port number example

In this example:

- An application on Computer B receives data simultaneously from Computer A and C.
- Both Computer A and C are running other applications that are communicating to other computers on the network.
- Because each communicating application on computers A, B, and C is identified by a *unique endpoint (IP address and port number),* messages from the three applications can reach their correct destinations.

- In the example above, port numbers and IP addresses work together to ensure that messages reach their correct destination.
- **Why is this important?**
  - When a port is blocked by a firewall, or if using a VPC it can be blocked by an AWS service like a Security Group or Network Access Control List, the source will not be able to send or receive traffic depending on the rules. Essentially ports can be blocked or allowed to certain traffic for security reasons.
  - When **troubleshooting issues, you can use commands such as netstat, ss, and telnet**. These commands are used at layer 4 of the OSI, but some can be used at layer 7. These will be covered more into detail in later sections.
  - The command **netstat** confirms established connections, so if a port is blocked, it will not show as a established connection.
  - The command **telnet** confirms TCP connections to a web server, note, that this can also be used at layer 7 in the OSI model
  - The command **ss** is very similar to netstat, however, it confirms IPv4 connections only.



Instructor Demonstration

IP address to binary conversion

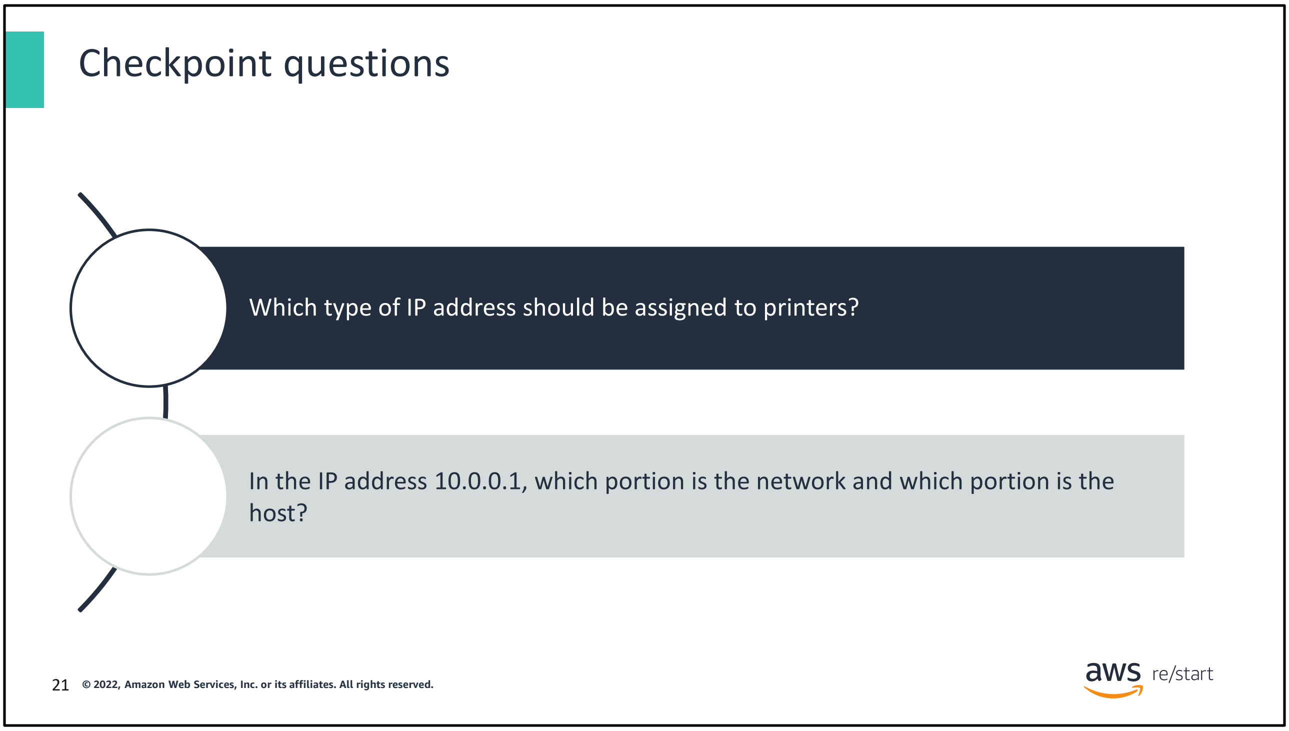
In this demonstration we will convert an IP address to a binary number.

Please convert the IP address of 219.103.21.59 to a binary number.

	128	64	32	16	8	4	2	1
219								
103								
21								
59								

The instructor will convert the IP address: **219.103.21.59** to binary.

- In binary, the IP address 219.103.21.59 converts to 11011011.0100111.00010101.00111011
- Remember that binary are zeroes and ones, they work like light switches where you turn them on and off.
- The ones you turn on (one) are the ones you use, the ones you turn off (zero) are the ones you don't use.



Checkpoint questions

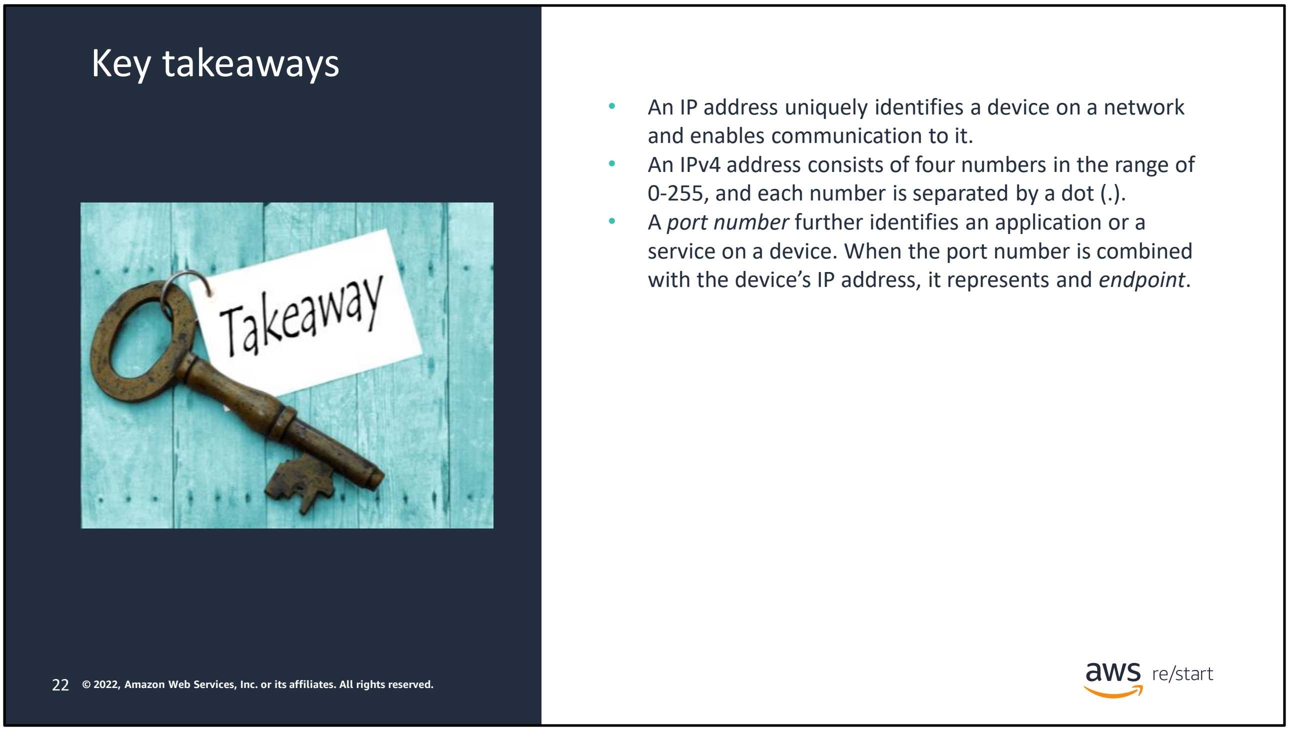
Which type of IP address should be assigned to printers?

In the IP address 10.0.0.1, which portion is the network and which portion is the host?

aws re/start

Q1:

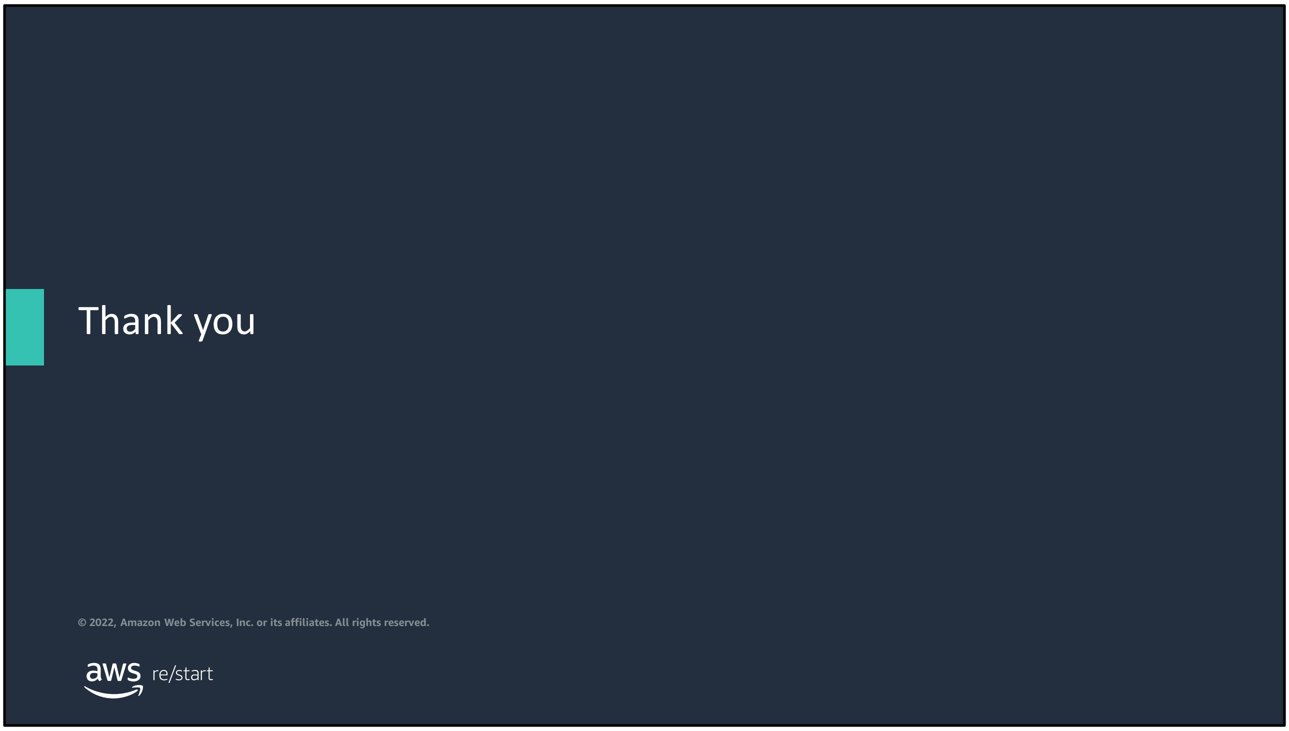
Q2: In the IP address 10.0.0.1, which portion is the network and which portion is the host?
10.0. is the network and 0.1 is the host.



Key takeaways

- An IP address uniquely identifies a device on a network and enables communication to it.
- An IPv4 address consists of four numbers in the range of 0-255, and each number is separated by a dot (.).
- A *port number* further identifies an application or a service on a device. When the port number is combined with the device's IP address, it represents and *endpoint*.

- An *IP address uniquely identifies* a device on a network and enables communication to it.
- An IPv4 address consists of four numbers in the range of 0-255, and each number is separated by a dot (.).
- A *port number* further identifies an application or a service on a device. When the port number is combined with the device's IP address, it represents and *endpoint*.



Thank you

Thank you.