Addressing the Network – IPv4

Network Fundamentals – Chapter 6

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Explain the structure IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.

Given an IPv4 address, classify by type and describe how it is used in the network

Explain how addresses are assigned to networks by ISPs and within networks by administrators

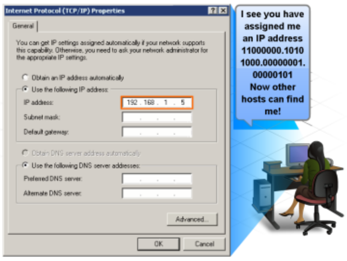
Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.

Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.

Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.

IP Addressing Structure

Describe the dotted decimal structure of a binary IP address and label its parts



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 5
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

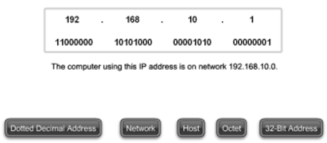
Advanced...
OK
Cancel
I see you have assigned me an IP address 11000000.10101000.00000001.00000101 Now other hosts can find me!

IP version 4 (IPv4) is the current form of addressing used on the Internet.

IP Addressing Structure

Describe the general role of 8-bit binary in network addressing and convert 8-bit binary to decimal

IPv4 Addresses



192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

The computer using this IP address is on network 192.168.10.0.

Roll over a label to see the parts of an IP address.

Dotted Decimal

Binary patterns representing IPv4 addresses are expressed as dotted decimals by separating each byte of the binary pattern, called an octet, with a dot.

It is called an octet because each decimal number represents one byte or 8 bits.

For example, the address:

10101100000100000000010000010100

is expressed in dotted decimal as:

172.16.4.20

Network and Host Portions

For each IPv4 address, some portion of the high-order bits represents the network address.

At Layer 3, we define a network as a group of hosts that have identical bit patterns in the network address portion of their addresses.

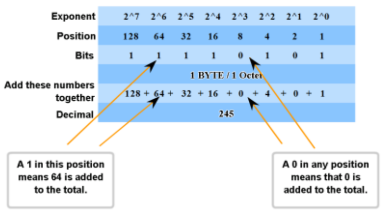
Although all 32 bits define the IPv4 host address, we have a variable number of bits that are called the host portion of the address.

The number of bits used in this host portion determines the number of hosts that we can have within the network.

IP Addressing Structure

Practice converting 8-bit binary to decimal

Binary To Decimal Conversion



Exponent	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Position	128	64	32	16	8	4	2	1
Bits	1	1	1	1	0	1	0	1
	1 BYTE / 1 Octet							
Add these numbers together	128 +	64 +	32 +	16 +	0 +	4 +	0 +	1
Decimal	245							

A 1 in this position means 64 is added to the total.

A 0 in any position means that 0 is added to the total.

11110101 in Binary = Decimal Number 245

Positional Notation

Learning to convert binary to decimal requires an understanding of the mathematical basis of a numbering system called positional notation.

Positional notation means that a digit represents different values depending on the position it occupies.

More specifically, the value that a digit represents is that value multiplied by the power of the base, or radix, represented by the position the digit occupies.

Some examples will help to clarify how this system works.

Example with Decimal

For the decimal number 245, the value that the 2 represents is 2*10^2 (2 times 10 to the power of 2).

The 2 is in what we commonly refer to as the "100s" position. Positional notation refers to this position as the base^2 position because the base, or radix, is 10 and the power is 2.

Using positional notation in the base 10 number system, 245 represents:

245 = (2 * 10^2) + (4 * 10^1) + (5 * 10^0)

or

245 = (2 * 100) + (4 * 10) + (5 * 1)

Binary Numbering System

In the binary numbering system, the radix is 2. Therefore, each position represents increasing powers of 2. In 8-bit binary numbers, the positions represent these quantities:

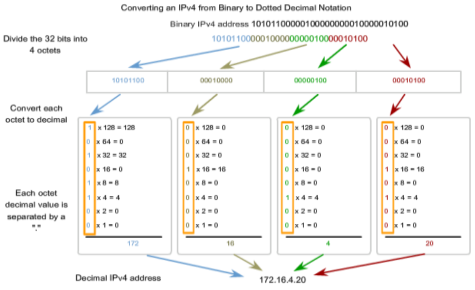
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

The base 2 numbering system only has two digits: 0 and 1.

When we interpret a byte as a decimal number, we have the quantity that position represents if the digit is a 1 and we do not have that quantity if the digit is a 0

Converting Binary to Decimal



Converting an IPv4 from Binary to Dotted Decimal Notation

Binary IPv4 address 10101100000100000000010000010100

Divide the 32 bits into 4 octets

10101100000100000000010000010100

10101100 | 00010000 | 00000100 | 00010100

Convert each octet to decimal

1 x 128 = 128
0 x 64 = 0
1 x 32 = 32
0 x 16 = 0
1 x 8 = 8
1 x 4 = 4
0 x 2 = 0
0 x 1 = 0
172

0 x 128 = 0
0 x 64 = 0
0 x 32 = 0
1 x 16 = 16
0 x 8 = 0
0 x 4 = 0
0 x 2 = 0
0 x 1 = 0
16

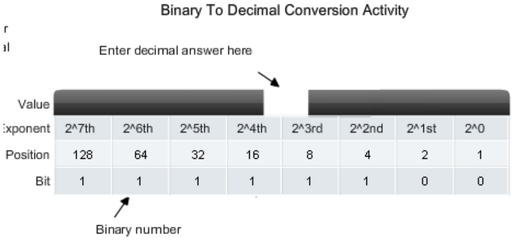
0 x 128 = 0
0 x 64 = 0
0 x 32 = 0
0 x 16 = 0
0 x 8 = 0
1 x 4 = 4
0 x 2 = 0
0 x 1 = 0
4

0 x 128 = 0
0 x 64 = 0
0 x 32 = 0
1 x 16 = 16
0 x 8 = 0
1 x 4 = 4
0 x 2 = 0
0 x 1 = 0
20

Each octet decimal value is separated by a "."

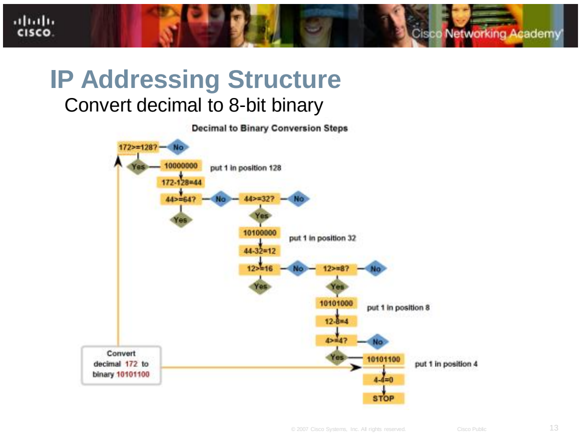
Decimal IPv4 address 172.16.4.20

Exercise



Binary To Decimal Conversion Activity

Value								
xponent	2^7th	2^6th	2^5th	2^4th	2^3rd	2^2nd	2^1st	2^0
Position	128	64	32	16	8	4	2	1
Bit	1	1	1	1	1	1	0	0



IP Addressing Structure

Convert decimal to 8-bit binary

Decimal to Binary Conversion Steps

172>=128? — No

Yes — 10000000 put 1 in position 128

172-128=44

44>=64? — No — 44>=32? — No

Yes

Yes

10100000 put 1 in position 32

44-32=12

12>=16 — No — 12>=8? — No

Yes

Yes

10101000 put 1 in position 8

12-8=4

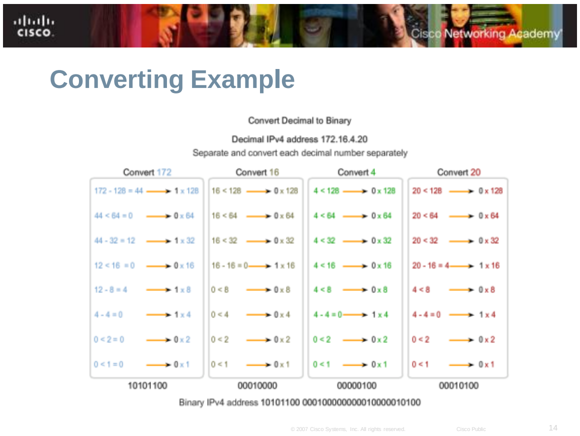
4>=4? — No

Yes — 10101100 put 1 in position 4

4-4=0

STOP

Convert decimal 172 to binary 10101100



Converting Example

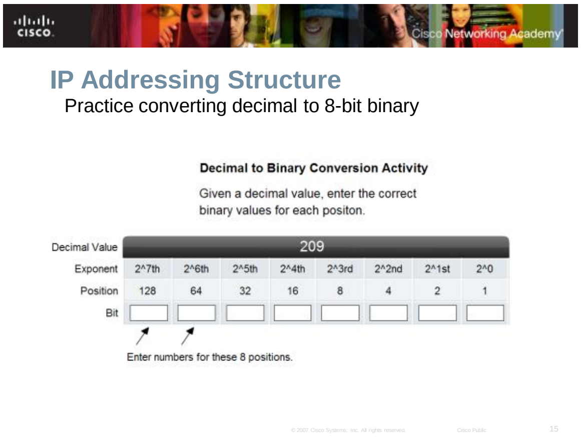
Convert Decimal to Binary

Decimal IPv4 address 172.16.4.20

Separate and convert each decimal number separately

Convert 172	Convert 16	Convert 4	Convert 20
172 - 128 = 44 → 1 x 128	16 < 128 → 0 x 128	4 < 128 → 0 x 128	20 < 128 → 0 x 128
44 < 64 = 0 → 0 x 64	16 < 64 → 0 x 64	4 < 64 → 0 x 64	20 < 64 → 0 x 64
44 - 32 = 12 → 1 x 32	16 < 32 → 0 x 32	4 < 32 → 0 x 32	20 < 32 → 0 x 32
12 < 16 = 0 → 0 x 16	16 - 16 = 0 → 1 x 16	4 < 16 → 0 x 16	20 - 16 = 4 → 1 x 16
12 - 8 = 4 → 1 x 8	0 < 8 → 0 x 8	4 < 8 → 0 x 8	4 < 8 → 0 x 8
4 - 4 = 0 → 1 x 4	0 < 4 → 0 x 4	4 - 4 = 0 → 1 x 4	4 - 4 = 0 → 1 x 4
0 < 2 = 0 → 0 x 2	0 < 2 → 0 x 2	0 < 2 → 0 x 2	0 < 2 → 0 x 2
0 < 1 = 0 → 0 x 1	0 < 1 → 0 x 1	0 < 1 → 0 x 1	0 < 1 → 0 x 1
10101100	00010000	00000100	00010100

Binary IPv4 address 10101100 00010000000001000010100



IP Addressing Structure

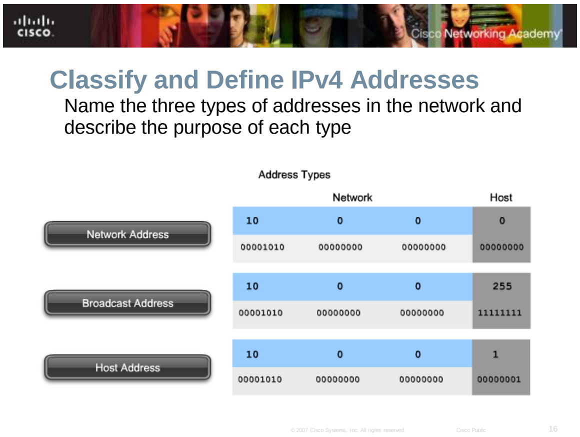
Practice converting decimal to 8-bit binary

Decimal to Binary Conversion Activity

Given a decimal value, enter the correct binary values for each positon.

Decimal Value	209							
Exponent	2^7th	2^6th	2^5th	2^4th	2^3rd	2^2nd	2^1st	2^0
Position	128	64	32	16	8	4	2	1
Bit	□	□	□	□	□	□	□	□

Enter numbers for these 8 positions.



Classify and Define IPv4 Addresses

Name the three types of addresses in the network and describe the purpose of each type

Address Types

	Network			Host
Network Address	10 00001010	0 00000000	0 00000000	0 00000000
Broadcast Address	10 00001010	0 00000000	0 00000000	255 11111111
Host Address	10 00001010	0 00000000	0 00000000	1 00000001

Network Address

The network address is a standard way to refer to a network. For example, we could refer to the network shown in the figure as "the 10.0.0.0 network."

This is a much more convenient and descriptive way to refer to the network than using a term like "the first network."

All hosts in the 10.0.0.0 network will have the same network bits.

Within the IPv4 address range of a network, the lowest address is reserved for the network address.

This address has a 0 for each host bit in the host portion of the address.

Broadcast Address

The IPv4 broadcast address is a special address for each network that allows communication to all the hosts in that network.

To send data to all hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

The broadcast address uses the highest address in the network range. This is the address in which the bits in the host portion are all 1s.

For the network 10.0.0.0 with 24 network bits, the broadcast address would be 10.0.0.255. This address is also referred to as the directed broadcast.

As described previously, every end device requires a unique address to deliver a packet to that **host**.

In IPv4 addresses, we assign the values between the network address and the broadcast address to the devices in that network.

Network Prefixes

An important question is: How do we know how many bits represent the network portion and how many bits represent the host portion?

When we express an IPv4 network address, we add a prefix length to the network address.

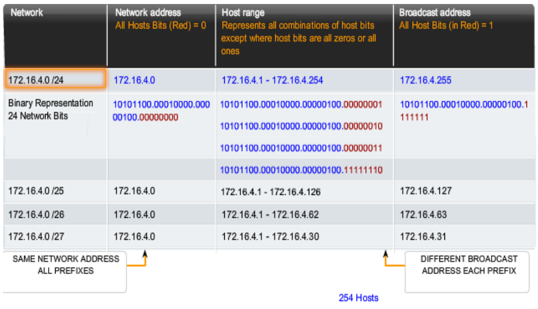
The prefix length is the number of bits in the address that gives us the network portion.

For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address.

This leaves the remaining 8 bits, the last octet, as the host portion.

The subnet mask consists of 32 bits, just as the address does, and uses 1s and 0s to indicate which bits of the address are network bits and which bits are host bits.

Example of Prefix



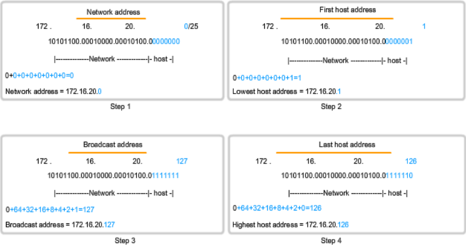
Network	Network address All Hosts Bits (Red) = 0	Host range Represents all combinations of host bits except where host bits are all zeros or all ones	Broadcast address All Host Bits (in Red) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
Binary Representation 24 Network Bits	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000.00000100.11111111
		10101100.00010000.00000100.11111110	
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

SAME NETWORK ADDRESS ALL PREFIXES

DIFFERENT BROADCAST ADDRESS EACH PREFIX

254 Hosts

Another Example



Network address

172 . 16. 20. 0/25

10101100.00010000.00010100.00000000

|--------------Network -------------|- host -|

0+0+0+0+0+0+0+0=0

Network address = 172.16.20.0

Step 1

First host address

172 . 16. 20. 1

10101100.00010000.00010100.00000001

|--------------Network -------------|- host -|

0+0+0+0+0+0+0+1=1

Lowest host address = 172.16.20.1

Step 2

Broadcast address

172 . 16. 20. 127

10101100.00010000.00010100.01111111

|--------------Network -------------|- host -|

0+64+32+16+8+4+2+1=127

Broadcast address = 172.16.20.127

Step 3

Last host address

172 . 16. 20. 126

10101100.00010000.00010100.01111110

|--------------Network -------------|- host -|

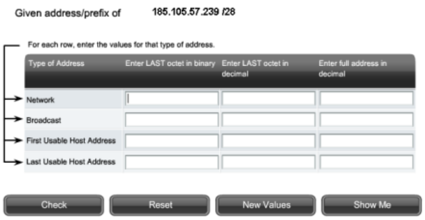
0+64+32+16+8+4+2+0=126

Highest host address = 172.16.20.126

Step 4

Classify and Define IPv4 Addresses

Determine the network, broadcast and host addresses for a given address and prefix combination

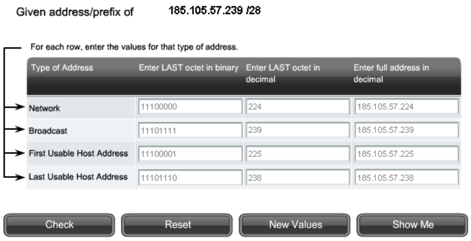


Given address/prefix of 185.105.57.239 /28

For each row, enter the values for that type of address.

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network			
Broadcast			
First Usable Host Address			
Last Usable Host Address			

Example with Answers



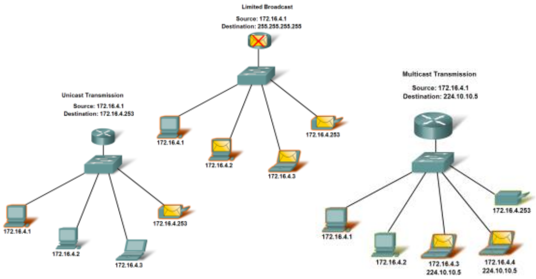
Given address/prefix of 185.105.57.239 /28

For each row, enter the values for that type of address.

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network	11100000	224	185.105.57.224
Broadcast	11101111	239	185.105.57.239
First Usable Host Address	11100001	225	185.105.57.225
Last Usable Host Address	11101110	238	185.105.57.238

Classify and Define IPv4 Addresses

Name the three types of communication in the Network Layer and describe the characteristics of each type



Three Ways of Communicating

In an IPv4 network, the hosts can communicate one of three different ways:

1. Unicast - the process of sending a packet from one host to an individual host
2. Broadcast - the process of sending a packet from one host to all hosts in the network
3. Multicast - the process of sending a packet from one host to a selected group of hosts

These three types of communication are used for different purposes in the data networks. In all three cases, the IPv4 address of the originating host is placed in the packet header as the source address.

Unicast Traffic

Unicast communication is used for the normal host-to-host communication in both a client/server and a peer-to-peer network.

Unicast packets use the host address of the destination device as the destination address and can be routed through an internetwork.

Broadcast and multicast, however, use special addresses as the destination address.

Using these special addresses, broadcasts are generally restricted to the local network.

The scope of multicast traffic also may be limited to the local network or routed through an internetwork.

Broadcast Traffic

Broadcast transmission is used for the location of special services/devices for which the address is not known or when a host needs to provide information to all the hosts on the network.

Some examples for using broadcast transmission are:

1. Mapping upper layer addresses to lower layer addresses
2. Requesting an address
3. Exchanging routing information by routing protocols

Unlike unicast, where the packets can be routed throughout the internetwork, broadcast packets are usually restricted to the local network.

This restriction is dependent on the configuration of the router that borders the network and the type of broadcast. There are two types of broadcasts: **directed broadcast** and **limited broadcast.**

Directed and Limited Broadcasts

A directed broadcast is sent to all hosts on a specific network.

This type of broadcast is useful for sending a broadcast to all hosts on a non-local network.

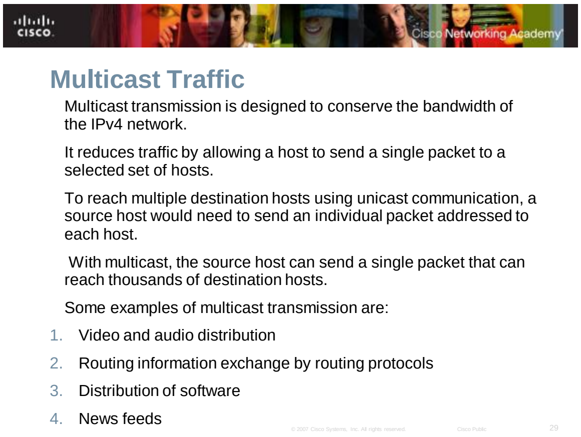
For example, for a host outside of the network to communicate with the hosts within the 172.16.4.0 /24 network, the destination address of the packet would be 172.16.4.255.

The limited broadcast is used for communication that is limited to the hosts on the local network.

These packets use a destination IPv4 address 255.255.255.255.

Routers do not forward this broadcast. Packets addressed to the limited broadcast address will only appear on the local network.

For this reason, an IPv4 network is also referred to as a broadcast domain. Routers form the boundary for a broadcast domain.



Multicast Traffic

Multicast transmission is designed to conserve the bandwidth of the IPv4 network.

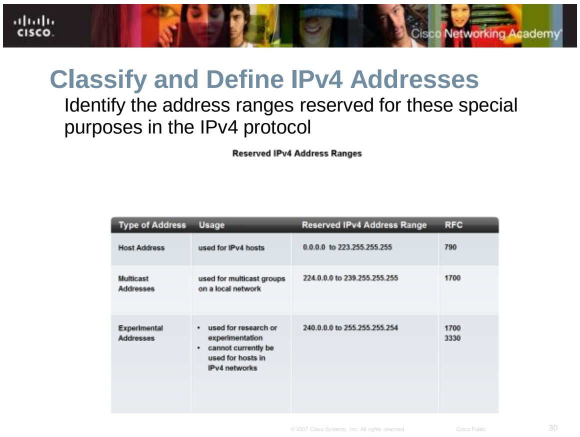
It reduces traffic by allowing a host to send a single packet to a selected set of hosts.

To reach multiple destination hosts using unicast communication, a source host would need to send an individual packet addressed to each host.

With multicast, the source host can send a single packet that can reach thousands of destination hosts.

Some examples of multicast transmission are:

1. Video and audio distribution
2. Routing information exchange by routing protocols
3. Distribution of software
4. News feeds

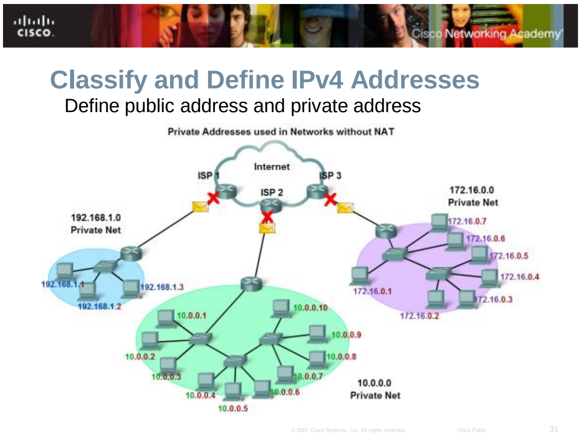


Classify and Define IPv4 Addresses

Identify the address ranges reserved for these special purposes in the IPv4 protocol

Reserved IPv4 Address Ranges

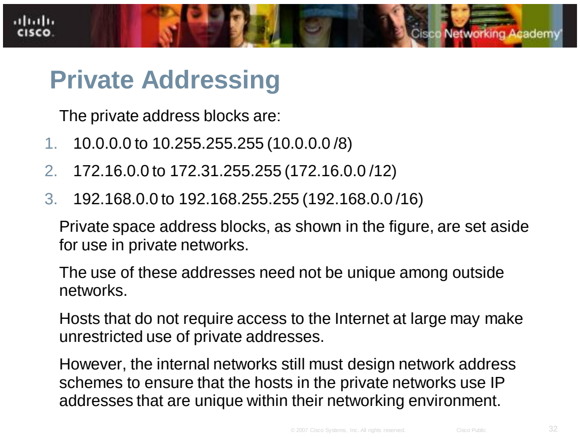
Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	• used for research or experimentation • cannot currently be used for hosts in IPv4 networks	240.0.0.0 to 255.255.255.254	1700 3330



Classify and Define IPv4 Addresses

Define public address and private address

Private Addresses used in Networks without NAT



Private Addressing

The private address blocks are:

1. 10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
2. 172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
3. 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)

Private space address blocks, as shown in the figure, are set aside for use in private networks.

The use of these addresses need not be unique among outside networks.

Hosts that do not require access to the Internet at large may make unrestricted use of private addresses.

However, the internal networks still must design network address schemes to ensure that the hosts in the private networks use IP addresses that are unique within their networking environment.

Important Note

Many hosts in different networks may use the same private space addresses.

Packets using these addresses as the source or destination should not appear on the public Internet.

The router or firewall device at the perimeter of these private networks must block or translate these addresses.

Even if these packets were to make their way to the Internet, the routers would not have routes to forward them to the appropriate private network.

NAT – Network Address Translation

With services to translate private addresses to public addresses, hosts on a privately addressed network can have access to resources across the Internet.

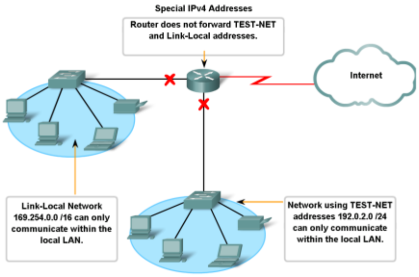
These services, called Network Address Translation (NAT), can be implemented on a device at the edge of the private network.

NAT allows the hosts in the network to "borrow" a public address for communicating to outside networks.

While there are some limitations and performance issues with NAT, clients for most applications can access services over the Internet without noticeable problems.

Classify and Define IPv4 Addresses

Describe the purpose of several special addresses


Special IPv4 Addresses

Router does not forward TEST-NET and Link-Local addresses.

Link-Local Network 169.254.0.0 /16 can only communicate within the local LAN.

Network using TEST-NET addresses 192.0.2.0 /24 can only communicate within the local LAN.

Special Addresses

Network and Broadcast Addresses

As explained earlier, within each network the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.

Default Route

Also presented earlier, we represent the IPv4 default route as 0.0.0.0.

The default route is used as a "catch all" route when a more specific route is not available. The use of this address also reserves all addresses in the 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8) address block.

Loopback Address

One such reserved address is the IPv4 loopback address 127.0.0.1.

The loopback is a special address that hosts use to direct traffic to themselves.

The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with one another.

By using the loopback address instead of the assigned IPv4 host address, two services on the same host can bypass the lower layers of the TCP/IP stack.

You can also ping the loopback address to test the configuration of TCP/IP on the local host.

Special Addresses

Link-Local - IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses.

These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available.

These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.

TEST-NET: The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples.

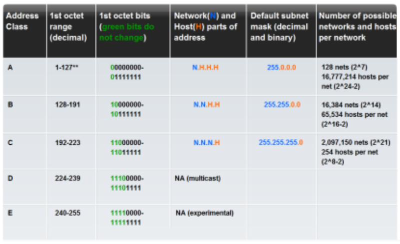
Unlike the experimental addresses, network devices will accept these addresses in their configurations.

You may often find these addresses used with the domain names example.com or example.net in RFCs, vendor, and protocol documentation. Addresses within this block should not appear on the Internet.

Classify and Define IPv4 Addresses

Identify the historic method for assigning addresses and the issues associated with the method

IP Address Classes



Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000- 01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000- 10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000- 11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000- 11101111	NA (multicast)		
E	240-255	11110000- 11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Class A and Class B Addressing

A class A address block was designed to support extremely large networks with more than 16 million host addresses.

Class A IPv4 addresses used a fixed /8 prefix with the first octet to indicate the network address. The remaining three octets were used for host addresses.

Class B address space was designed to support the needs of moderate to large size networks with more than 65,000 hosts.

A class B IP address used the two high-order octets to indicate the network address.

The other two octets specified host addresses. As with class A, address space for the remaining address classes needed to be reserved.

For class B addresses, the most significant two bits of the high-order octet were 10. This restricted the address block for class B to 128.0.0.0 /16 to 191.255.0.0 /16.

Class C Addressing

The class C address space was the most commonly available of the historic address classes. This address space was intended to provide addresses for small networks with a maximum of 254 hosts.

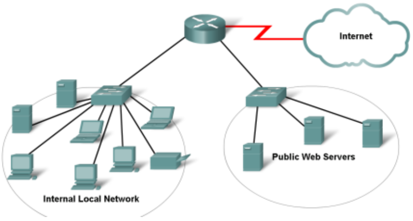
Class C address blocks used a /24 prefix. This meant that a class C network used only the last octet as host addresses with the three high-order octets used to indicate the network address.

Class C address blocks set aside address space for class D (multicast) and class E (experimental) by using a fixed value of 110 for the three most significant bits of the high-order octet.

Assigning Addresses

Explain the importance of using a structured process to assign IP addresses to hosts and the implications for choosing private vs. public addresses

IPv4 Address Planning and Assignment
Public and Private Addresses



Private or Public

An important part of planning an IPv4 addressing scheme is deciding when private addresses are to be used and where they are to be applied.

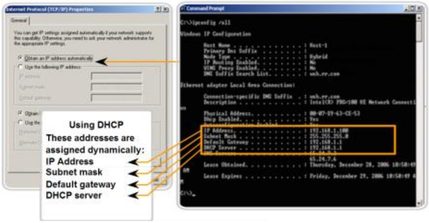
Considerations include:

1. Will there be more devices connected to the network than public addresses allocated by the network's ISP?
2. Will the devices need to be accessed from outside the local network?
3. If devices that may be assigned private addresses require access to the Internet, is the network capable of providing a Network Address Translation (NAT) service?

Assigning Addresses

Explain how end user devices can obtain addresses either statically through an administrator or dynamically through DHCP

Assigning Dynamic Addresses



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:
● Obtain
○ Use the

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : Host-1
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : wsh.rr.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : wsh.rr.com
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connecti
on
        Physical Address. . . . . . . . . : 00-07-E9-63-CE-53
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 65.24.7.3
                                            65.24.7.6
        Lease Obtained. . . . . . . . . . : Thursday, December 28, 2006 10:58:49
 AM
        Lease Expires . . . . . . . . . . : Friday, December 29, 2006 10:58:49 A
M

C:\>_
```

Using DHCP
These addresses are assigned dynamically:
IP Address
Subnet mask
Default gateway
DHCP server

Static Assignment

With a static assignment, the network administrator must manually configure the network information for a host, as shown in the figure. At a minimum, this includes entering the host IP address, subnet mask, and default gateway.

Static addresses have some advantages over dynamic addresses.

For instance, they are useful for printers, servers, and other networking devices that need to be accessible to clients on the network.

If hosts normally access a server at a particular IP address, it would cause problems if that address changed.

Additionally, static assignment of addressing information can provide increased control of network resources. However, it can be time-consuming to enter the information on each host.

When using static IP addressing, it is necessary to maintain an accurate list of the IP address assigned to each device. These are permanent addresses and are not normally reused.

Dynamic Assignment

DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information.

The configuration of the DHCP server requires that a block of addresses, called an address pool, be defined to be assigned to the DHCP clients on a network.

Addresses assigned to this pool should be planned so that they exclude any addresses used for the other types of devices.

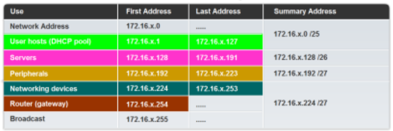
DHCP is generally the preferred method of assigning IP addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

Another benefit of DHCP is that an address is not permanently assigned to a host but is only "leased" for a period of time.

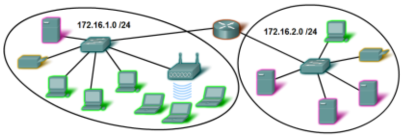
Assigning Addresses

Explain which types of addresses should be assigned to devices other than end user devices

Devices IP Address Ranges



Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



Addresses for Servers and Printers

Any network resource such as a server or a printer should have a static IPv4 address, as shown in the figure.

The client hosts access these resources using the IPv4 addresses of these devices.

Therefore, predictable addresses for each of these servers and peripherals are necessary.

Servers and peripherals are a concentration point for network traffic.

There are many packets sent to and from the IPv4 addresses of these devices.

When monitoring network traffic with a tool like Wireshark, a network administrator should be able to rapidly identify these devices. Using a consistent numbering system for these devices makes the identification easier.

Addresses for Hosts Accessible from the Internet

In the case of servers accessible by the Internet, each of these must have a public space address associated with it.

Additionally, variations in the address of one of these devices will make this device inaccessible from the Internet.

In many cases, these devices are on a network that is numbered using private addresses.

This means that the router or firewall at the perimeter of the network must be configured to translate the internal address of the server into a public address.

Because of this additional configuration in the perimeter intermediary device, it is even more important that these devices have a predictable address.

Intermediary Devices

Most intermediary devices are assigned Layer 3 addresses. Either for the device management or for their operation.

Devices such as hubs, switches, and wireless access points do not require IPv4 addresses to operate as intermediary devices.

However, if we need to access these devices as hosts to configure, monitor, or troubleshoot network operation, they need to have addresses assigned.

Because we need to know how to communicate with intermediary devices, they should have predictable addresses.

Therefore, their addresses are typically assigned manually. Additionally, the addresses of these devices should be in a different range within the network block than user device addresses.

Routers and Firewalls

Unlike the other intermediary devices mentioned, routers and firewall devices have an IPv4 address assigned to each interface.

Each interface is in a different network and serves as the gateway for the hosts in that network.

Typically, the router interface uses either the lowest or highest address in the network.

This assignment should be uniform across all networks in the corporation so that network personnel will always know the gateway of the network no matter which network they are working on.

Because the hosts in each network use a router or firewall device interface as the gateway out of the network, many packets flow through these interfaces.

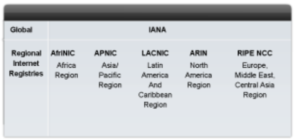
Therefore, these devices can play a major role in network security by filtering packets based on source and/or destination IPv4 addresses.

Grouping the different types of devices into logical addressing groups makes the assignment and operation of this packet filtering more efficient.

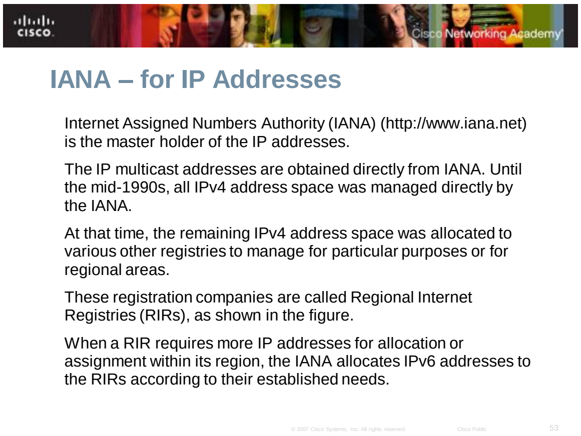
Assigning Addresses

Describe the process for requesting IPv4 public addresses, the role ISPs play in the process, and the role of the regional agencies that manage IP address registries

Entities that Oversee IP Address Allocation



Global	IANA				
Regional Internet Registries	AfriNIC Africa Region	APNIC Asia/ Pacific Region	LACNIC Latin America And Caribbean Region	ARIN North America Region	RIPE NCC Europe, Middle East, Central Asia Region



IANA – for IP Addresses

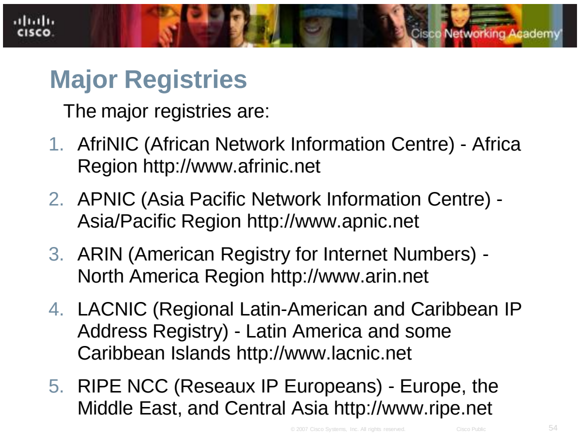
Internet Assigned Numbers Authority (IANA) (http://www.iana.net) is the master holder of the IP addresses.

The IP multicast addresses are obtained directly from IANA. Until the mid-1990s, all IPv4 address space was managed directly by the IANA.

At that time, the remaining IPv4 address space was allocated to various other registries to manage for particular purposes or for regional areas.

These registration companies are called Regional Internet Registries (RIRs), as shown in the figure.

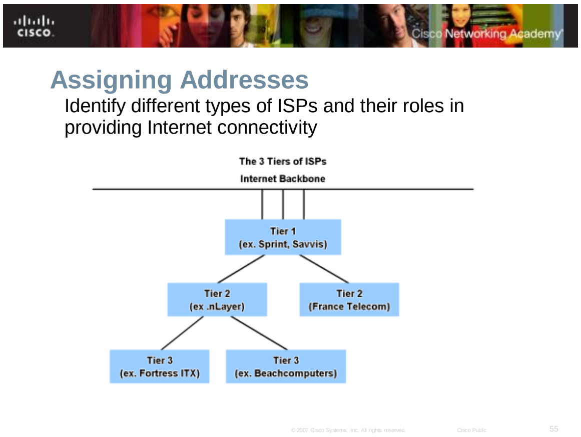
When a RIR requires more IP addresses for allocation or assignment within its region, the IANA allocates IPv6 addresses to the RIRs according to their established needs.



Major Registries

The major registries are:

1. AfriNIC (African Network Information Centre) - Africa Region http://www.afrinic.net
2. APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region http://www.apnic.net
3. ARIN (American Registry for Internet Numbers) - North America Region http://www.arin.net
4. LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands http://www.lacnic.net
5. RIPE NCC (Reseaux IP Europeans) - Europe, the Middle East, and Central Asia http://www.ripe.net



Assigning Addresses

Identify different types of ISPs and their roles in providing Internet connectivity

The 3 Tiers of ISPs

Internet Backbone

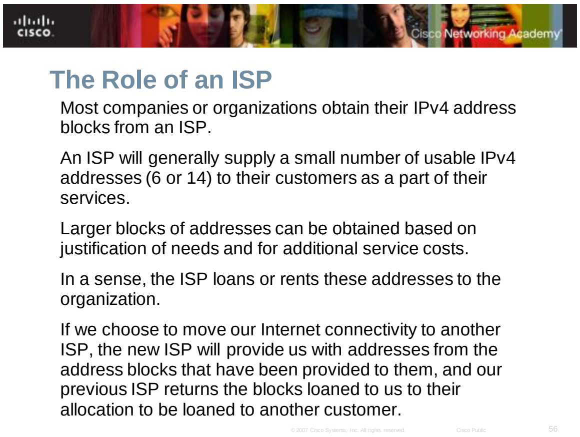
Tier 1 (ex. Sprint, Savvis)

Tier 2 (ex .nLayer)

Tier 2 (France Telecom)

Tier 3 (ex. Fortress ITX)

Tier 3 (ex. Beachcomputers)



The Role of an ISP

Most companies or organizations obtain their IPv4 address blocks from an ISP.

An ISP will generally supply a small number of usable IPv4 addresses (6 or 14) to their customers as a part of their services.

Larger blocks of addresses can be obtained based on justification of needs and for additional service costs.

In a sense, the ISP loans or rents these addresses to the organization.

If we choose to move our Internet connectivity to another ISP, the new ISP will provide us with addresses from the address blocks that have been provided to them, and our previous ISP returns the blocks loaned to us to their allocation to be loaned to another customer.

ISP Services

To get access to the services of the Internet, we have to connect our data network to the Internet using an Internet Service Provider (ISP).

ISPs have their own set of internal data networks to manage Internet connectivity and to provide related services.

Among the other services that an ISP generally provides to its customers are DNS services, e-mail services, and a website.

Depending on the level of service required and available, customers use different tiers of an ISP.

Tier 1, 2 and 3

At the top of the ISP hierarchy are Tier 1 ISPs. These ISPs are large national or international ISPs that are directly connected to the Internet backbone.

The primary advantages for customers of Tier 1 ISPs are reliability and speed

Tier 2 ISPs acquire their Internet service from Tier 1 ISPs. Tier 2 ISPs generally focus on business customers.

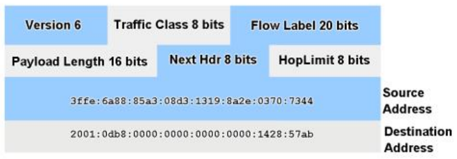
The primary disadvantage of Tier 2 ISPs, as compared to Tier 1 ISPs, is slower Internet access.

Tier 3 ISPs purchase their Internet service from Tier 2 ISPs. The focus of these ISPs is the retail and home markets in a specific locale.

Assigning Addresses

Identify several changes made to the IP protocol in IPv6 and describe the motivation for migrating from IPv4 to IPv6.

IPv6 Header



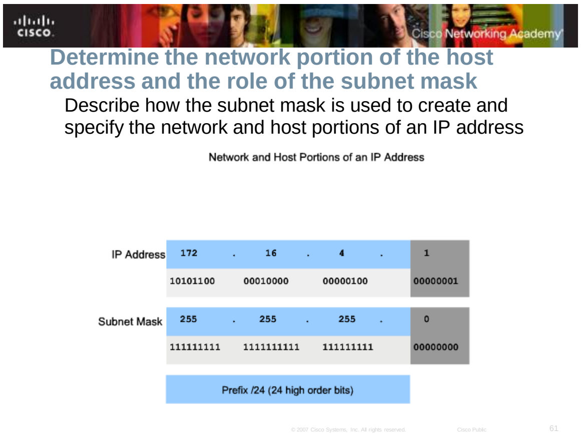
IPv6 Overview

Creating expanded addressing capabilities was the initial motivation for developing this new protocol. Other issues were also considered during the development of IPv6, such as:

1. **Improved packet handling**
2. **Increased scalability and longevity**
3. **QoS mechanisms**
4. **Integrated security**

To provide these features, IPv6 offers:

1. *128-bit hierarchical addressing - to expand addressing capabilities*
2. *Header format simplification - to improve packet handling*
3. *Improved support for extensions and options - for increased scalability/longevity and improved packet handling*
4. *Flow labeling capability - as QoS mechanisms*
5. *Authentication and privacy capabilities - to integrate security*

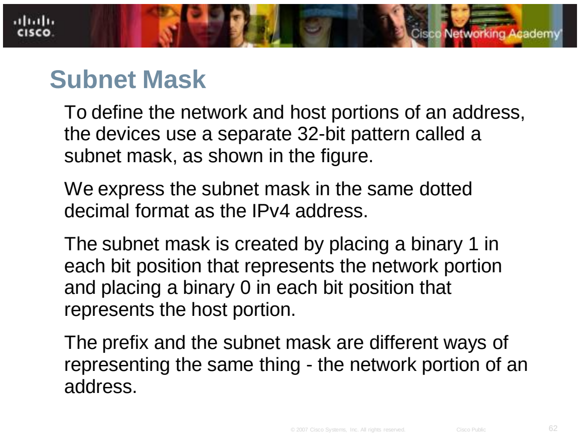


Determine the network portion of the host address and the role of the subnet mask

Describe how the subnet mask is used to create and specify the network and host portions of an IP address

Network and Host Portions of an IP Address

IP Address	172 .	16 .	4 .	1
	10101100	00010000	00000100	00000001
Subnet Mask	255 .	255 .	255 .	0
	111111111	1111111111	111111111	00000000
	Prefix /24 (24 high order bits)			



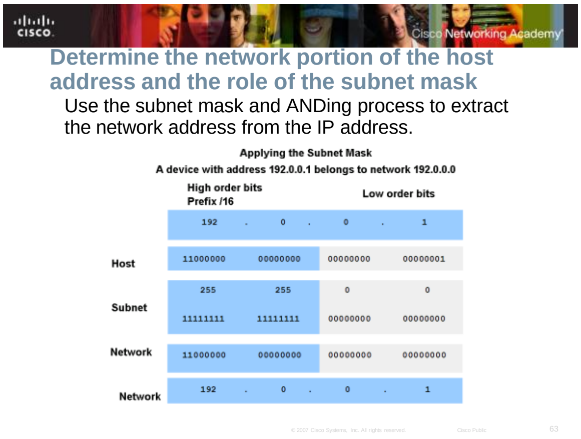
Subnet Mask

To define the network and host portions of an address, the devices use a separate 32-bit pattern called a subnet mask, as shown in the figure.

We express the subnet mask in the same dotted decimal format as the IPv4 address.

The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.

The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.



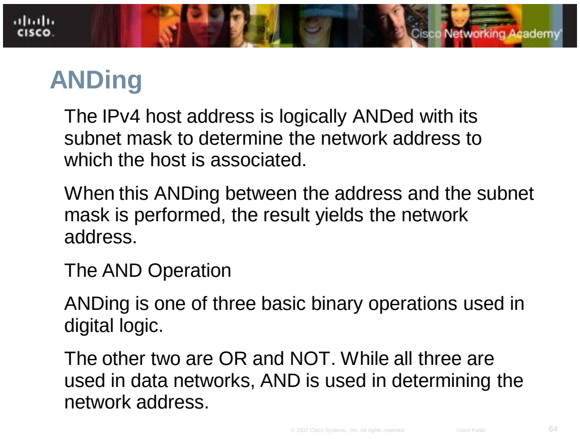
Determine the network portion of the host address and the role of the subnet mask

Use the subnet mask and ANDing process to extract the network address from the IP address.

Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host	11000000	00000000	00000000	00000001
Subnet	255	255	0	0
	11111111	11111111	00000000	00000000
Network	11000000	00000000	00000000	00000000
Network	192 .	0 .	0 .	1



ANDing

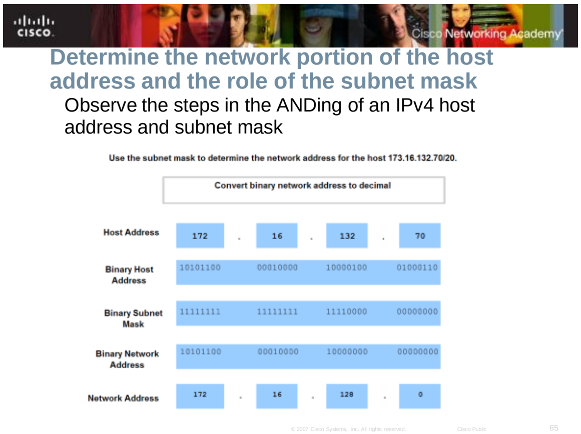
The IPv4 host address is logically ANDed with its subnet mask to determine the network address to which the host is associated.

When this ANDing between the address and the subnet mask is performed, the result yields the network address.

The AND Operation

ANDing is one of three basic binary operations used in digital logic.

The other two are OR and NOT. While all three are used in data networks, AND is used in determining the network address.



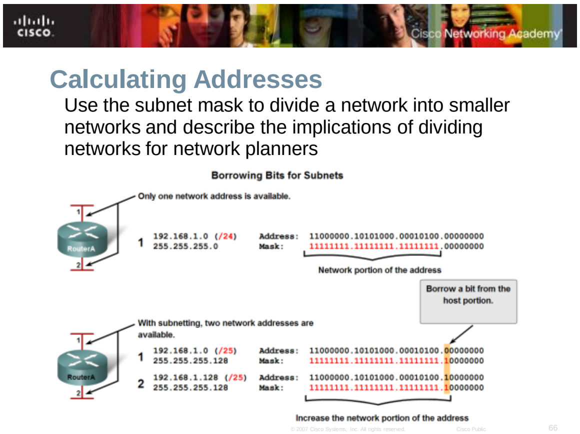
Determine the network portion of the host address and the role of the subnet mask

Observe the steps in the ANDing of an IPv4 host address and subnet mask

Use the subnet mask to determine the network address for the host 173.16.132.70/20.

Convert binary network address to decimal

Host Address	172	16	132	70
Binary Host Address	10101100	00010000	10000100	01000110
Binary Subnet Mask	11111111	11111111	11110000	00000000
Binary Network Address	10101100	00010000	10000000	00000000
Network Address	172	16	128	0



Calculating Addresses

Use the subnet mask to divide a network into smaller networks and describe the implications of dividing networks for network planners

Borrowing Bits for Subnets

Only one network address is available.

```
1  192.168.1.0 (/24)     Address:  11000000.10101000.00010100.00000000
   255.255.255.0         Mask:     11111111.11111111.11111111.00000000
```

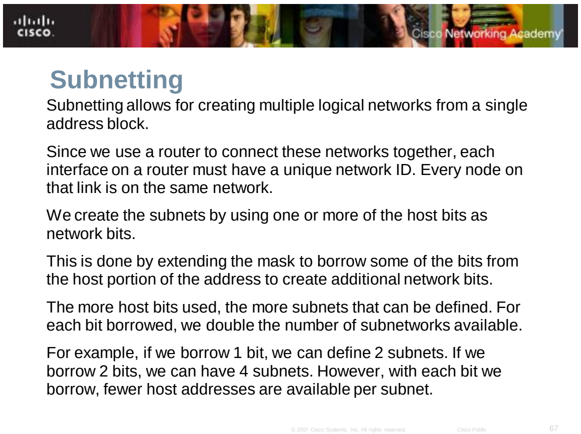
Network portion of the address

Borrow a bit from the host portion.

With subnetting, two network addresses are available.

```
1  192.168.1.0 (/25)     Address:  11000000.10101000.00010100.00000000
   255.255.255.128       Mask:     11111111.11111111.11111111.10000000
2  192.168.1.128 (/25)   Address:  11000000.10101000.00010100.10000000
   255.255.255.128       Mask:     11111111.11111111.11111111.10000000
```

Increase the network portion of the address



Subnetting

Subnetting allows for creating multiple logical networks from a single address block.

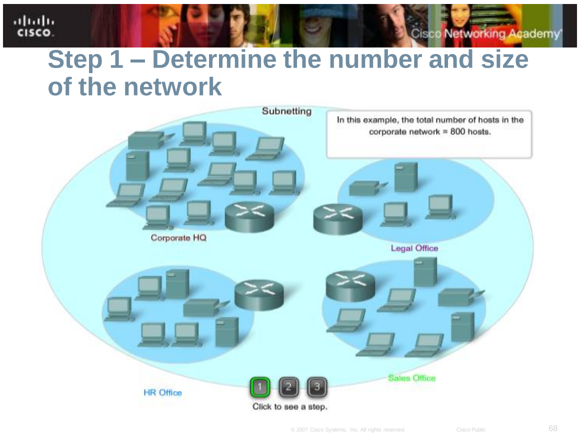
Since we use a router to connect these networks together, each interface on a router must have a unique network ID. Every node on that link is on the same network.

We create the subnets by using one or more of the host bits as network bits.

This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits.

The more host bits used, the more subnets that can be defined. For each bit borrowed, we double the number of subnetworks available.

For example, if we borrow 1 bit, we can define 2 subnets. If we borrow 2 bits, we can have 4 subnets. However, with each bit we borrow, fewer host addresses are available per subnet.

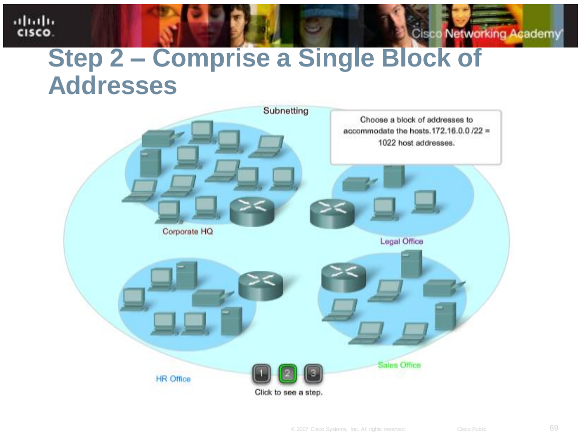


Step 1 – Determine the number and size of the network

Subnetting

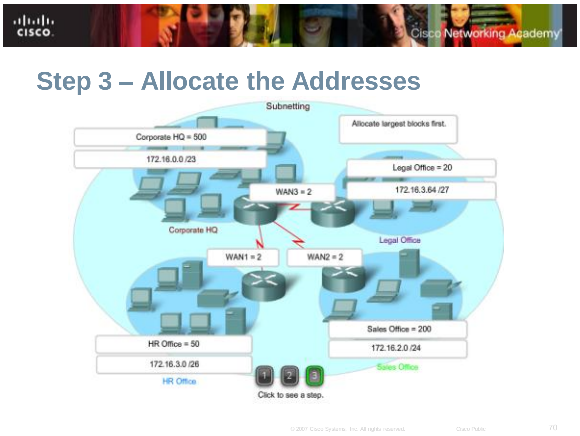
In this example, the total number of hosts in the corporate network = 800 hosts.

Click to see a step.



Step 2 – Comprise a Single Block of Addresses

Choose a block of addresses to accommodate the hosts.172.16.0.0 /22 = 1022 host addresses.



Step 3 – Allocate the Addresses

Allocate largest blocks first.

Corporate HQ = 500

172.16.0.0 /23

Legal Office = 20

172.16.3.64 /27

WAN3 = 2

WAN1 = 2

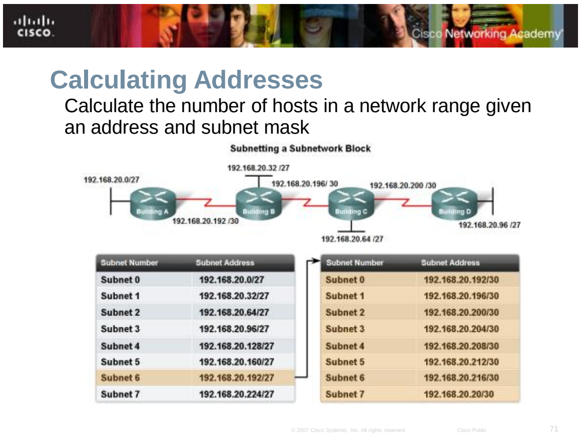
WAN2 = 2

Sales Office = 200

172.16.2.0 /24

HR Office = 50

172.16.3.0 /26



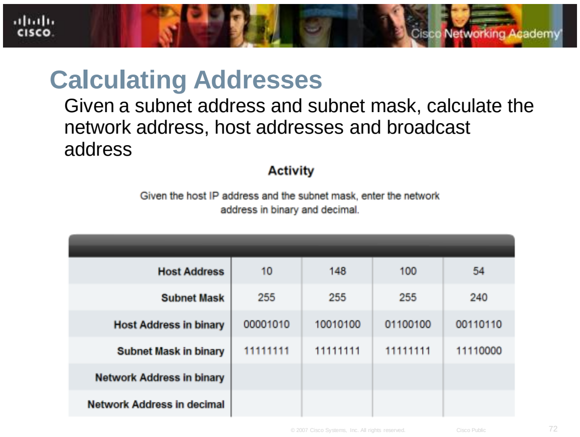
Calculating Addresses

Calculate the number of hosts in a network range given an address and subnet mask

Subnetting a Subnetwork Block

Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.20/30



Calculating Addresses

Given a subnet address and subnet mask, calculate the network address, host addresses and broadcast address

Activity

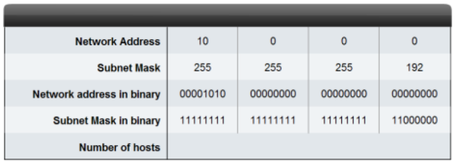
Given the host IP address and the subnet mask, enter the network address in binary and decimal.

Host Address	10	148	100	54
Subnet Mask	255	255	255	240
Host Address in binary	00001010	10010100	01100100	00110110
Subnet Mask in binary	11111111	11111111	11111111	11110000
Network Address in binary				
Network Address in decimal				

Calculating Addresses

Given a pool of addresses and masks, assign a host parameter with address, mask and gateway

Given the network address and the subnet mask, enter the number of possible hosts. Click next to Number of Hosts to enter your response.

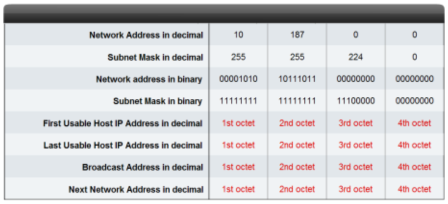


Network Address	10	0	0	0
Subnet Mask	255	255	255	192
Network address in binary	00001010	00000000	00000000	00000000
Subnet Mask in binary	11111111	11111111	11111111	11000000
Number of hosts				

Calculating Addresses

Given a diagram of a multi-layered network, address range, number of hosts in each network and the ranges for each network, create a network scheme that assigns addressing ranges to each network

Given the network address and the subnet mask, define the range of hosts, the broadcast address, and the next network address.

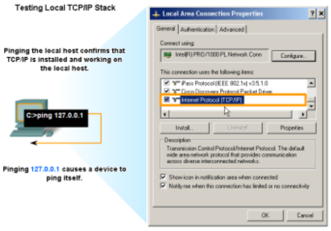


Network Address in decimal	10	187	0	0
Subnet Mask in decimal	255	255	224	0
Network address in binary	00001010	10111011	00000000	00000000
Subnet Mask in binary	11111111	11111111	11100000	00000000
First Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Last Usable Host IP Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Broadcast Address in decimal	1st octet	2nd octet	3rd octet	4th octet
Next Network Address in decimal	1st octet	2nd octet	3rd octet	4th octet

Testing the Network Layer

Describe the general purpose of the ping command, trace the steps of its operation in a network, and use the ping command to determine if the IP protocol is operational on a local host

Testing Local TCP/IP Stack



```
C:>ping 127.0.0.1
```

Pinging the local host confirms that TCP/IP is installed and working on the local host.

Pinging 127.0.0.1 causes a device to ping itself.

Local Area Connection Properties

Connect using: Intel(R) PRO/1000 PL Network Conn

This connection uses the following items:

- ☑ iPass Protocol (IEEE 802.1x) v3.5.1.0
- ☑ Cisco Discovery Protocol Packet Driver
- ☑ Internet Protocol (TCP/IP)

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

PING – Packet InterNetwork Groper

Ping is a utility for testing IP connectivity between hosts. Ping sends out requests for responses from a specified host address.

Ping uses a Layer 3 protocol that is a part on the TCP/IP suite called Internet Control Message Protocol (ICMP). Ping uses an ICMP Echo Request datagram.

If the host at the specified address receives the Echo request, it responds with an ICMP Echo Reply datagram.

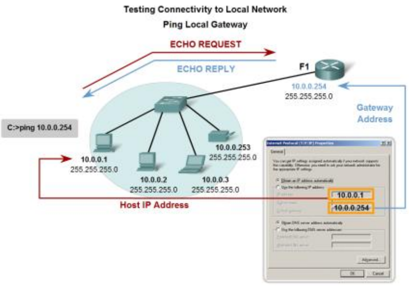
For each packet sent, ping measures the time required for the reply.

As each response is received, ping provides a display of the time between the ping being sent and the response received.

This is a measure of the network performance. Ping has a timeout value for the response. If a response is not received within that timeout, ping gives up and provides a message indicating that a response was not received.

Testing the Network Layer

Use ping to verify that a local host can communicate with a gateway across a local area network



Testing the Gateway

You can also use ping to test the host ability to communicate on the local network.

This is generally done by pinging the IP address of the gateway of the host, as shown in the figure.

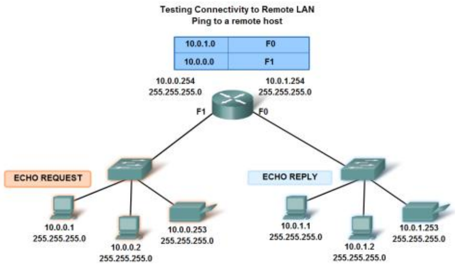
A ping to the gateway indicates that the host and the router's interface serving as that gateway are both operational on the local network.

For this test, the gateway address is most often used, because the router is normally always operational. If the gateway address does not respond, you can try the

IP address of another host that you are confident is operational in the local network.

Testing the Network Layer

Use ping to verify that a local host can communicate via a gateway to a device in remote network


Testing Connectivity to Remote LAN
Ping to a remote host

10.0.1.0	F0
10.0.0.0	F1

Testing connectivity to the Remote LAN

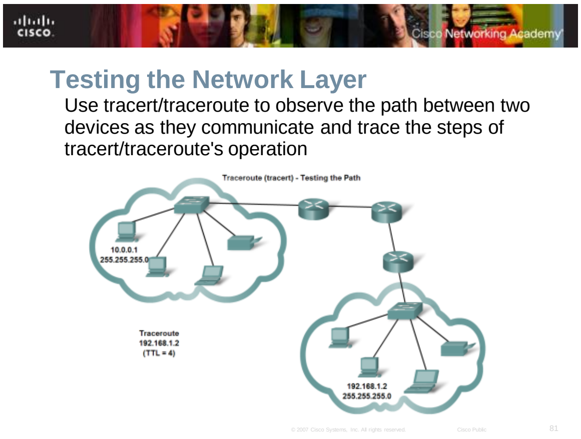
You can also use ping to test the ability of the local IP host to communicate across an internetwork.

The local host can ping an operational host of a remote network, as shown in the figure.

If this ping is successful, you will have verified the operation of a large piece of the internetwork.

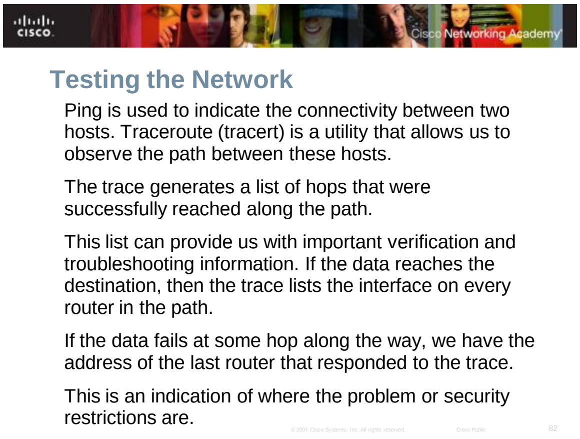
It means that we have verified our host's communication on the local network, the operation of the router serving as our gateway, and all other routers that might be in the path between our network and the network of the remote host.

Additionally, you have verified the same functionality of the remote host. If, for any reason, the remote host could not use its local network to communicate outside its network, then it would not have responded.



Testing the Network Layer

Use tracert/traceroute to observe the path between two devices as they communicate and trace the steps of tracert/traceroute's operation



Testing the Network

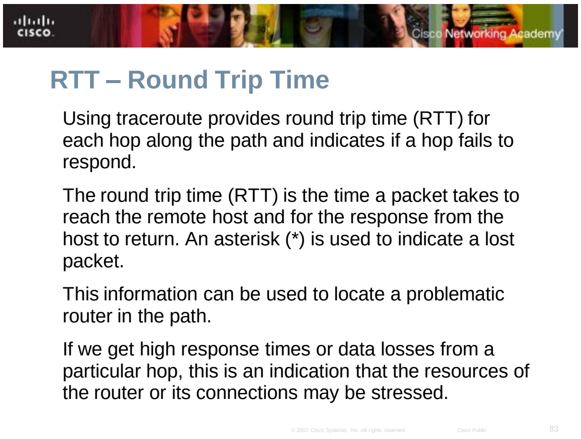
Ping is used to indicate the connectivity between two hosts. Traceroute (tracert) is a utility that allows us to observe the path between these hosts.

The trace generates a list of hops that were successfully reached along the path.

This list can provide us with important verification and troubleshooting information. If the data reaches the destination, then the trace lists the interface on every router in the path.

If the data fails at some hop along the way, we have the address of the last router that responded to the trace.

This is an indication of where the problem or security restrictions are.



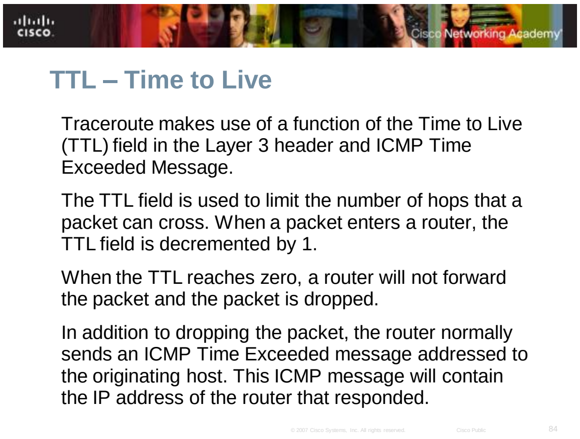
RTT – Round Trip Time

Using traceroute provides round trip time (RTT) for each hop along the path and indicates if a hop fails to respond.

The round trip time (RTT) is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost packet.

This information can be used to locate a problematic router in the path.

If we get high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be stressed.



TTL – Time to Live

Traceroute makes use of a function of the Time to Live (TTL) field in the Layer 3 header and ICMP Time Exceeded Message.

The TTL field is used to limit the number of hops that a packet can cross. When a packet enters a router, the TTL field is decremented by 1.

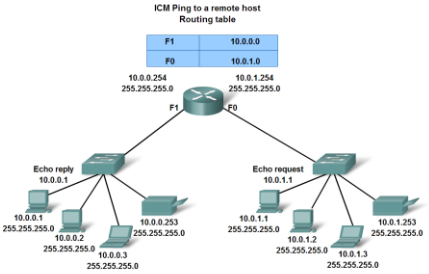
When the TTL reaches zero, a router will not forward the packet and the packet is dropped.

In addition to dropping the packet, the router normally sends an ICMP Time Exceeded message addressed to the originating host. This ICMP message will contain the IP address of the router that responded.

Testing the Network Layer

Describe the role of ICMP in the TCP/IP suite and its impact on the IP protocol

ICM Ping to a remote host
Routing table



F1	10.0.0.0
F0	10.0.1.0

ICMP

ICMP is the messaging protocol for the TCP/IP suite. ICMP provides control and error messages and is used by the ping and traceroute utilities.

Although ICMP uses the basic support of IP as if it were a higher-level protocol ICMP, it is actually a separate Layer 3 of the TCP/IP suite.

The types of ICMP messages - and the reasons why they are sent - are extensive. We will discuss some of the more common messages.

ICMP messages that may be sent include:

1. Host confirmation
2. Unreachable Destination or Service
3. Time exceeded
4. Route redirection
5. Source quench

1. Host Confirmation

An ICMP Echo Message can be used to determine if a host is operational.

The local host sends an ICMP Echo Request to a host. The host receiving the echo message replies with the ICMP Echo Reply, as shown in the figure.

This use of the ICMP Echo messages is the basis of the ping utility.

2. Unreachable Destination

The ICMP Destination Unreachable can used to notify a host that the destination or service is unreachable.

When a host or gateway receives a packet that it cannot deliver, it may send an ICMP Destination Unreachable packet to the host originating the packet.

The Destination Unreachable packet will contain codes that indicate why the packet could not be delivered.

Among the Destination Unreachable codes are:

0 = net unreachable

1 = host unreachable

2 = protocol unreachable

3 = port unreachable

3. Time Exceeded

An ICMP Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the TTL field of the packet has expired.

If a router receives a packet and decrements the TTL field in the packet to zero, it discards the packet.

The router may also send an ICMP Time Exceeded message to the source host to inform the host of the reason the packet was dropped.

4. Route Redirection

A router may use the ICMP Redirect Message to notify the hosts on a network that a better route is available for a particular destination.

This message may only be used when the source host is on the same physical network as both gateways.

If a router receives a packet for which it has a route and for which the next hop is attached to the same interface as the packet arrived, the router may send an ICMP Redirect Message to the source host.

This message will inform the source host of the next hop contained in a route in the routing table.

5. Source Quench

The ICMP Source Quench message can be used to tell the source to temporarily stop sending packets.

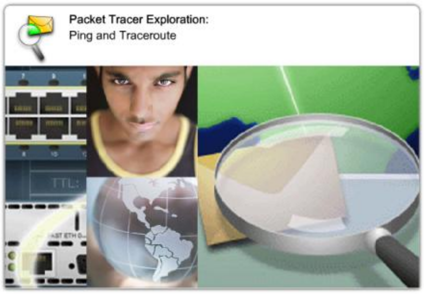
If a router does not have enough buffer space to receive incoming packets, a router will discard the packets.

If the router has to do so, it may also send an ICMP Source Quench message to source hosts for every message that it discards.

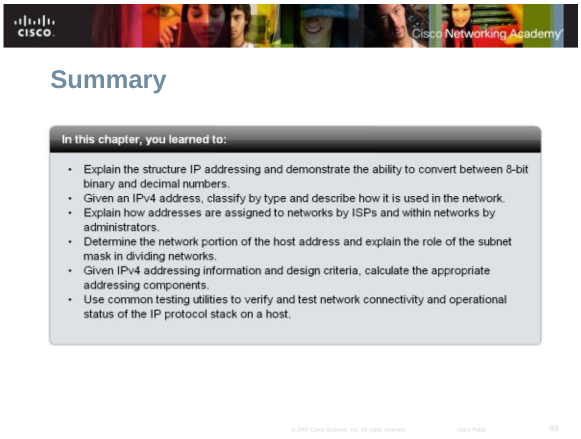
A destination host may also send a source quench message if datagrams arrive too fast to be processed.

When a host receives an ICMP Source Quench message, it reports it to the Transport layer. The source host can then use the TCP flow control mechanisms to adjust the transmission.

Labs – Packet Tracer



Packet Tracer Exploration:
Ping and Traceroute



Cisco Networking Academy

Summary

In this chapter, you learned to:

- Explain the structure IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.
- Given an IPv4 address, classify by type and describe how it is used in the network.
- Explain how addresses are assigned to networks by ISPs and within networks by administrators.
- Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.
- Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.
- Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.