Computación en Internet I

Andrés A. Aristizábal P.
aaaristizabal@icesi.edu.co

Departamento de Tecnologías de Información y Comunicaciones

2023-1

Agenda

1. **Addresses**
   - Introducing IP Addresses
   - Subnetting
   - Network Address Translation
2. **Workshop**

Agenda del día

1. **Addresses**
   - Introducing IP Addresses
   - Subnetting
   - Network Address Translation
2. **Workshop**

Introducing IP Addresses

What is an IP address?

Introducing IP Addresses

What is an IP address?

- It is a number that uniquely identifies every host on an IP network.

Introducing IP Addresses

What is an IP address?

- It is a number that uniquely identifies every host on an IP network.
- IP addresses operate at the network layer of the TCP/IP protocol stack.

Introducing IP Addresses

What is an IP address?

- It is a number that uniquely identifies every host on an IP network.
- IP addresses operate at the network layer of the TCP/IP protocol stack.
- They are independent of lower-level data link layer MAC addresses.

Introducing IP Addresses

What is an IP address?

- It is a number that uniquely identifies every host on an IP network.
- IP addresses operate at the network layer of the TCP/IP protocol stack.
- They are independent of lower-level data link layer MAC addresses.
- They are 32-bit binary numbers (IPv4).

What is the Internet Protocol main purpose?

What is the Internet Protocol main purpose?

- To enable communications between networks.

Introducing IP Addresses

What is the Internet Protocol main purpose?

- To enable communications between networks.
- As a result, a 32-bit IP address actually consists of two parts:
  - *The network ID* (or network address) which identifies the network on which a host computer can be found.
  - *The host ID* (or host address) which identifies a specific device on the network indicated by the network ID.

Introducing IP Addresses

What is the Internet Protocol main purpose?

- To enable communications between networks.
- As a result, a 32-bit IP address actually consists of two parts:
  - *The network ID* (or network address) which identifies the network on which a host computer can be found.
  - *The host ID* (or host address) which identifies a specific device on the network indicated by the network ID.

What is most of the complexity of working with IP addresses?

Introducing IP Addresses

What is the Internet Protocol main purpose?

- To enable communications between networks.
- As a result, a 32-bit IP address actually consists of two parts:
  - *The network ID* (or network address) which identifies the network on which a host computer can be found.
  - *The host ID* (or host address) which identifies a specific device on the network indicated by the network ID.

What is most of the complexity of working with IP addresses?

- Figuring out which part of the complete 32-bit IP address is the network ID and which part is the host ID.

What is the dotted-decimal notation?

What is the dotted-decimal notation?

- The format in which IP addresses are usually represented.

What is the dotted-decimal notation?

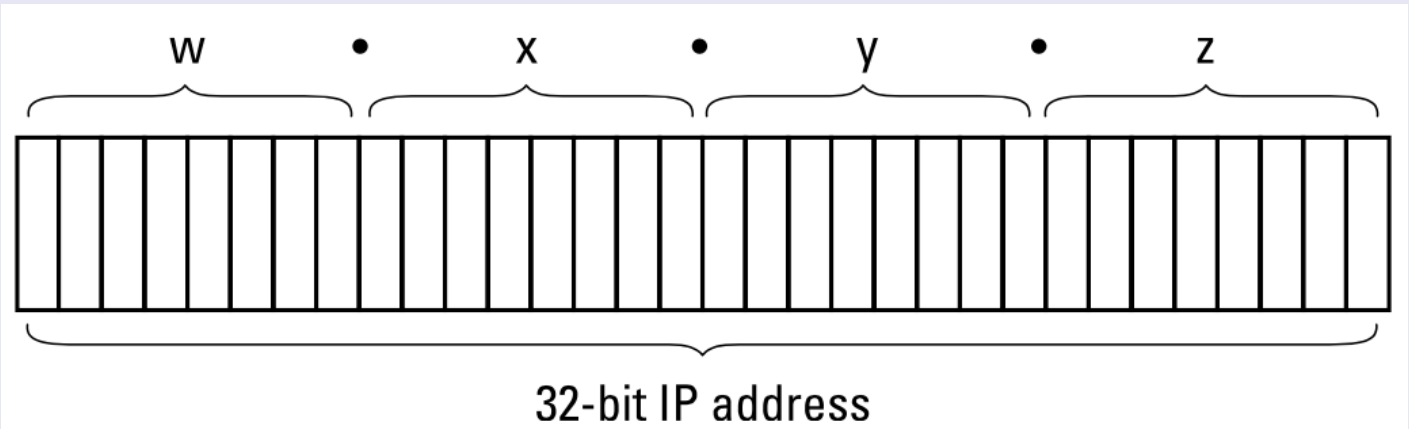
- The format in which IP addresses are usually represented.
- In dotted-decimal notation, each group of eight bits (an octet) is represented by its decimal equivalent.

What is the dotted-decimal notation?

- The format in which IP addresses are usually represented.
- In dotted-decimal notation, each group of eight bits (an octet) is represented by its decimal equivalent.
  - *The network ID* (or network address) which identifies the network on which a host computer can be found.
  - *The host ID* (or host address) which identifies a specific device on the network indicated by the network ID.

What is the dotted-decimal notation?

- The format in which IP addresses are usually represented.
- In dotted-decimal notation, each group of eight bits (an octet) is represented by its decimal equivalent.
  - *The network ID* (or network address) which identifies the network on which a host computer can be found.
  - *The host ID* (or host address) which identifies a specific device on the network indicated by the network ID.



Classifying IP Addresses

Which are the IP address classes?

Classifying IP Addresses

Which are the IP address classes?

- The IP protocol defines five different address classes: A, B, C, D, and E.

Classifying IP Addresses

Which are the IP address classes?

- The IP protocol defines five different address classes: A, B, C, D, and E.
- Each of the first three classes, uses a different size for the network ID and host ID portion of the address.

Classifying IP Addresses

Which are the IP address classes?

- The IP protocol defines five different address classes: A, B, C, D, and E.
- Each of the first three classes, uses a different size for the network ID and host ID portion of the address.
- Class D is for a special type of address called a multicast address.

Classifying IP Addresses

Which are the IP address classes?

- The IP protocol defines five different address classes: A, B, C, D, and E.
- Each of the first three classes, uses a different size for the network ID and host ID portion of the address.
- Class D is for a special type of address called a multicast address.
- Class E is an experimental address class that isn't used.

Classifying IP Addresses

How to determine into which class a particular address fits?

Classifying IP Addresses

How to determine into which class a particular address fits?

- Class A: The first bit is zero.

Classifying IP Addresses

How to determine into which class a particular address fits?

- Class A: The first bit is zero.
- Class B: The first bit is one, and the second bit is zero.

Classifying IP Addresses

How to determine into which class a particular address fits?

- Class A: The first bit is zero.
- Class B: The first bit is one, and the second bit is zero.
- Class C: The first two bits are both one, and the third bit is zero.

Classifying IP Addresses

How to determine into which class a particular address fits?

- Class A: The first bit is zero.
- Class B: The first bit is one, and the second bit is zero.
- Class C: The first two bits are both one, and the third bit is zero.
- Class D: The first three bits are all one, and the fourth bit is zero.

Classifying IP Addresses

How to determine into which class a particular address fits?

- Class A: The first bit is zero.
- Class B: The first bit is one, and the second bit is zero.
- Class C: The first two bits are both one, and the third bit is zero.
- Class D: The first three bits are all one, and the fourth bit is zero.
- Class E: The first four bits are all one.

Classifying IP Addresses

Which are the details of the first three classes?

Classifying IP Addresses

Which are the details of the first three classes?

Class	Address Number Range	Starting Bits	Length of Network ID	Number of Networks	Hosts
A	1–126.*x.y.z*	0	8	126	16,777,214
B	128–191.*x.y.z*	10	16	16,384	65,534
C	192–223.*x.y.z*	110	24	2,097,152	254

Classifying IP Addresses

Class address A

Classifying IP Addresses

Class address A

- Designed for very large networks.

Classifying IP Addresses

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.

Classifying IP Addresses

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.
- The remaining three octets are the host ID.

Classifying IP Addresses

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.
- The remaining three octets are the host ID.
- Only 126 Class A networks can exist in the entire Internet.

Classifying IP Addresses

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.
- The remaining three octets are the host ID.
- Only 126 Class A networks can exist in the entire Internet.
- Each network can accommodate more than 16 million hosts.

Classifying IP Addresses

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.
- The remaining three octets are the host ID.
- Only 126 Class A networks can exist in the entire Internet.
- Each network can accommodate more than 16 million hosts.
- Only about 40 Class A addresses are actually assigned to companies or organizations.

Class address A

- Designed for very large networks.
- The first octet of the address is the network ID.
- The remaining three octets are the host ID.
- Only 126 Class A networks can exist in the entire Internet.
- Each network can accommodate more than 16 million hosts.
- Only about 40 Class A addresses are actually assigned to companies or organizations.
- The rest are either reserved for use by the Internet Assigned Numbers Authority (IANA) or are assigned to organizations that manage IP assignments for geographic regions such as Europe, Asia, and Latin America.

Classifying IP Addresses

Class address B

Class address B

- The first two octets of the IP address are used as the network ID.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.
- A total of 16,384 Class B networks can exist.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.
- A total of 16,384 Class B networks can exist.
- Can accommodate more than 65,000 hosts.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.
- A total of 16,384 Class B networks can exist.
- Can accommodate more than 65,000 hosts.
- The problem is that even though they are much smaller than Class A networks, they still allocate far too many host IDs.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.
- A total of 16,384 Class B networks can exist.
- Can accommodate more than 65,000 hosts.
- The problem is that even though they are much smaller than Class A networks, they still allocate far too many host IDs.
- Very few networks have tens of thousands of hosts.

Class address B

- The first two octets of the IP address are used as the network ID.
- The second two octets are used as the host ID.
- A total of 16,384 Class B networks can exist.
- Can accommodate more than 65,000 hosts.
- The problem is that even though they are much smaller than Class A networks, they still allocate far too many host IDs.
- Very few networks have tens of thousands of hosts.
- Careless assignment of Class B addresses can lead to a large percentage of the available host addresses being wasted.

Classifying IP Addresses

Class address C

Classifying IP Addresses

Class address C

- The first three octets are used for the network ID.

Classifying IP Addresses

Class address C

- The first three octets are used for the network ID.
- The fourth octet is used for the host ID.

Classifying IP Addresses

Class address C

- The first three octets are used for the network ID.
- The fourth octet is used for the host ID.
- Can accommodate only 254 hosts.

Classifying IP Addresses

Class address C

- The first three octets are used for the network ID.
- The fourth octet is used for the host ID.
- Can accommodate only 254 hosts.
- Allow for more than 2 million networks.

Classifying IP Addresses

Class address C

- The first three octets are used for the network ID.
- The fourth octet is used for the host ID.
- Can accommodate only 254 hosts.
- Allow for more than 2 million networks.
- The problem is that they're too small.

Agenda del día

1. **Addresses**
   - Introducing IP Addresses
   - Subnetting
   - Network Address Translation
2. **Workshop**

What is subnetting?

Subnetting

What is subnetting?

- A technique that lets network administrators use the 32 bits available in an IP address more efficiently.

Subnetting

What is subnetting?

- A technique that lets network administrators use the 32 bits available in an IP address more efficiently.
- Done by creating networks that aren't limited to the scales provided by Class A, B, and C IP addresses.

Subnetting

What is subnetting?

- A technique that lets network administrators use the 32 bits available in an IP address more efficiently.
- Done by creating networks that aren't limited to the scales provided by Class A, B, and C IP addresses.
- Networks with more realistic host limits can be created.

How does it work?

Subnetting

How does it work?

- Provides a more flexible way to designate which portion of an IP address represents the network ID and which portion represents the host ID.

How does it work?

- Provides a more flexible way to designate which portion of an IP address represents the network ID and which portion represents the host ID.
- With standard IP address classes, only three possible network ID sizes exist:
  - 8 bits for Class A.
  - 16 bits for Class B.
  - 24 bits for Class C.

How does it work?

- Provides a more flexible way to designate which portion of an IP address represents the network ID and which portion represents the host ID.
- With standard IP address classes, only three possible network ID sizes exist:
  - 8 bits for Class A.
  - 16 bits for Class B.
  - 24 bits for Class C.
- An arbitrary number of bits to use for the network ID can be selected.

What are the reasons for using subnetting?

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.
- The second one is that even if a single organization has thousands of network devices, operating all those devices with the same network ID would slow the network to a crawl.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.
- The second one is that even if a single organization has thousands of network devices, operating all those devices with the same network ID would slow the network to a crawl.
- The way TCP/IP works dictates that all the computers with the same network ID must be on the same physical network.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.
- The second one is that even if a single organization has thousands of network devices, operating all those devices with the same network ID would slow the network to a crawl.
- The way TCP/IP works dictates that all the computers with the same network ID must be on the same physical network.
- The physical network comprises a single broadcast domain.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.
- The second one is that even if a single organization has thousands of network devices, operating all those devices with the same network ID would slow the network to a crawl.
- The way TCP/IP works dictates that all the computers with the same network ID must be on the same physical network.
- The physical network comprises a single broadcast domain.
- This means that a single network medium must carry all the traffic for the network.

What are the reasons for using subnetting?

- Two reasons compel people to use subnetting.
- The first is to allocate the limited IP address space more efficiently.
- The second one is that even if a single organization has thousands of network devices, operating all those devices with the same network ID would slow the network to a crawl.
- The way TCP/IP works dictates that all the computers with the same network ID must be on the same physical network.
- The physical network comprises a single broadcast domain.
- This means that a single network medium must carry all the traffic for the network.
- For performance reasons, networks are usually segmented into broadcast domains that are smaller than even Class C addresses provide.

What is a subnet?

What is a subnet?

- A network that falls within a Class A, B, or C network.

What is a subnet?

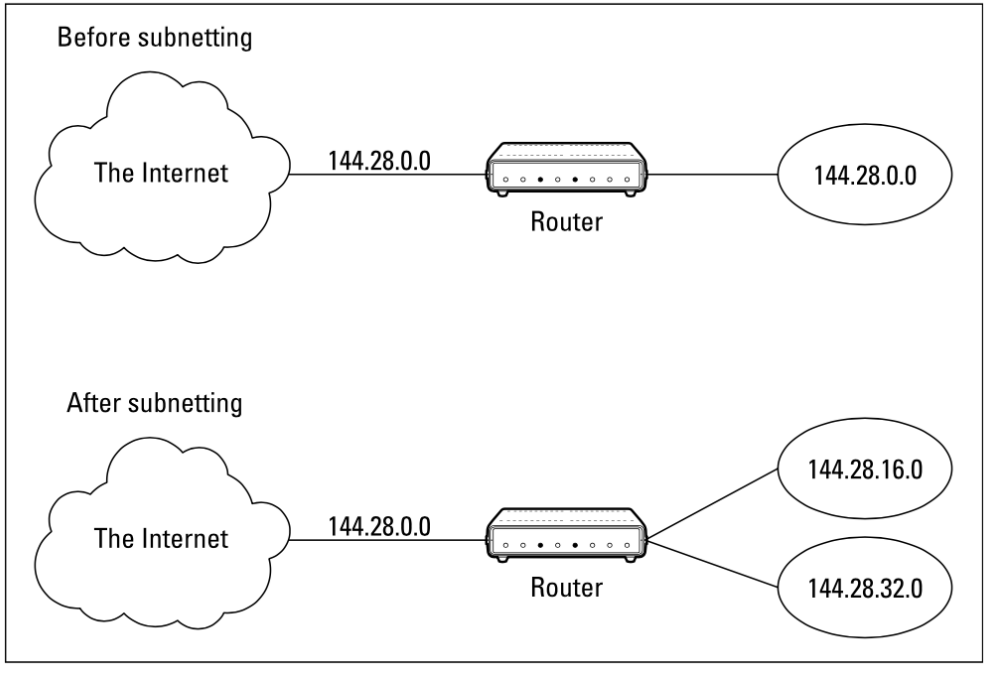
- A network that falls within a Class A, B, or C network.
- Created by using one or more of the Class A, B, or C host bits to extend the network ID.

What is a subnet?

- A network that falls within a Class A, B, or C network.
- Created by using one or more of the Class A, B, or C host bits to extend the network ID.
- Instead of the standard 8-, 16-, or 24-bit network ID, subnets can have network IDs of any length.

What is a subnet?

- A network that falls within a Class A, B, or C network.
- Created by using one or more of the Class A, B, or C host bits to extend the network ID.
- Instead of the standard 8-, 16-, or 24-bit network ID, subnets can have network IDs of any length.



What is a subnet mask?

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.
- Those bits that represent the host ID appear as a 0 in the mask.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.
- Those bits that represent the host ID appear as a 0 in the mask.
- A subnet mask always has a consecutive string of ones on the left, followed by a string of zeros.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.
- Those bits that represent the host ID appear as a 0 in the mask.
- A subnet mask always has a consecutive string of ones on the left, followed by a string of zeros.
- The subnet mask itself is usually represented in dotted-decimal notation.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.
- Those bits that represent the host ID appear as a 0 in the mask.
- A subnet mask always has a consecutive string of ones on the left, followed by a string of zeros.
- The subnet mask itself is usually represented in dotted-decimal notation.
- It doesn't represent any device or network on the Internet.

What is a subnet mask?

- For subnetting to work, the router must be told which portion of the host ID should be used for the subnet network ID.
- This is accomplished by using another 32-bit number, known as a subnet mask.
- Those IP address bits that represent the network ID are represented by a 1 in the mask.
- Those bits that represent the host ID appear as a 0 in the mask.
- A subnet mask always has a consecutive string of ones on the left, followed by a string of zeros.
- The subnet mask itself is usually represented in dotted-decimal notation.
- It doesn't represent any device or network on the Internet.
- It is way of indicating which portion of an IP address should be used to determine the network ID.

How to determine the network ID of an IP address?

How to determine the network ID of an IP address?

- The router must have both the IP address and the subnet mask.

How to determine the network ID of an IP address?

- The router must have both the IP address and the subnet mask.
- The router then performs a bitwise operation called a logical AND on the IP address in order to extract the network ID.

How to determine the network ID of an IP address?

- The router must have both the IP address and the subnet mask.
- The router then performs a bitwise operation called a logical AND on the IP address in order to extract the network ID.

```
144 . 28 . 16 . 17
IP address: 10010000 00011100 00010000 00010001
Subnet mask: 11111111 11111111 11110000 00000000
Network ID: 10010000 00011100 00010000 00000000
 144  .  28 . 16 . 0
```

What is the network prefix notation?

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.
- The network prefix is indicated with a slash immediately after the IP address.

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.
- The network prefix is indicated with a slash immediately after the IP address.
- Is followed by the number of network ID bits to use.

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.
- The network prefix is indicated with a slash immediately after the IP address.
- Is followed by the number of network ID bits to use.
- Network prefix notation is also called classless interdomain routing notation (CIDR).

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.
- The network prefix is indicated with a slash immediately after the IP address.
- Is followed by the number of network ID bits to use.
- Network prefix notation is also called classless interdomain routing notation (CIDR).
- It provides a way of indicating which portion of an address is the network ID and which is the host ID without relying on standard address classes.

What is the network prefix notation?

- Since a subnet mask always begins with a consecutive sequence of ones to indicate which bits to use for the network ID.
  - A shorthand notation (a network prefix) to indicate how many bits of an IP address represent the network ID can be used.
- The network prefix is indicated with a slash immediately after the IP address.
- Is followed by the number of network ID bits to use.
- Network prefix notation is also called classless interdomain routing notation (CIDR).
- It provides a way of indicating which portion of an address is the network ID and which is the host ID without relying on standard address classes.
- The IP address 144.28.16.17 with the subnet mask 255.255.240.0 can be represented as 144.28.16.17/20.

What are the default subnets?

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- A subnet mask is not actually required to use one of these defaults.

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- A subnet mask is not actually required to use one of these defaults.
- The IP address class can be determined by examining the first three bits of the IP address.

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- A subnet mask is not actually required to use one of these defaults.
- The IP address class can be determined by examining the first three bits of the IP address.
- If the first bit is 0, the address is Class A, and the subnet mask 255.0.0 is applied.

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- A subnet mask is not actually required to use one of these defaults.
- The IP address class can be determined by examining the first three bits of the IP address.
- If the first bit is 0, the address is Class A, and the subnet mask 255.0.0 is applied.
- If the first two bits are 10, the address is Class B, and 255.255.0.0 is used.

What are the default subnets?

Class	Binary	Dotted-Decimal	Network Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

- A subnet mask is not actually required to use one of these defaults.
- The IP address class can be determined by examining the first three bits of the IP address.
- If the first bit is 0, the address is Class A, and the subnet mask 255.0.0 is applied.
- If the first two bits are 10, the address is Class B, and 255.255.0.0 is used.
- If the first three bits are 110, the Class C default mask 255.255.255.0 is used.

Which are some additional restrictions that are placed on subnets and subnet masks?

Which are some additional restrictions that are placed on subnets and subnet masks?

- The minimum number of network ID bits is eight.
  - As a result, the first octet of a subnet mask is always 255.

Which are some additional restrictions that are placed on subnets and subnet masks?

- The minimum number of network ID bits is eight.
  - As a result, the first octet of a subnet mask is always 255.
- The maximum number of network ID bits is 30.
  - At least two bits for the host ID portion of the address to allow for at least two hosts.

Which are some additional restrictions that are placed on subnets and subnet masks?

- The minimum number of network ID bits is eight.
  - As a result, the first octet of a subnet mask is always 255.
- The maximum number of network ID bits is 30.
  - At least two bits for the host ID portion of the address to allow for at least two hosts.
- The network ID portion of a subnet mask is always composed of consecutive bits set to 1.
  - Only eight values are possible for each octet of a subnet mask: 0, 128, 192, 224, 248, 252, 254, and 255.

Which are some additional restrictions that are placed on subnets and subnet masks?

- The minimum number of network ID bits is eight.
  - As a result, the first octet of a subnet mask is always 255.
- The maximum number of network ID bits is 30.
  - At least two bits for the host ID portion of the address to allow for at least two hosts.
- The network ID portion of a subnet mask is always composed of consecutive bits set to 1.
  - Only eight values are possible for each octet of a subnet mask: 0, 128, 192, 224, 248, 252, 254, and 255.
- A subnet address can't be all zeros or all ones.

How can a subnet be thought of?

How can a subnet be thought of?

- As a range or block of IP addresses that have a common network ID.

How can a subnet be thought of?

- As a range or block of IP addresses that have a common network ID.
- For example, the CIDR 192.168.1.0/28 represents the following block of 14 IP addresses:

```
192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4
192.168.1.5 192.168.1.6 192.168.1.7 192.168.1.8
192.168.1.9 192.168.1.10 192.168.1.11 192.168.1.12
192.168.1.13 192.168.1.14
```

How to determine the range of actual IP addresses that the CIDR represents?

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.
- Determine how many host IDs are allowed based on the size of the network ID and count them off.

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.
- Determine how many host IDs are allowed based on the size of the network ID and count them off.
- When the octet where the network ID mask ends is not 0 the calculation is a little harder.

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.
- Determine how many host IDs are allowed based on the size of the network ID and count them off.
- When the octet where the network ID mask ends is not 0 the calculation is a little harder.
- The first step is to determine the actual network ID.

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.
- Determine how many host IDs are allowed based on the size of the network ID and count them off.
- When the octet where the network ID mask ends is not 0 the calculation is a little harder.
- The first step is to determine the actual network ID.
- Determine the number of allowable hosts in the subnet based on the network prefix.
  - Calculated by subtracting the last octet of the subnet mask from 254.

How to determine the range of actual IP addresses that the CIDR represents?

- Straightforward when the octet within which the network ID mask ends happens to be 0.
- Determine how many host IDs are allowed based on the size of the network ID and count them off.
- When the octet where the network ID mask ends is not 0 the calculation is a little harder.
- The first step is to determine the actual network ID.
- Determine the number of allowable hosts in the subnet based on the network prefix.
  - Calculated by subtracting the last octet of the subnet mask from 254.
  - To determine the first IP address in the block, 1 has to be added the network ID.

What about an example?

What about an example?

- Take the CIDR 192.168.1.0/28.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.
- The size of the network id is 28.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.
- The size of the network id is 28.
- Therefore 32-28 = 4.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.
- The size of the network id is 28.
- Therefore 32-28 = 4.
- $2^4 = 16$.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.
- The size of the network id is 28.
- Therefore 32-28 = 4.
- $2^4 = 16$.
- Since the host ID can't be 0 (reserved to represent the network itself) nor 255 (reserved for use as a broadcast request that's intended for all hosts on the network) 16-2 = 14.

What about an example?

- Take the CIDR 192.168.1.0/28.
- Clearly the octet within which the network ID mask ends is 0.
- The size of the network id is 28.
- Therefore 32-28 = 4.
- $2^4 = 16$.
- Since the host ID can't be 0 (reserved to represent the network itself) nor 255 (reserved for use as a broadcast request that's intended for all hosts on the network) 16-2 = 14.
- 192.168.1.1, 92.168.1.2, 92.168.1.3, 92.168.1.4, 192.168.1.5, 92.168.1.6, 92.168.1.7, 92.168.1.8, 92.168.1.9, 92.168.1.10, 92.168.1.11, 192.168.1.5, 92.168.1.12, 92.168.1.3, 92.168.1.13, 92.168.1.14

Another example?

Another example?

- Take the IP address192.168.1.100 when the subnet mask is 255.255.255.240.

Another example?

- Take the IP address192.168.1.100 when the subnet mask is 255.255.255.240.
- Determine the network ID.

Another example?

- Take the IP address192.168.1.100 when the subnet mask is 255.255.255.240.
- Determine the network ID.
  - 11000000 10101000 00000001 01100100
  - AND
  - 11111111 11111111 11111111 11110000
  - = 11000000 10101000 00000001 01100000
  - = 192.168.1.96

Another example?

- Take the IP address192.168.1.100 when the subnet mask is 255.255.255.240.
- Determine the network ID.
  - 11000000 10101000 00000001 01100100
  - AND
  - 11111111 11111111 11111111 11110000
  - = 11000000 10101000 00000001 01100000
  - = 192.168.1.96
- Subtracting the last octet of the subnet mask from 254, 254 - 240 = 14.

Another example?

- Take the IP address192.168.1.100 when the subnet mask is 255.255.255.240.
- Determine the network ID.
  - 11000000 10101000 00000001 01100100
  - AND
  - 11111111 11111111 11111111 11110000
  - = 11000000 10101000 00000001 01100000
  - = 192.168.1.96
- Subtracting the last octet of the subnet mask from 254, 254 - 240 = 14.
- 192.168.1.97, 192.168.1.98, 192.168.1.99, 192.168.1.100, 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104, 192.168.1.105, 192.168.1.106, 192.168.1.107, 192.168.1.108, 192.168.1.109, 192.168.1.110

What about private and public addresses?

What about private and public addresses?

- Any host with a direct connection to the Internet must have a globally unique IP address.

What about private and public addresses?

- Any host with a direct connection to the Internet must have a globally unique IP address.
- Not all hosts are connected directly to the Internet.
  - Some are on networks that aren't connected to the Internet.
  - Some hosts are hidden behind firewalls, so their Internet connection is indirect.

What about private and public addresses?

- Any host with a direct connection to the Internet must have a globally unique IP address.
- Not all hosts are connected directly to the Internet.
  - Some are on networks that aren't connected to the Internet.
  - Some hosts are hidden behind firewalls, so their Internet connection is indirect.
- Several blocks of IP addresses are set aside just for this purpose.

What about private and public addresses?

- Any host with a direct connection to the Internet must have a globally unique IP address.
- Not all hosts are connected directly to the Internet.
  - Some are on networks that aren't connected to the Internet.
  - Some hosts are hidden behind firewalls, so their Internet connection is indirect.
- Several blocks of IP addresses are set aside just for this purpose.
- Three such ranges of private addresses exist.

What are these ranges?

What are these ranges?

CIDR	Subnet Mask	Address Range
10.0.0.0/8	255.0.0.0	10.0.0.1–10.255.255.254
172.16.0.0/12	255.240.0.0	172.16.1.1–172.31.255.254
192.168.0.0/16	255.255.0.0	192.168.0.1–192.168.255.254

Agenda del día

1. **Addresses**
   - Introducing IP Addresses
   - Subnetting
   - Network Address Translation
2. **Workshop**

Network Address Translation

What is NAT?

Network Address Translation

What is NAT?

- A technique called network address translation (NAT) used by many firewalls to hide the actual IP address of a host from the outside world.

Network Address Translation

What is NAT?

- A technique called network address translation (NAT) used by many firewalls to hide the actual IP address of a host from the outside world.
- The NAT device must use a globally unique IP to represent the host to the Internet.

Network Address Translation

What is NAT?

- A technique called network address translation (NAT) used by many firewalls to hide the actual IP address of a host from the outside world.
- The NAT device must use a globally unique IP to represent the host to the Internet.
- Behind the firewall, though, the host can use any IP address it wants.

Network Address Translation

What is NAT?

- A technique called network address translation (NAT) used by many firewalls to hide the actual IP address of a host from the outside world.
- The NAT device must use a globally unique IP to represent the host to the Internet.
- Behind the firewall, though, the host can use any IP address it wants.
- When packets cross the firewall, the NAT device translates the private IP address to the public IP address and vice versa.

Network Address Translation

What is one of the benefits of NAT?

What is one of the benefits of NAT?

- It helps to slow down the rate at which the IP address space is assigned.

What is one of the benefits of NAT?

- It helps to slow down the rate at which the IP address space is assigned.
- That's because a NAT device can use a single public IP address for more than one host.

Network Address Translation

What is one of the benefits of NAT?

- It helps to slow down the rate at which the IP address space is assigned.
- That's because a NAT device can use a single public IP address for more than one host.
- It does so by keeping track of outgoing packets so that it can match incoming packets with the correct host.

Workshop

Complete workshop for today's class. To be handed in the next class.