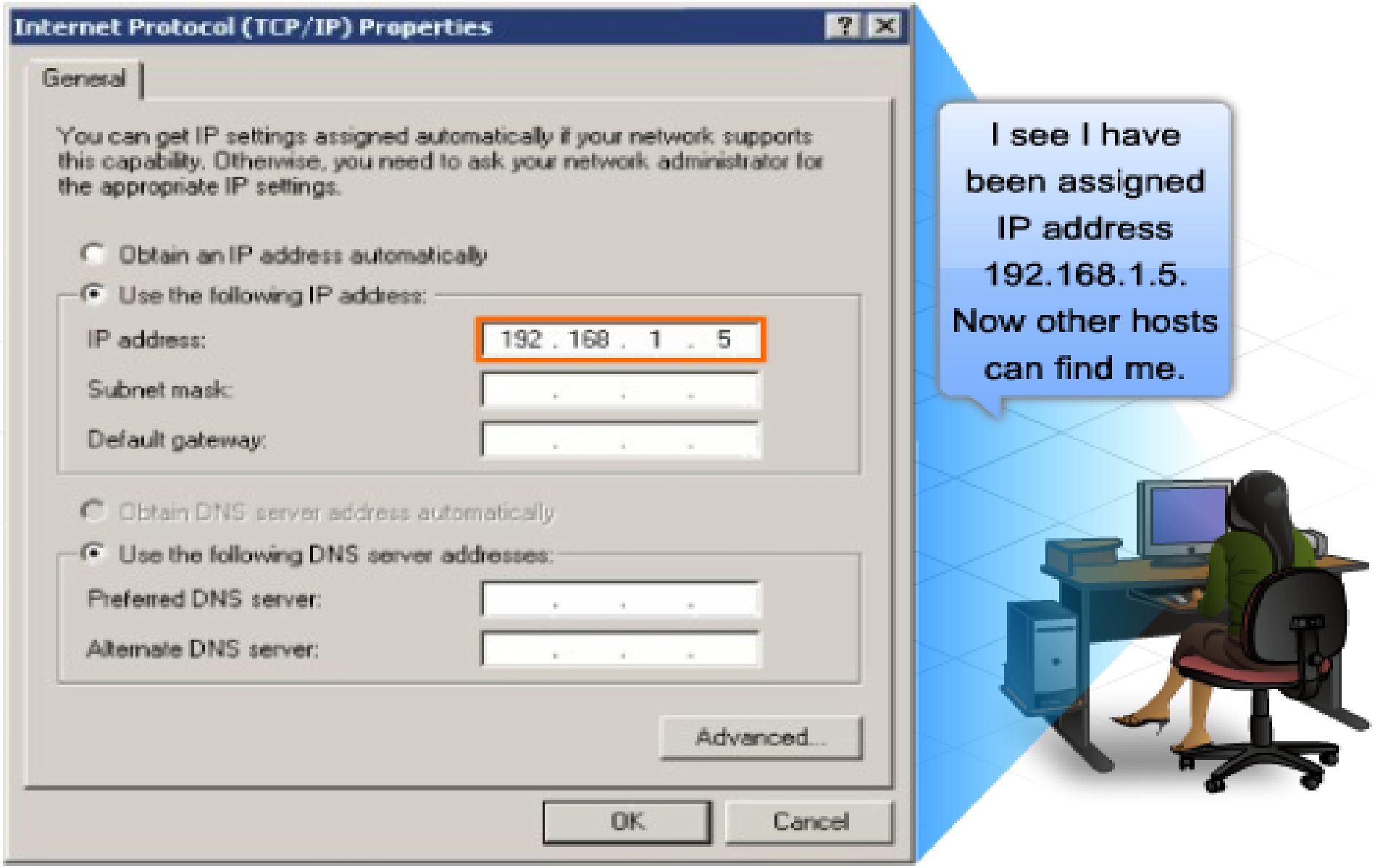
CH 6
ADDRESSING

6.0.1 INTRODUCTION



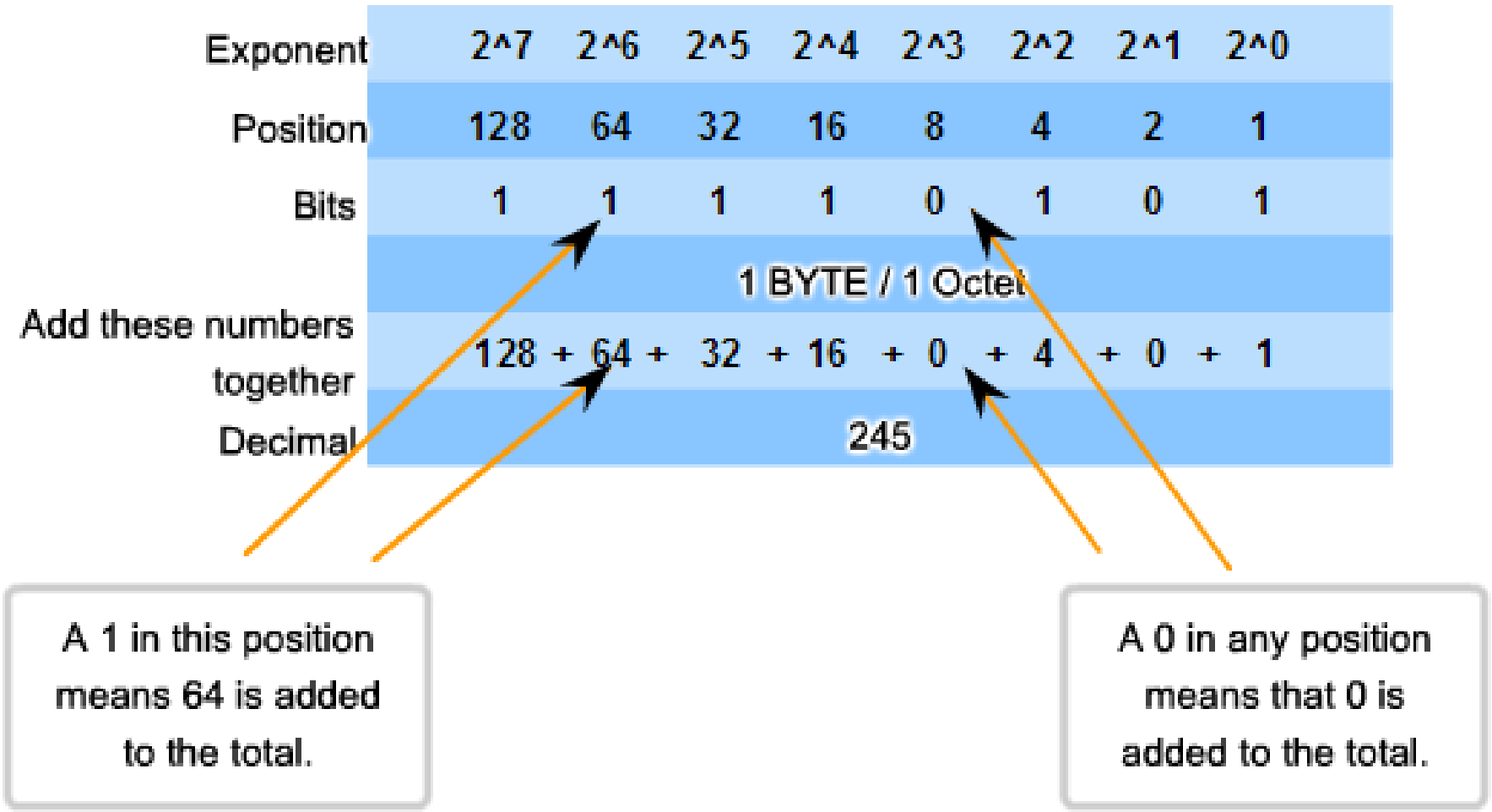
IP version 4 (IPv4) is the current form of addressing used on the Internet.

6.1.1 IPv4 ADDRESS

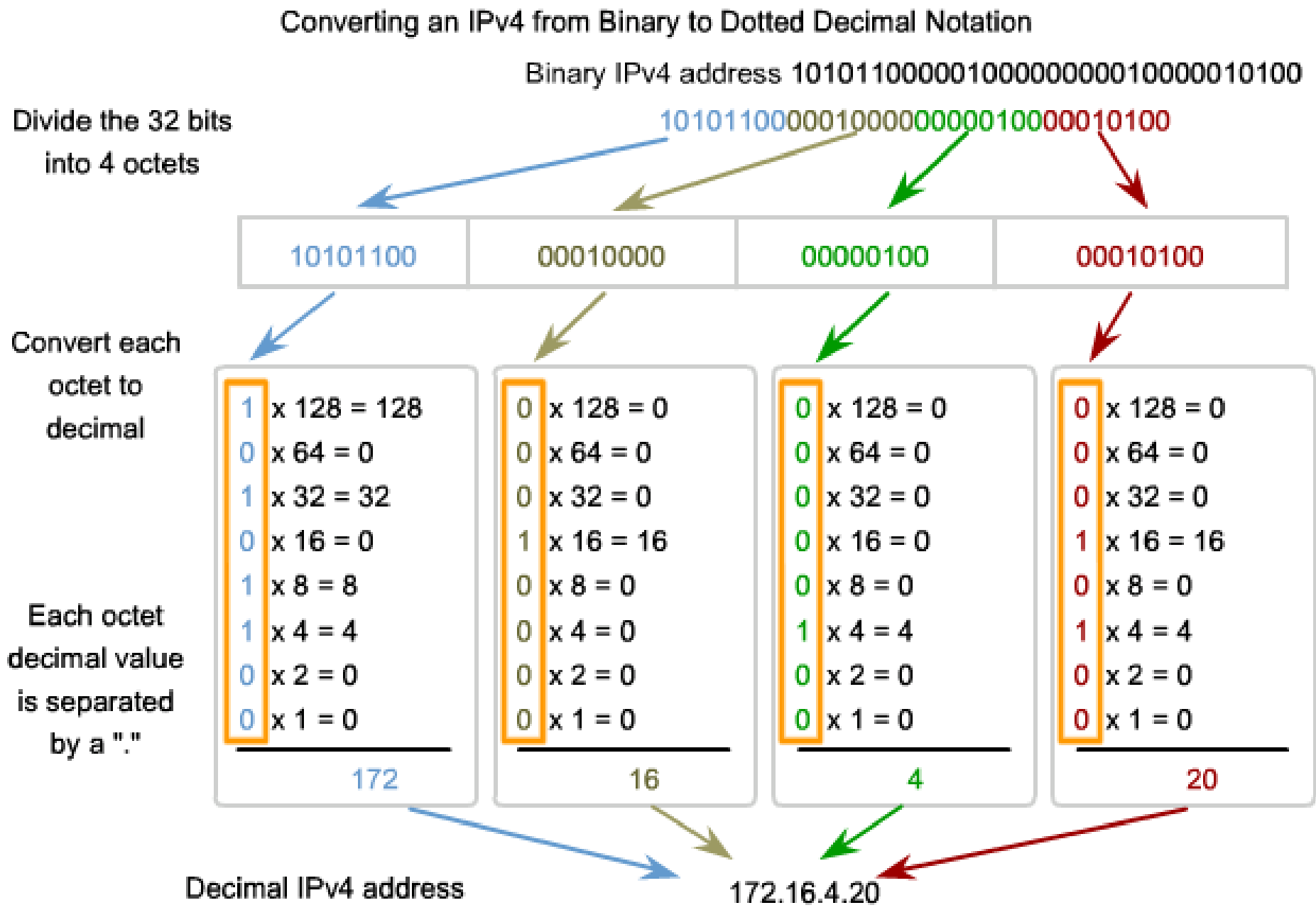
192	.	168	.	10	.	1
11000000		10101000		00001010		00000001

The computer using this IP address is on network 192.168.10.0.

6.1.2 BINARY TO DECIMAL CONVERSION



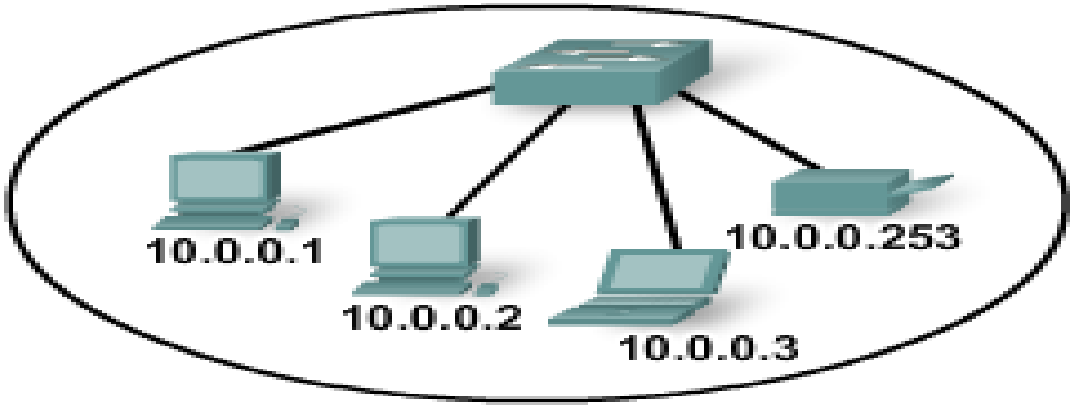
6.1.2 BINARY TO DECIMAL CONVERSION



6.2.1 TYPES OF IPv4 ADDRESSES

Address Types

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



6.2.1 TYPES OF IPv4 ADDRESSES

Using Different Prefixes for the 172.16.4.0 Network

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
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
Binary Representation 27 Network Bits	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.00011110	10101100.00010000.00000100.00011111

SAME NETWORK ADDRESS ALL PREFIXES

DIFFERENT BROADCAST ADDRESS EACH PREFIX

30 Hosts

DIFFERENT NUMBER OF HOSTS EACH PREFIX

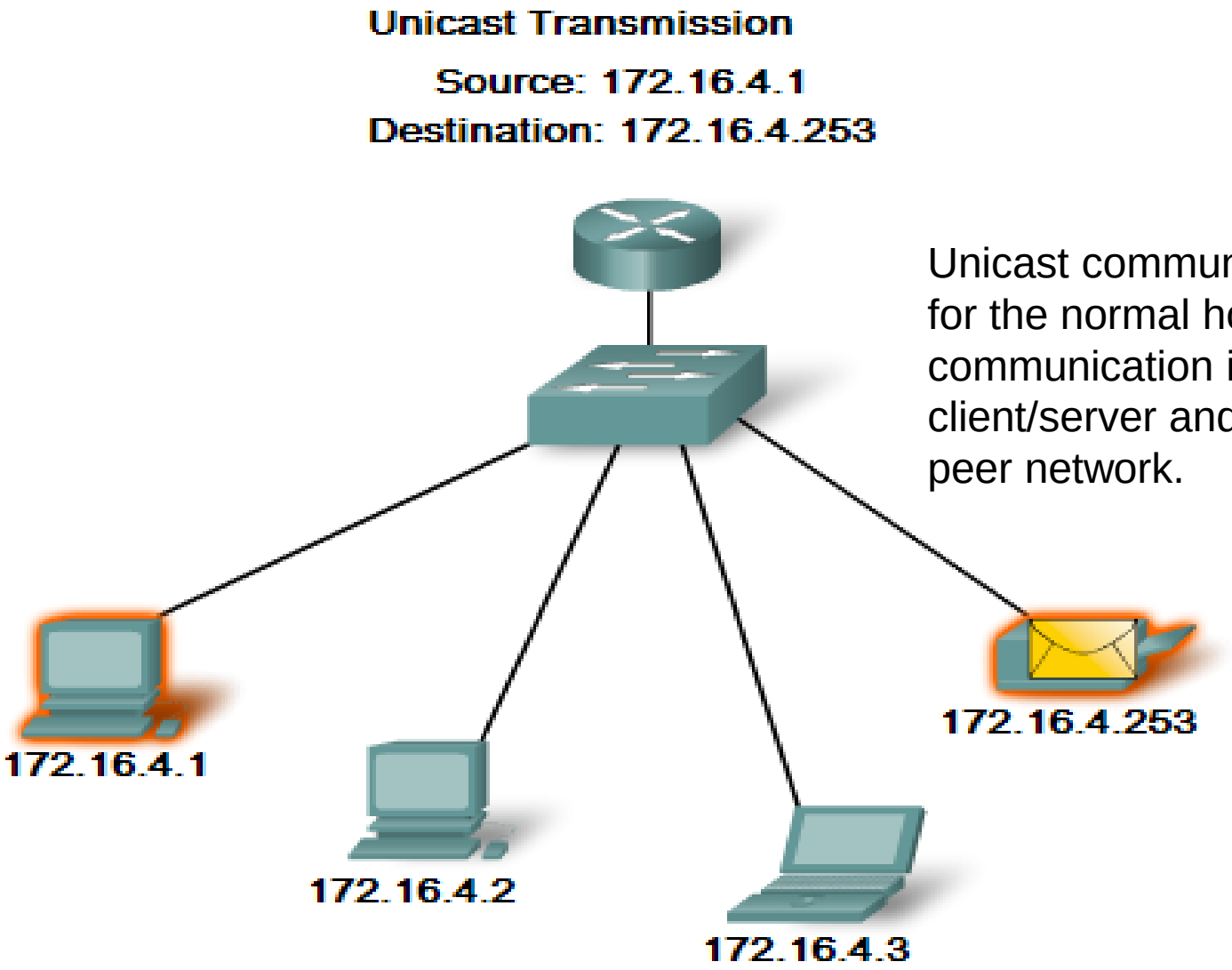
Roll over the rows to see binary numbers for addresses and number of hosts.

6.2.2 CALCULATING NETWORK, HOST AND BROADCAST

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

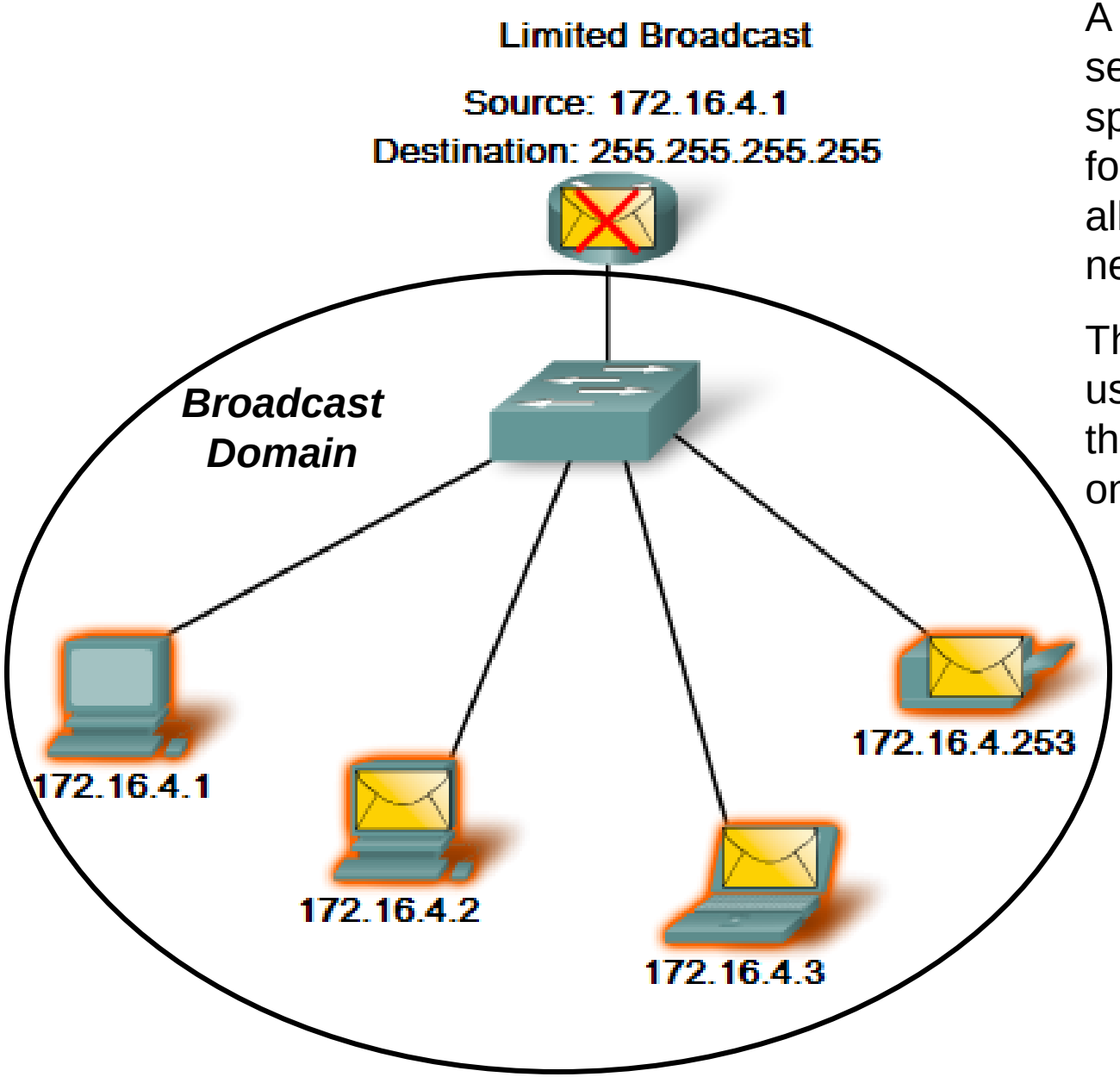
Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network	01000000	64	188.23.29.64
Broadcast	01001111	79	188.23.29.79
First Usable Host Address	01000001	65	188.23.29.65
Last Usable Host Address	01001110	78	188.23.29.78

6.2.3 UNICAST COMMUNICATION



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

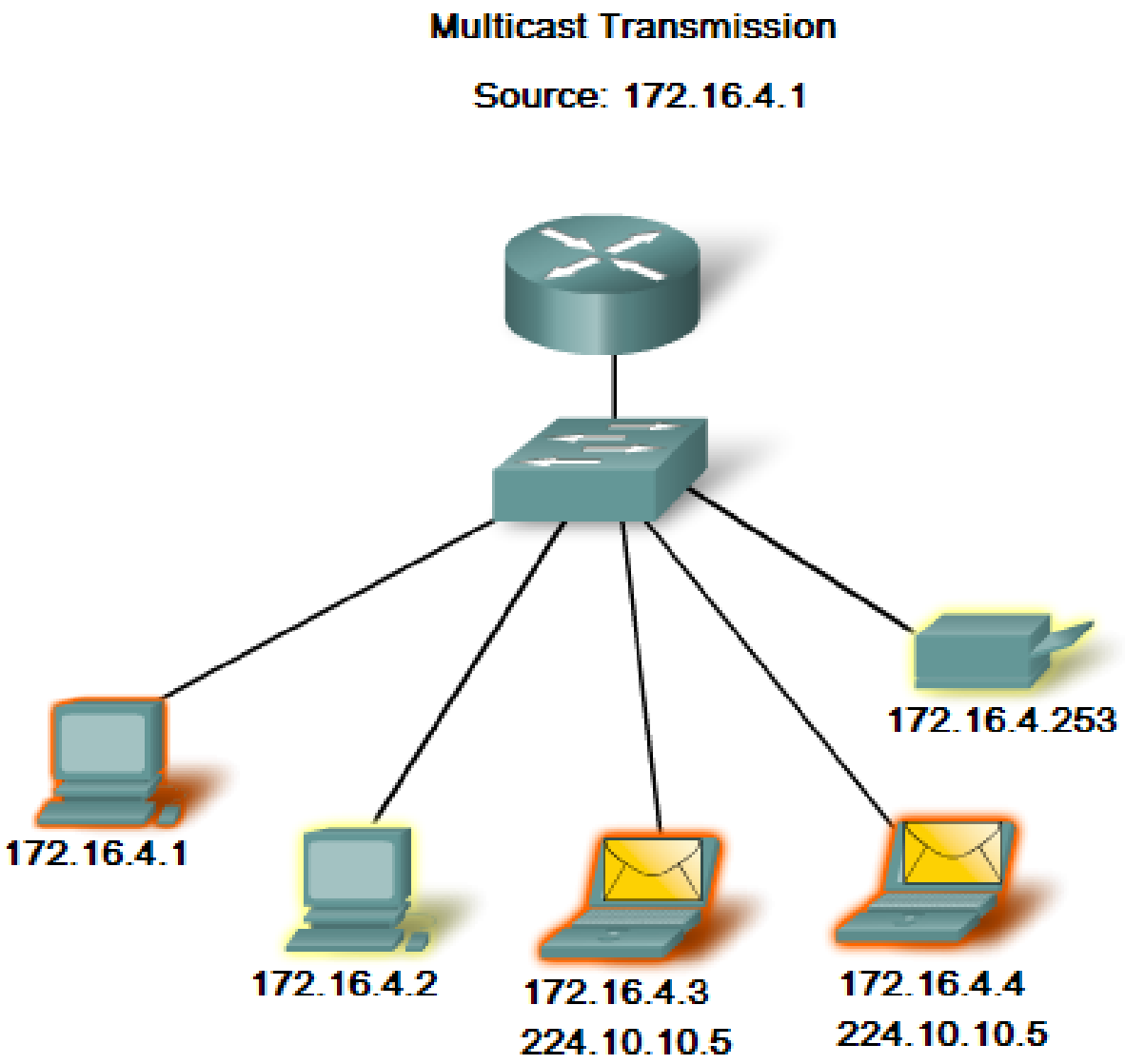
6.2.3 LIMITED BROADCAST



A **directed broadcast** is sent to all hosts on a specific network. (useful for sending a broadcast to all hosts on a non-local network)

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

6.2.3 Multicast Transmission



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.

The multicast clients use services initiated by a client program to subscribe to the multicast group.

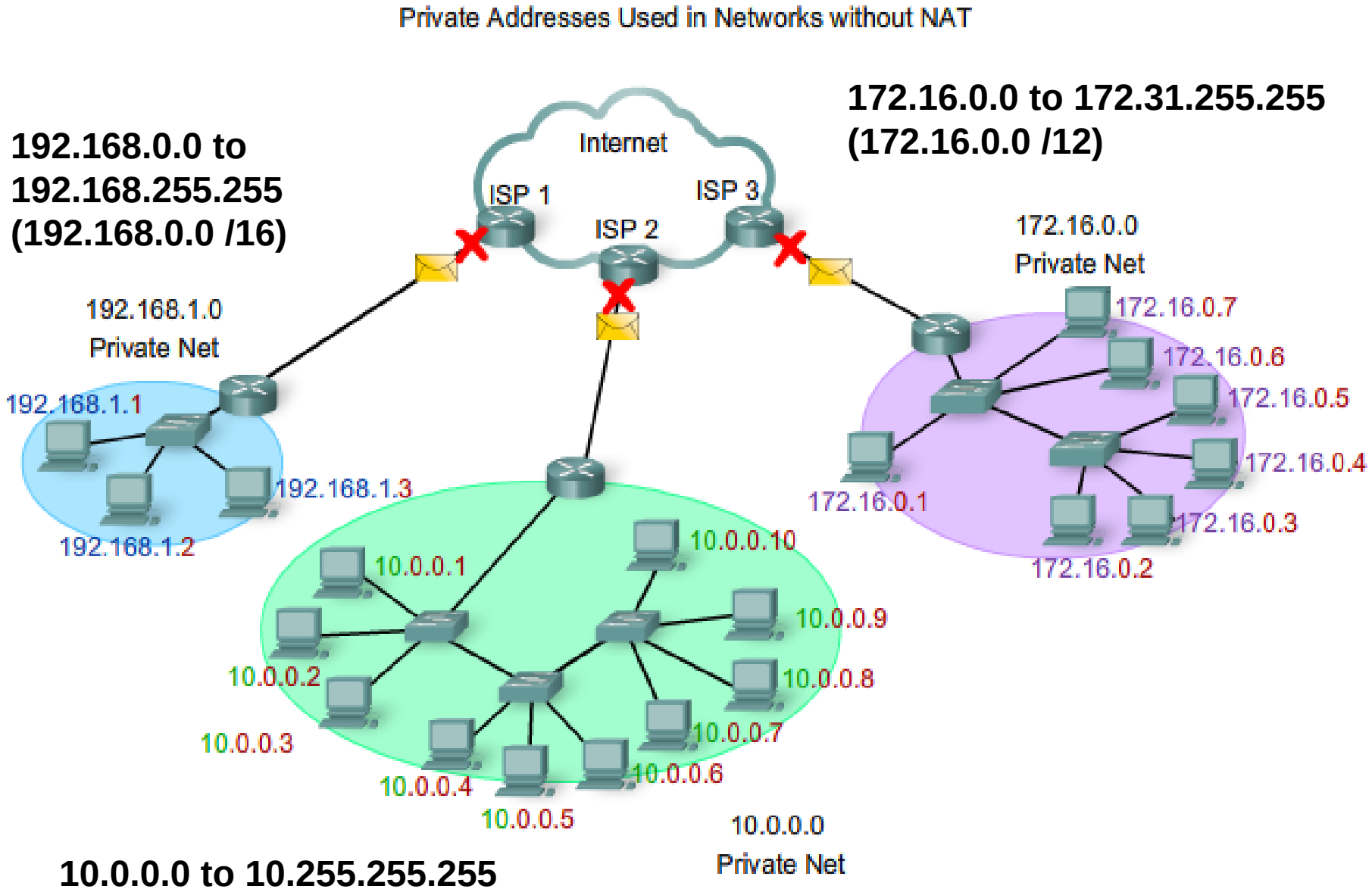
Video and audio distribution
Routing information exchange by routing protocols
Distribution of software
News feeds

6.2.4 RESERVED IPv4 ADDRESS RANGES

Reserved IPv4 Address Ranges

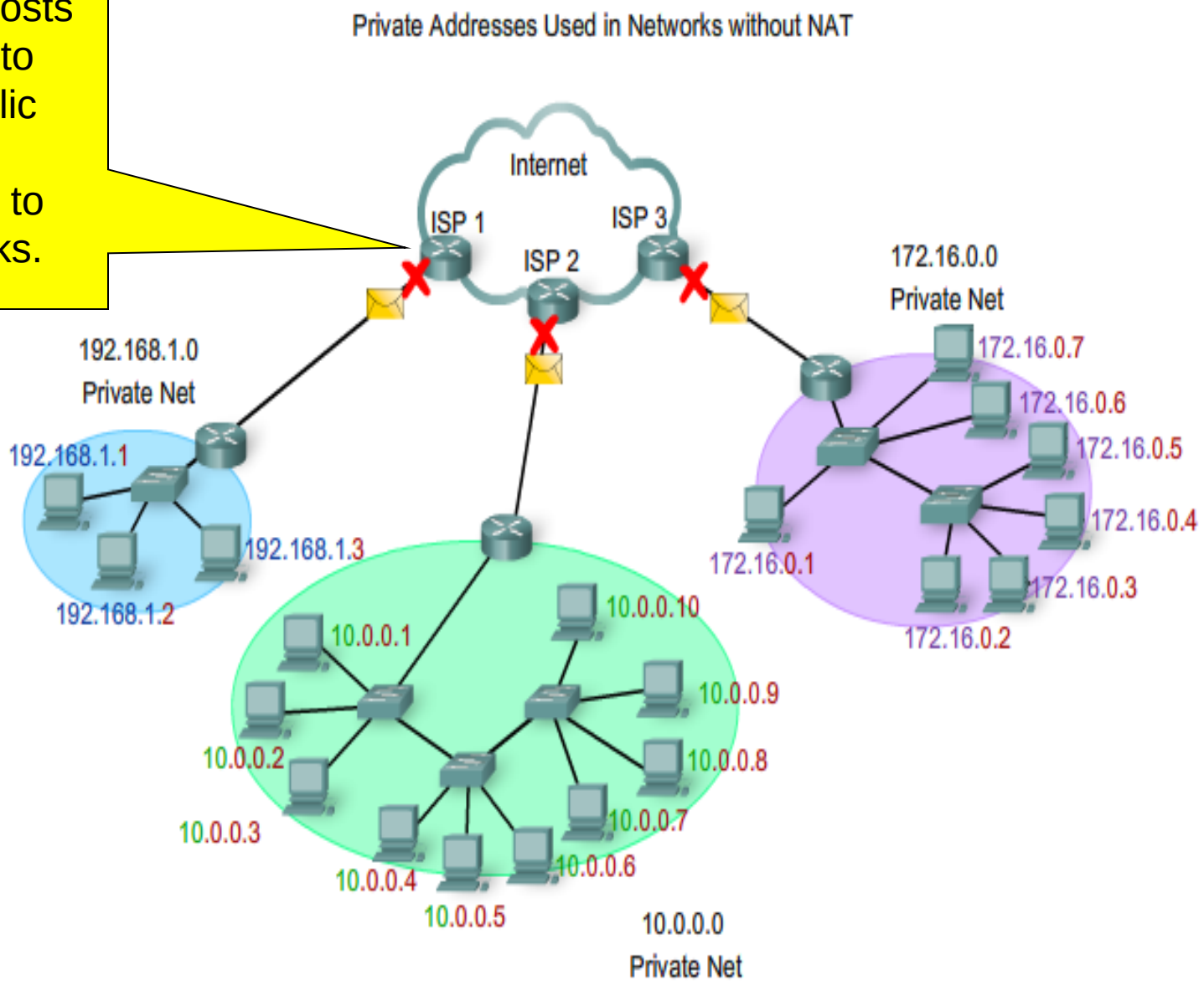
Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	• used for research or experimentation • cannot currently be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

6.2.5 Public and Private Addresses



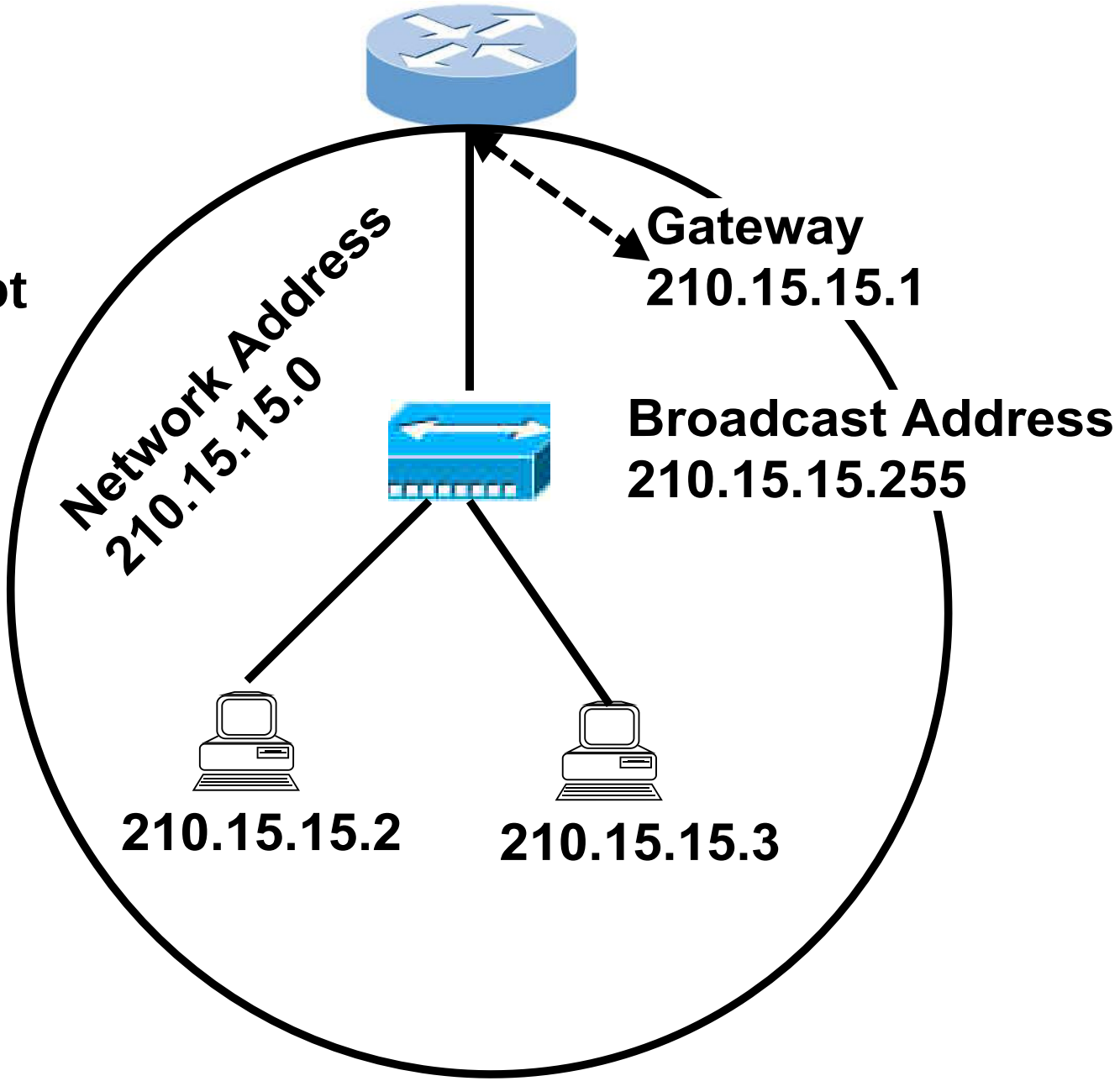
6.2.5 Public and Private Addresses

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



6.2.6 Network Address and Broadcast Address

Within each network the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.



6.2.6 Default and Loopback

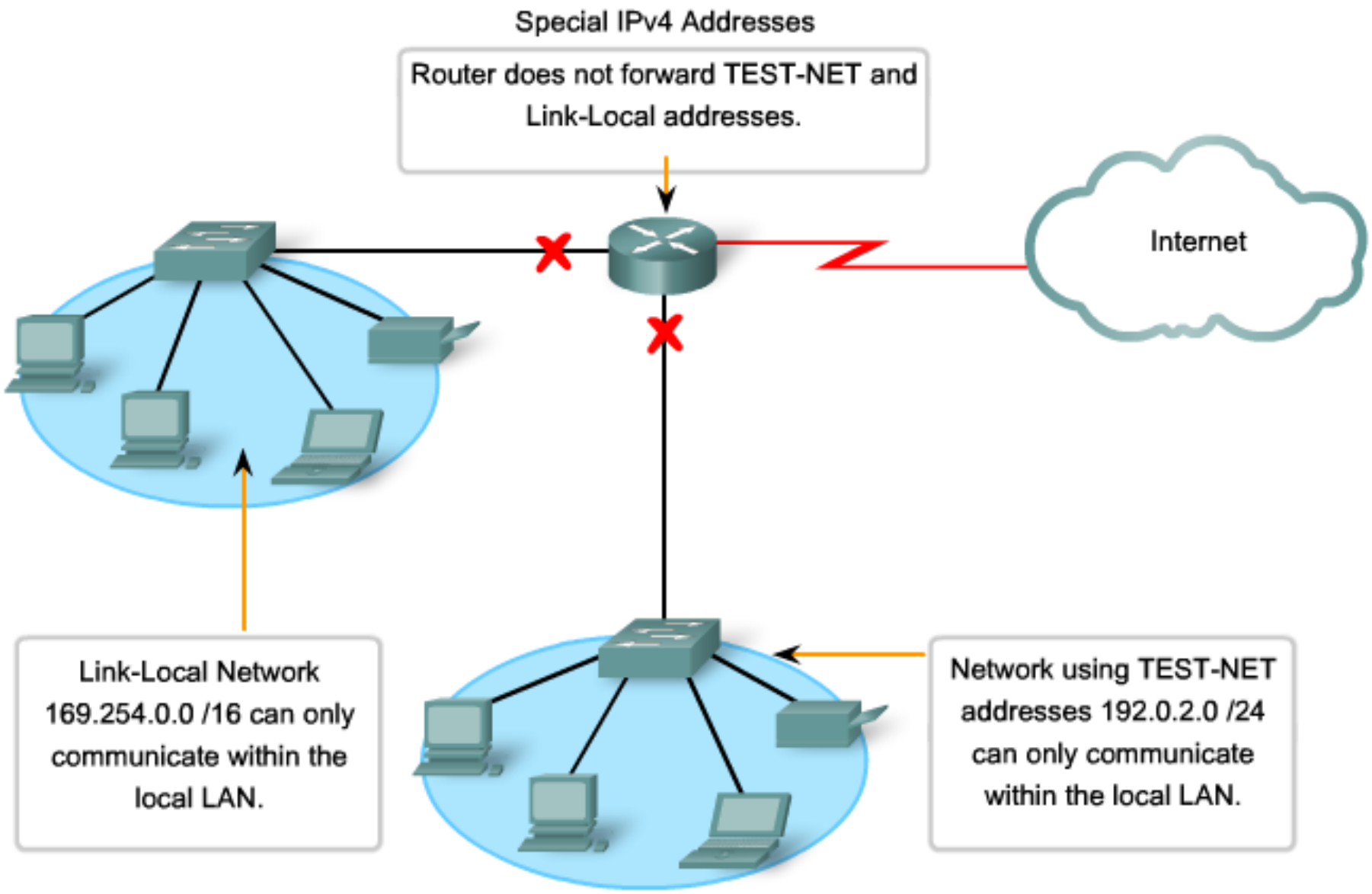
Default Route

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

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.

6.2.6 Special IPv4 Addresses



6.2.7 Legacy IPv4 Addressing

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.

6.3.1 Planning Addresses

Providing and Controlling Access

Some hosts provide resources to the internal network as well as to the external network. One example of these devices is servers.
Addresses for these resources need to be planned and documented
If a server has a random address assigned, blocking access to its address is difficult and clients may not be able to locate this resource.

Monitoring Security and Performance

We need to monitor the security and performance of the network hosts and the network as a whole.
We examine network traffic looking for addresses that are generating or receiving excessive packets

Assigning Addresses within a Network

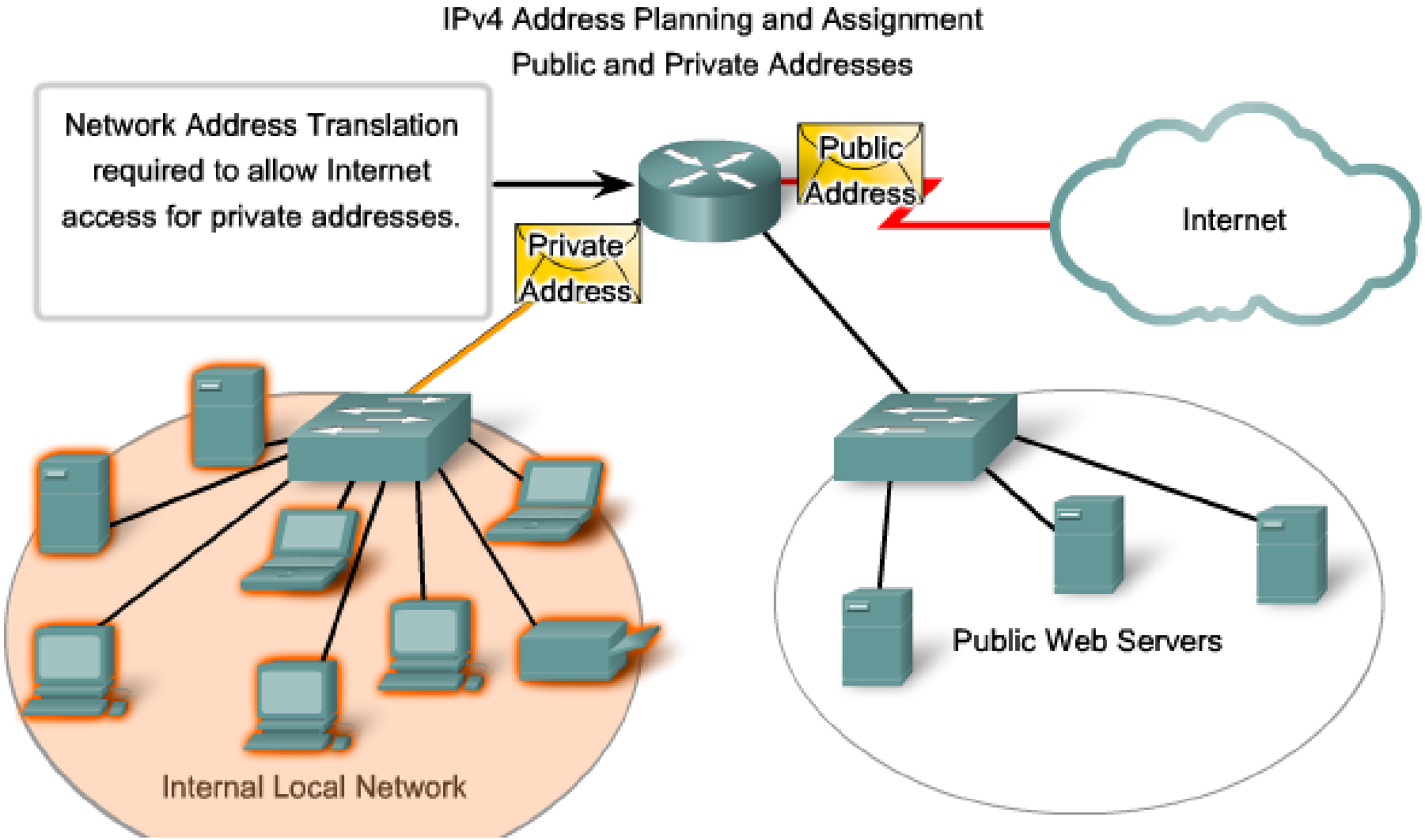
Hosts are associated with an IPv4 network by a common network portion of the address. Within a network, there are different types of hosts.

Some examples of different types of hosts are:

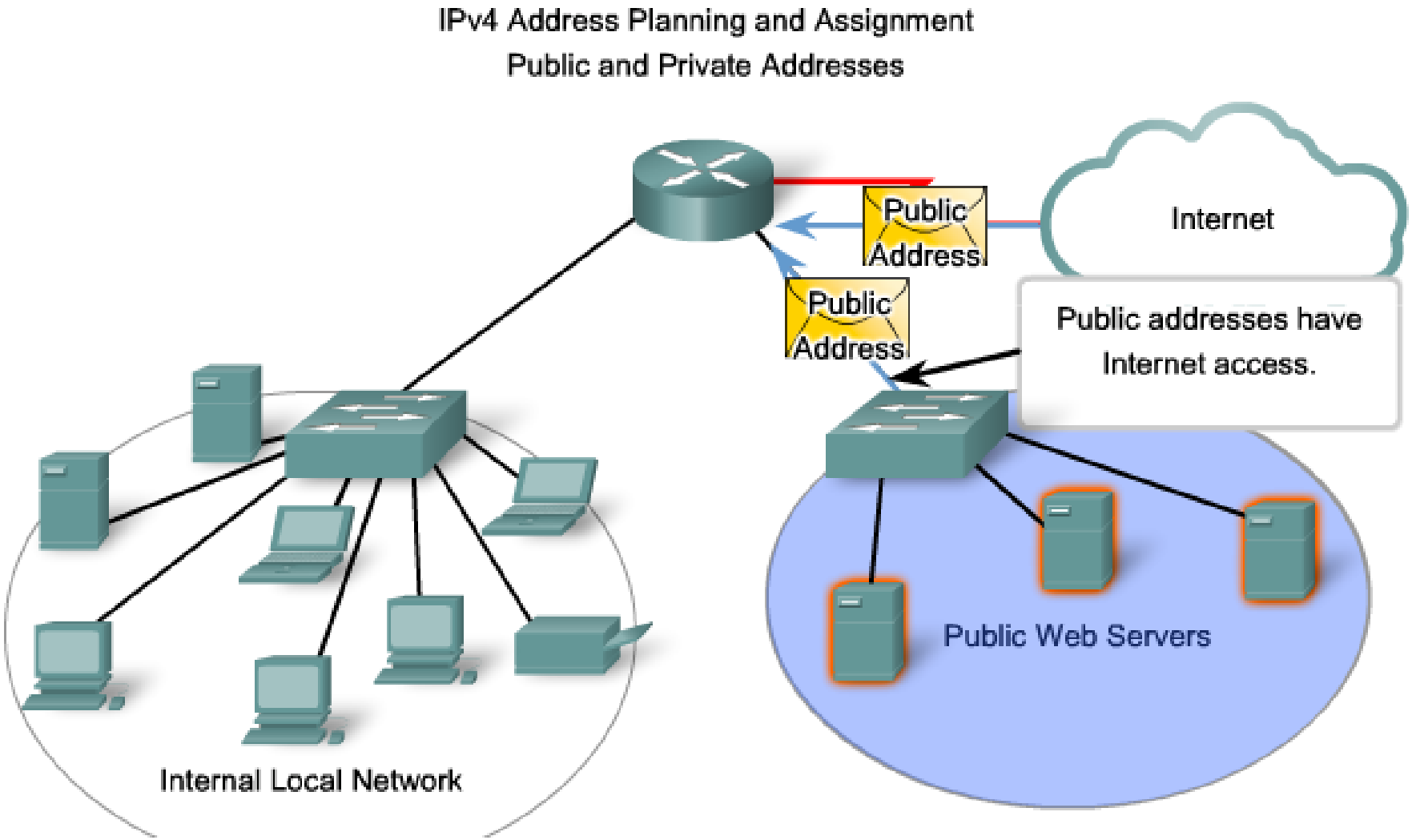
- End devices for users
- Servers and peripherals
- Hosts that are accessible from the Internet
- Intermediary devices

Each of these different device types should be allocated to a logical block of addresses within the address range of the network.

6.3.1 Planning Access to the Network

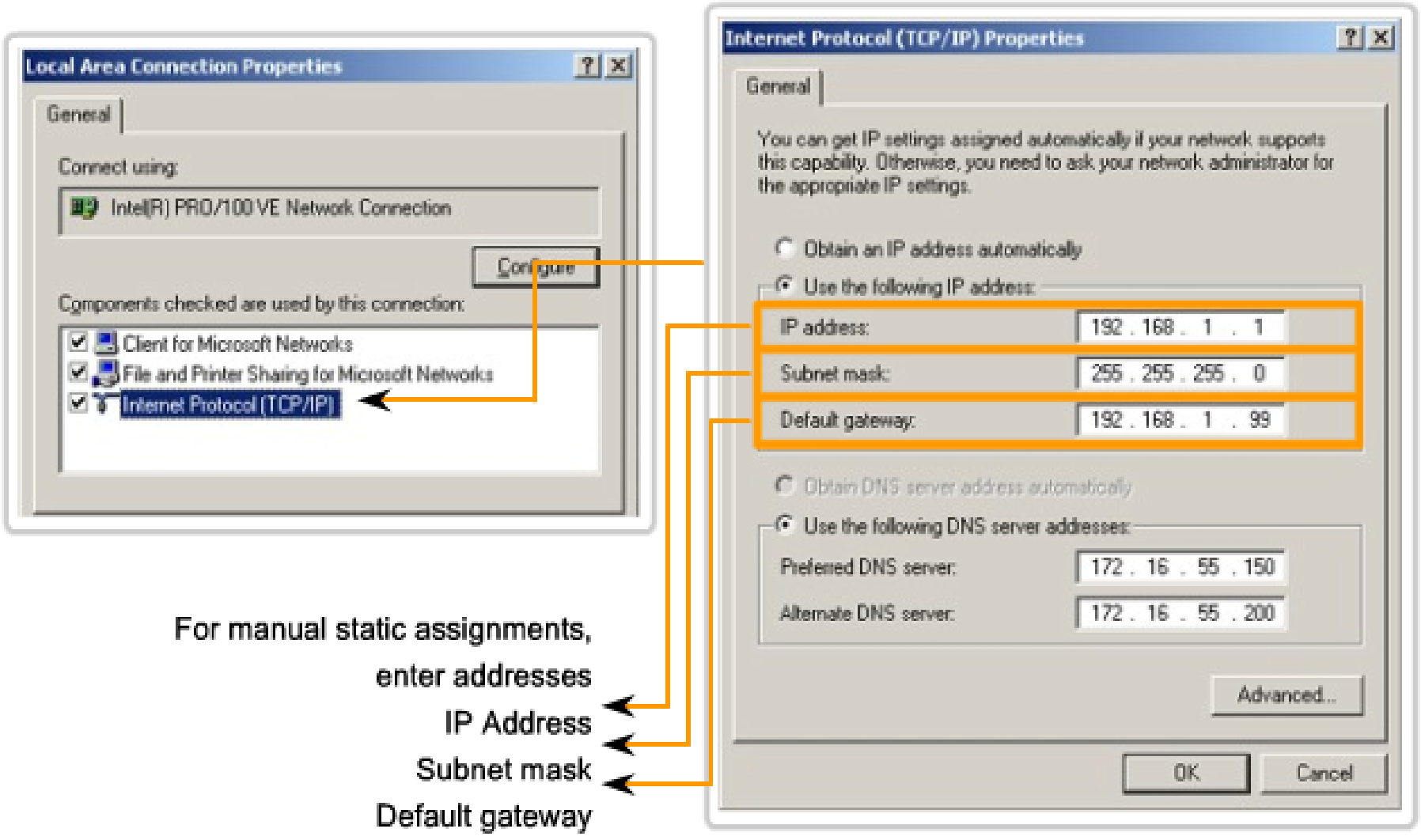


6.3.1 Planning Access to the Network

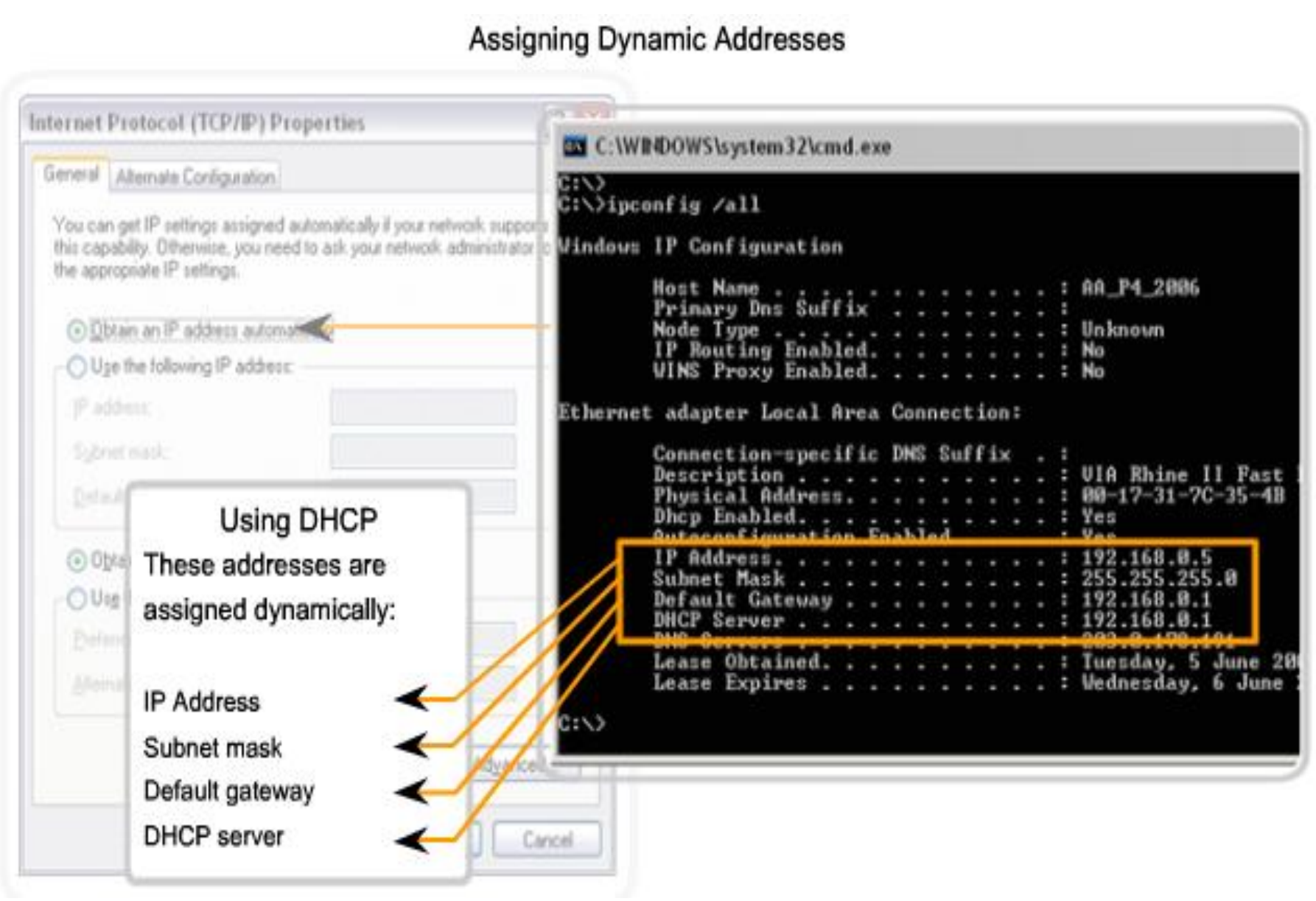


6.3.2 Static and Dynamic Addresses

Addressing End Devices



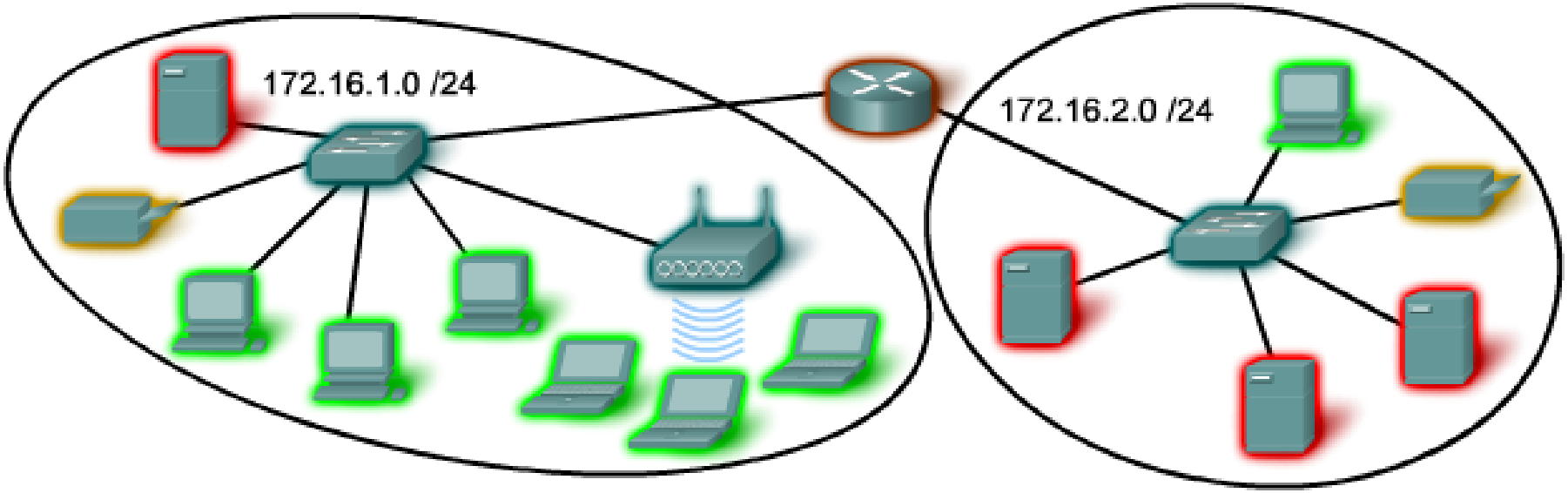
6.3.2 Static and Dynamic Addressing



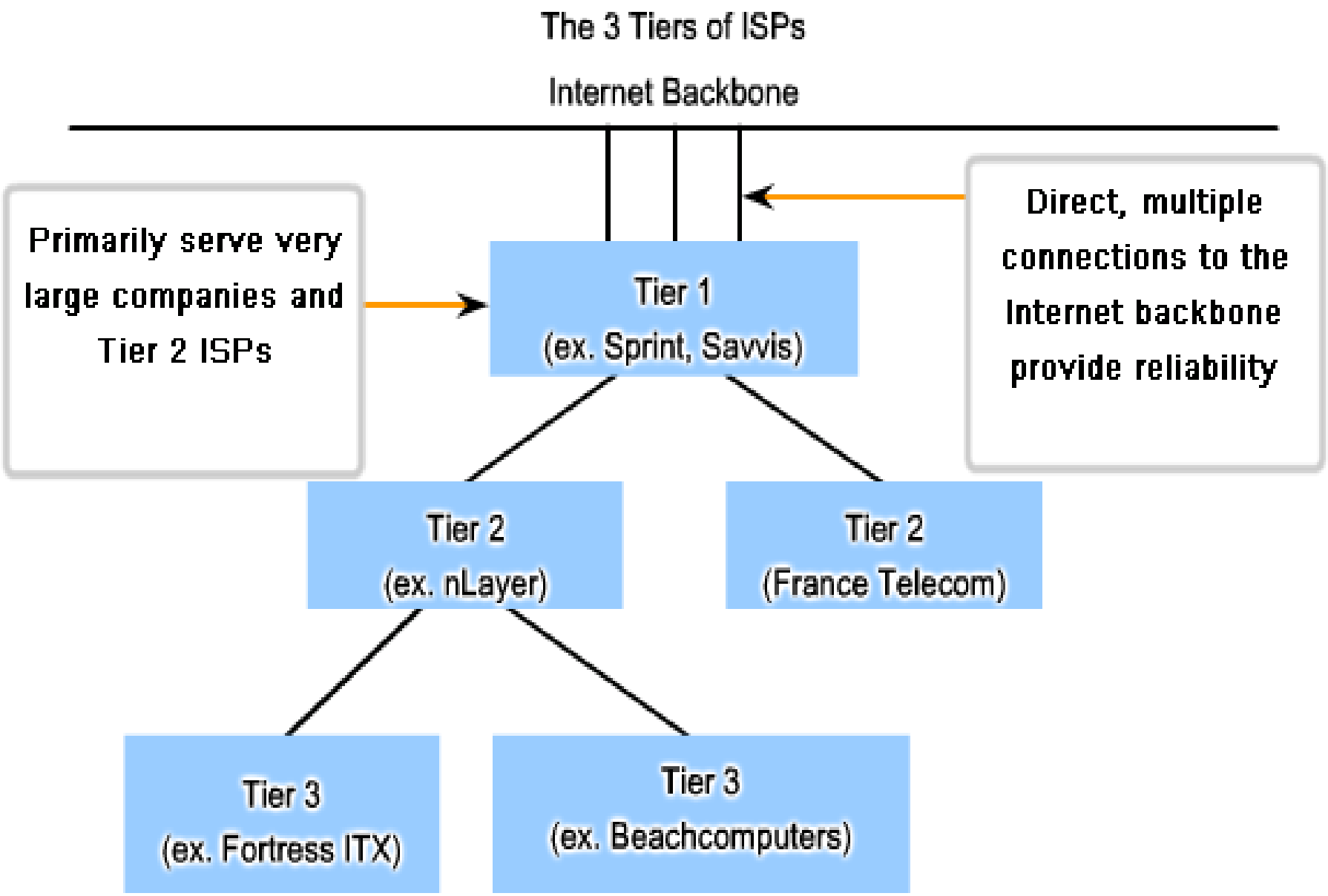
6.3.3 Assigning IP Addresses to other devices

Devices IP Address Ranges

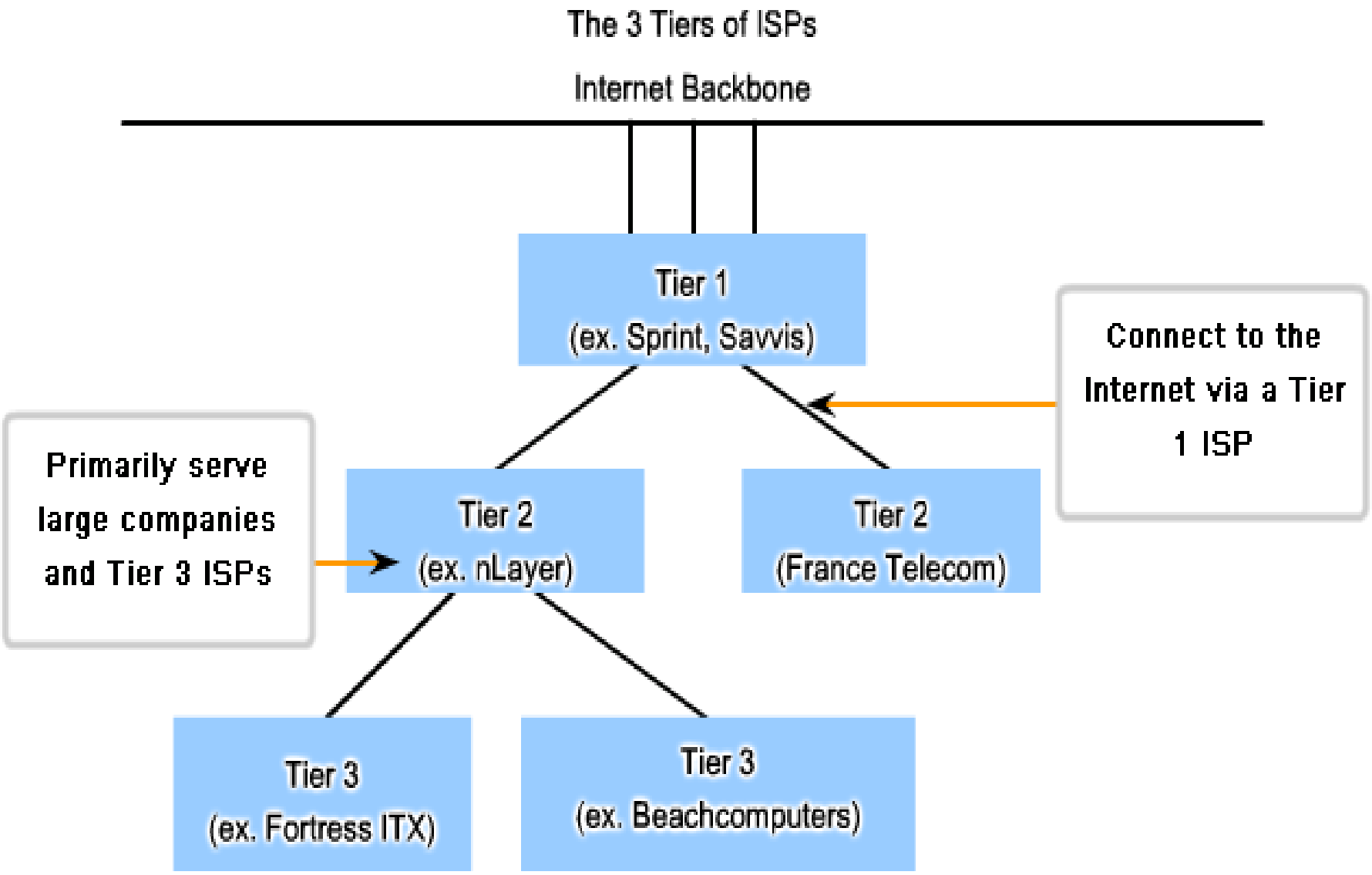
Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224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



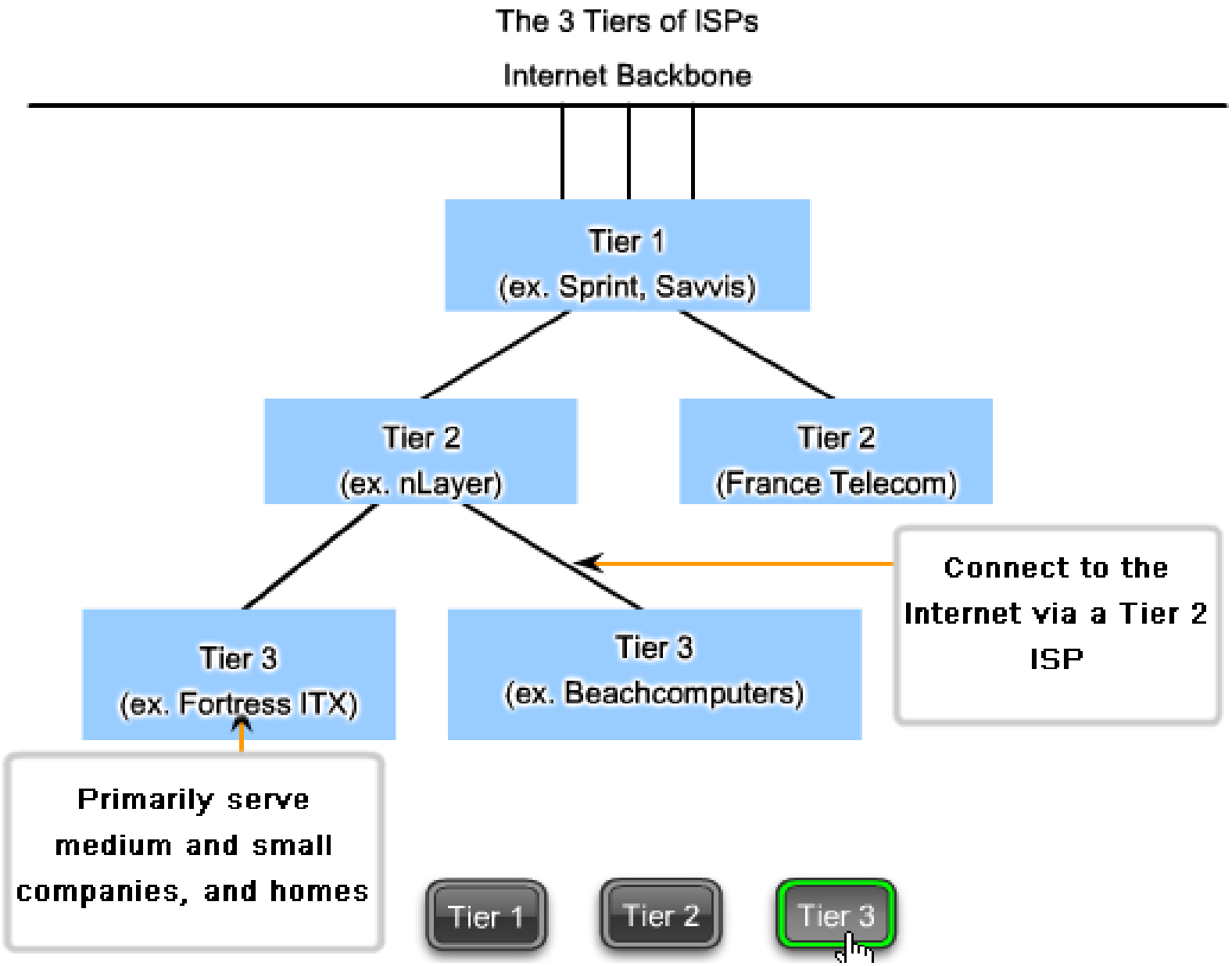
6.3.5 ISP's


The 3 Tiers of ISPs
Internet Backbone
Primarily serve very large companies and Tier 2 ISPs
Tier 1
(ex. Sprint, Savvis)
Direct, multiple connections to the Internet backbone provide reliability
Tier 2
(ex. nLayer)
Tier 2
(France Telecom)
Tier 3
(ex. Fortress ITX)
Tier 3
(ex. Beachcomputers)

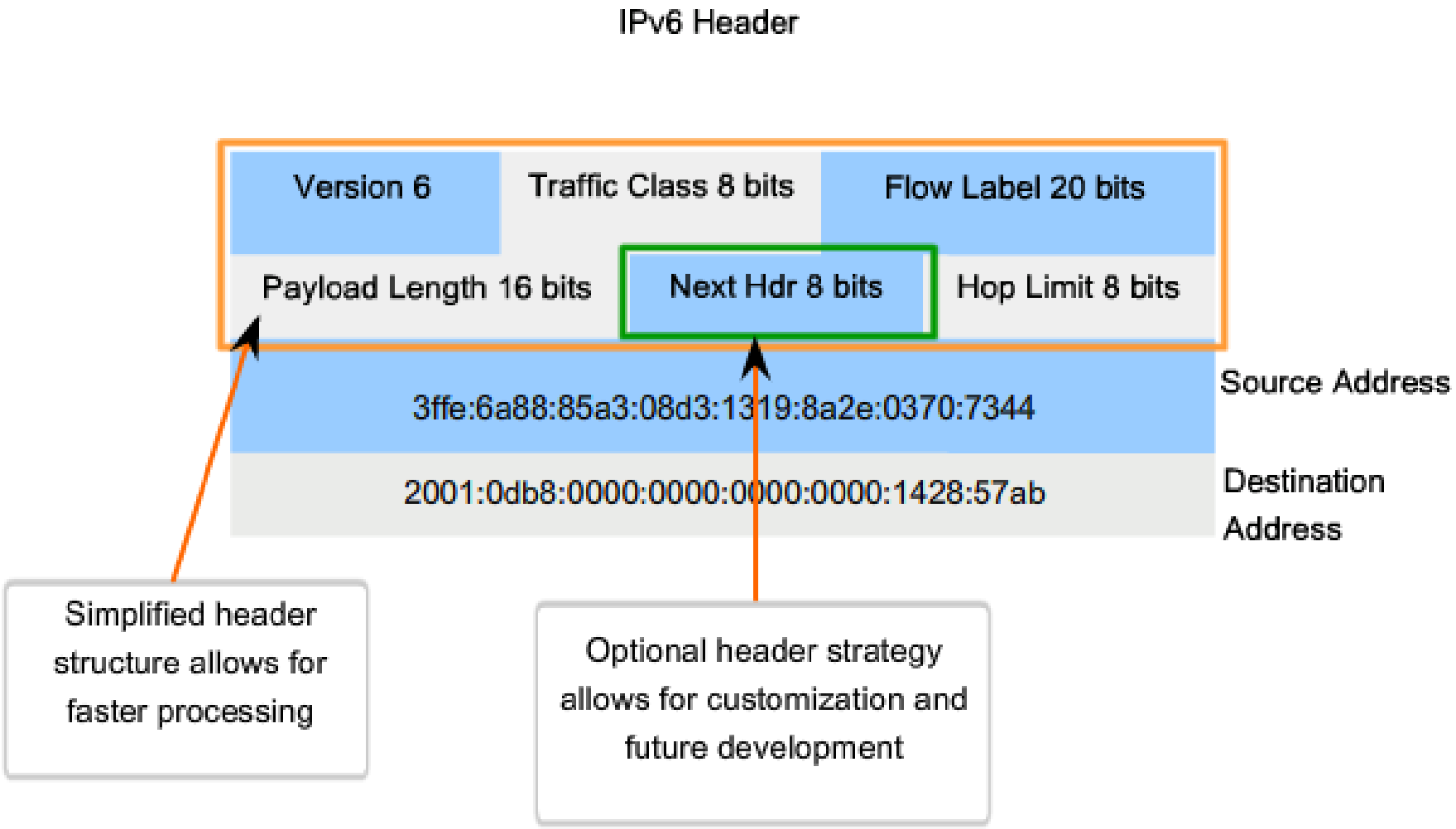
6.3.5 ISP's


The 3 Tiers of ISPs
Internet Backbone
Tier 1
(ex. Sprint, Savvis)
Connect to the Internet via a Tier 1 ISP
Primarily serve large companies and Tier 3 ISPs
Tier 2
(ex. nLayer)
Tier 2
(France Telecom)
Tier 3
(ex. Fortress ITX)
Tier 3
(ex. Beachcomputers)

6.3.5 ISP's


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)
Connect to the Internet via a Tier 2 ISP
Primarily serve medium and small companies, and homes
Tier 1
Tier 2
Tier 3

6.3.6 IPv6


IPv6 Header
Version 6
Traffic Class 8 bits
Flow Label 20 bits
Payload Length 16 bits
Next Hdr 8 bits
Hop Limit 8 bits
3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344
Source Address
2001:0db8:0000:0000:0000:0000:1428:57ab
Destination Address
Simplified header structure allows for faster processing
Optional header strategy allows for customization and future development

6.3.6 IPv6

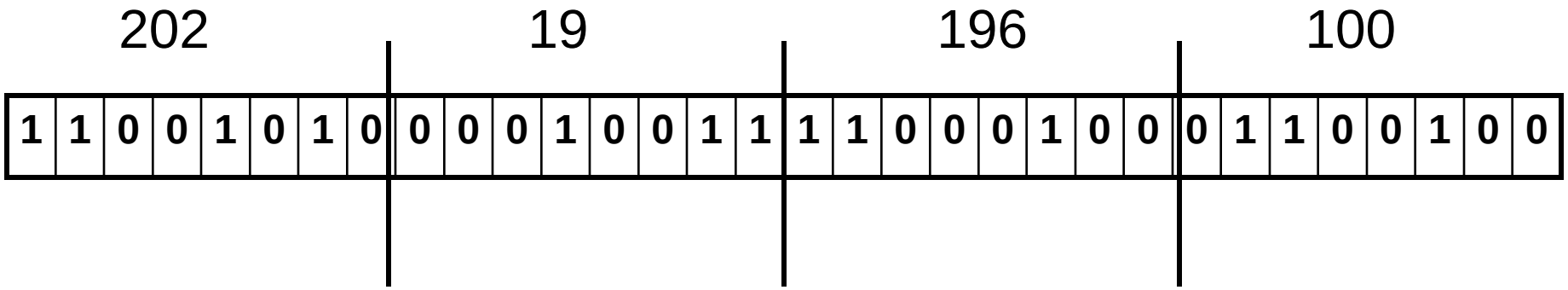
IPv6 – 128 bits long, in hex – 16 bit fields

6.4.1 Subnet Mask

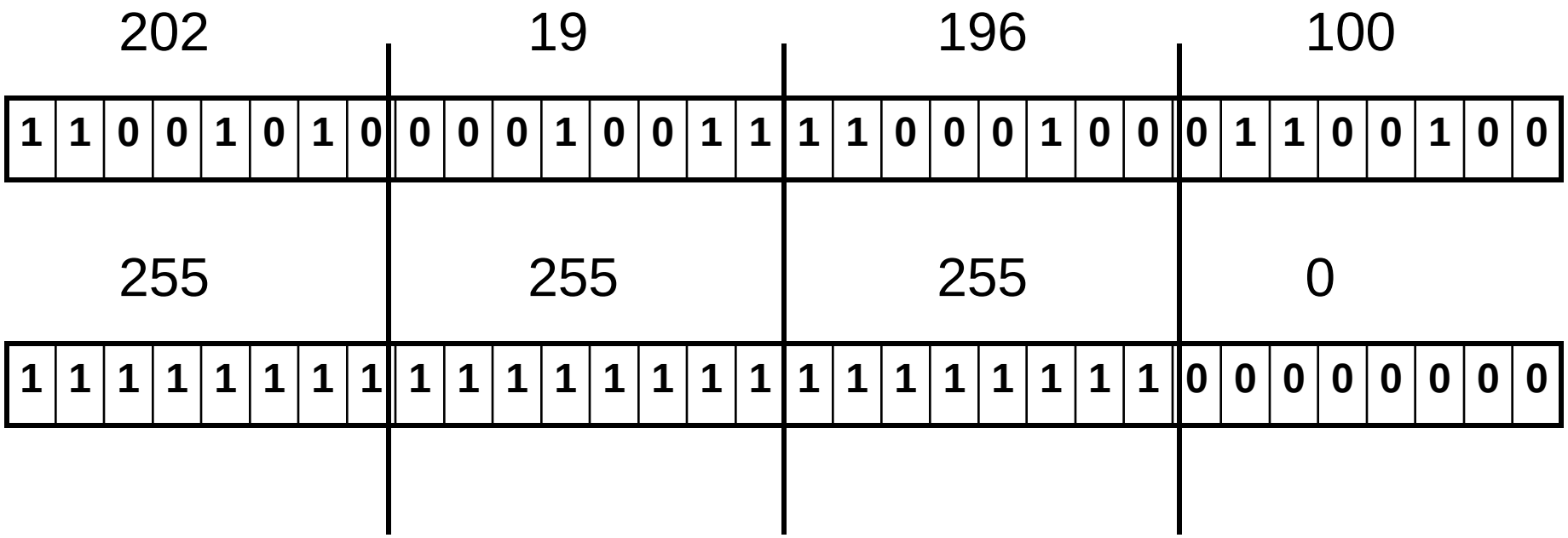
Address
172.16.20.35
10101100.00010000.00010100.00100011

Subnet mask
255.255.255.224
11111111.11111111.11111111.11100000
or
172.16.20.35/27

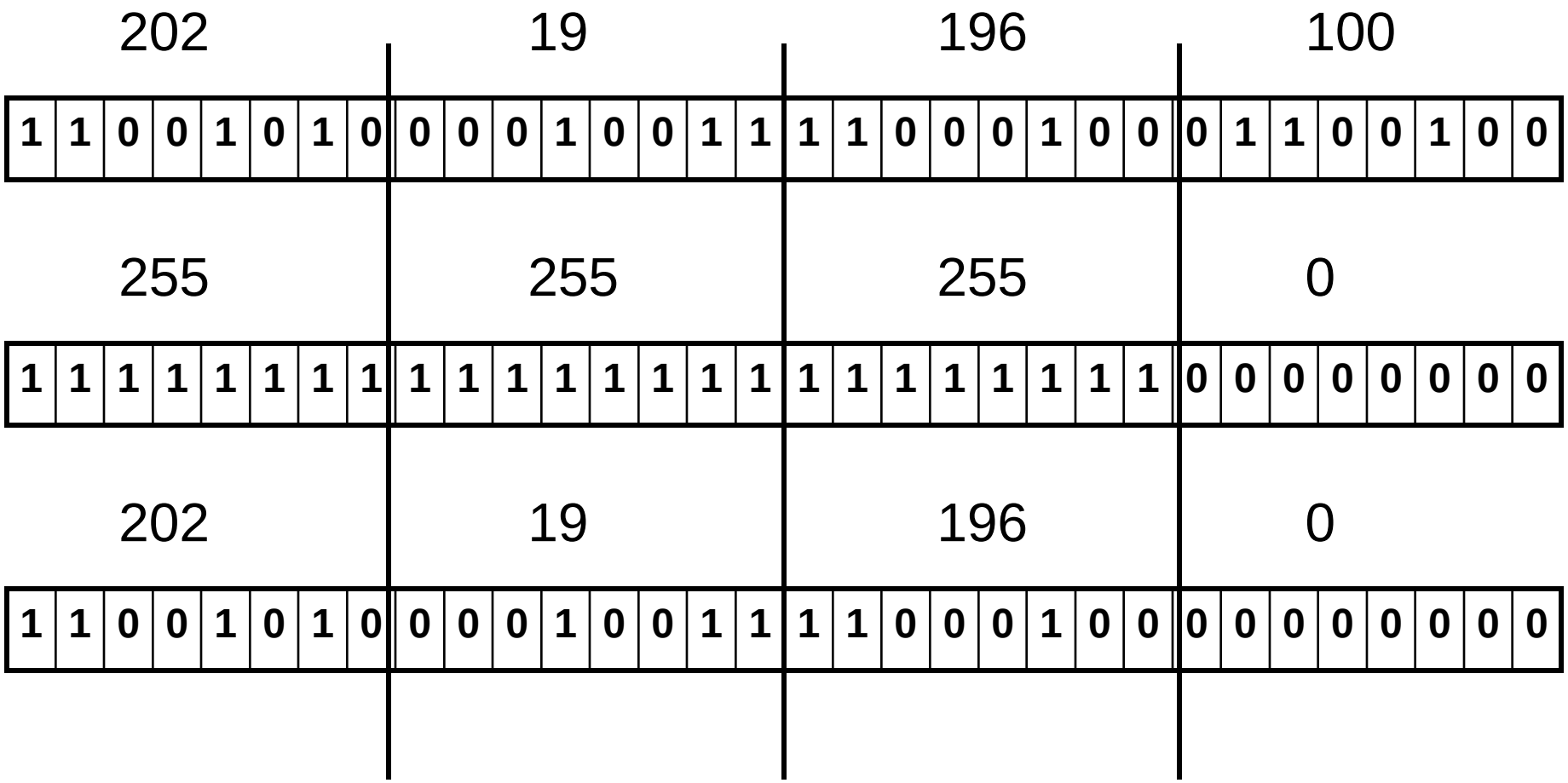
IP Address

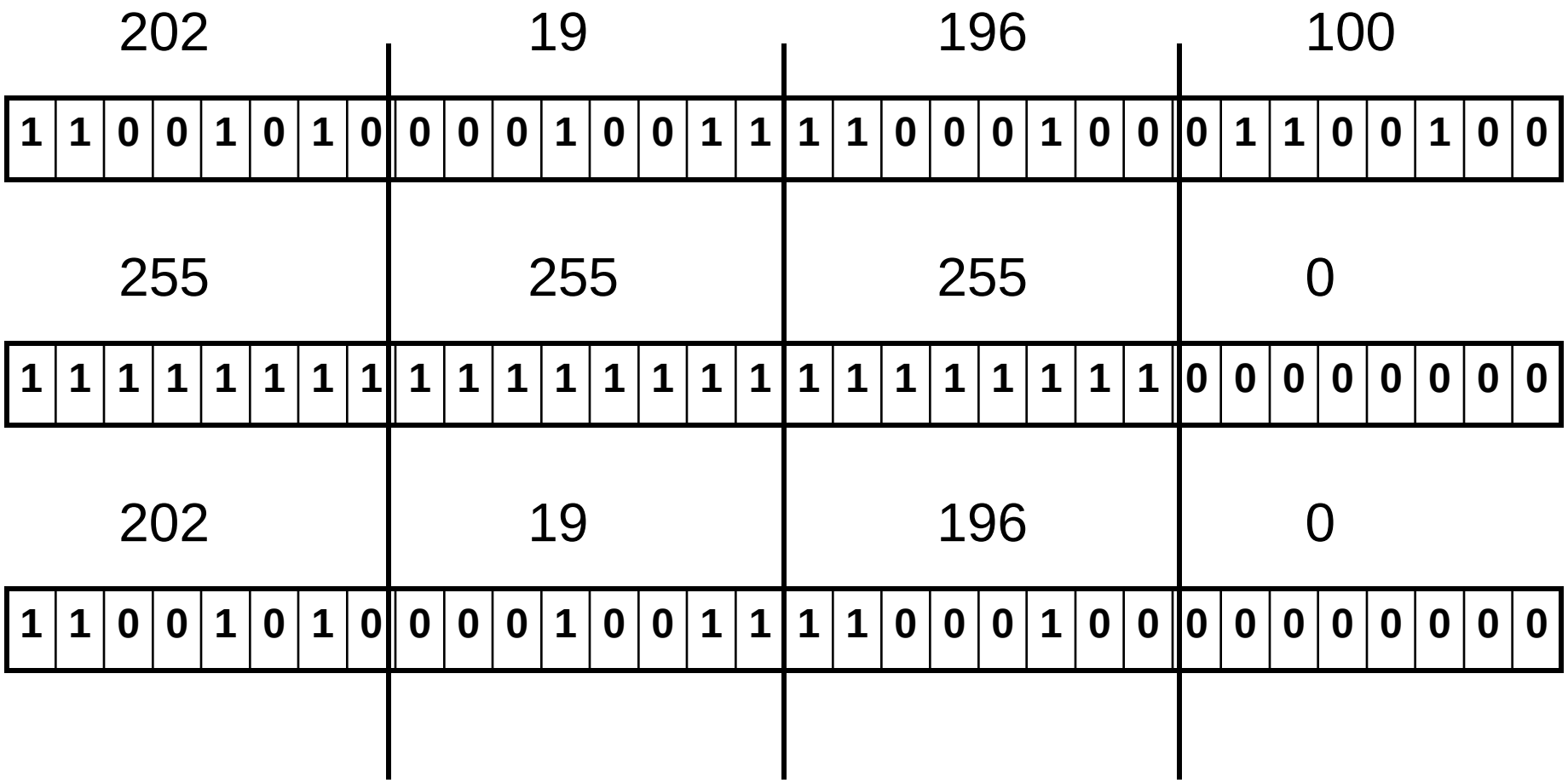


IP Address & Subnet Mask



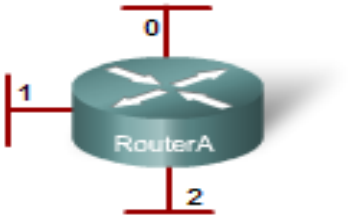
IP Address & Subnet Mask used to extract Network Address




202
19
196
100
1 1 0 0 1 0 1 0
0 0 0 1 0 0 1 1
1 1 0 0 0 1 0 0
0 1 1 0 0 1 0 0
255
255
255
0
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
0 0 0 0 0 0 0 0
202
19
196
0
1 1 0 0 1 0 1 0
0 0 0 1 0 0 1 1
1 1 0 0 0 1 0 0
0 0 0 0 0 0 0 0

6.5.1 Basic Subnetting

Borrowing Bits for Subnets



-	192.168.1.0 (/24) 255.255.255.0	Address: Mask:	11000000.10101000.00000001.00000000 11111111.11111111.11111111.00000000
0	192.168.1.0 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00000001.00000000 11111111.11111111.11111111.11000000
1	192.168.1.64 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00000001.01000000 11111111.11111111.11111111.11000000
2	192.168.1.128 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00000001.10000000 11111111.11111111.11111111.11000000
3	192.168.1.192 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00000001.11000000 11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

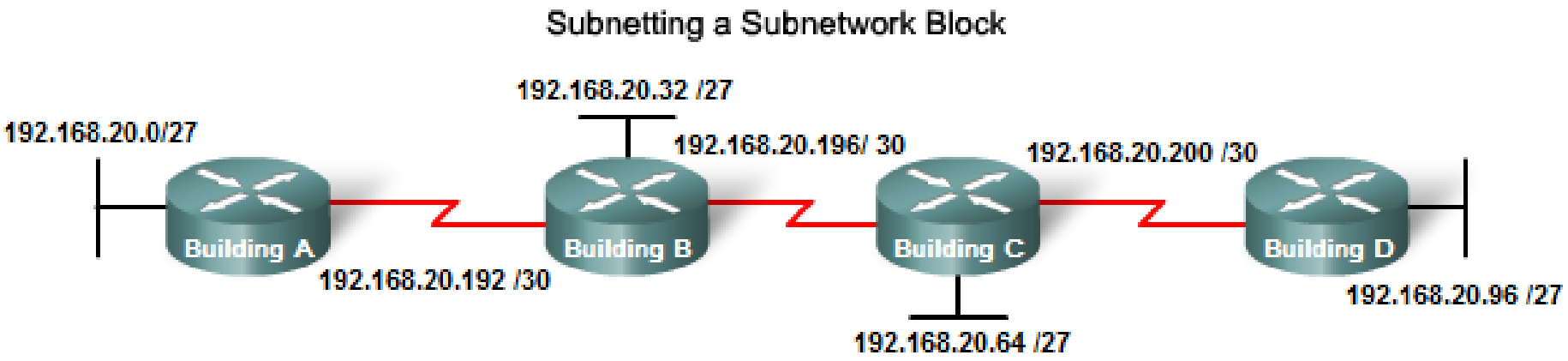
A 1 in these positions in the mask means that these values are part of the network address.

More subnets are available, but fewer addresses are available per subnet.

Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

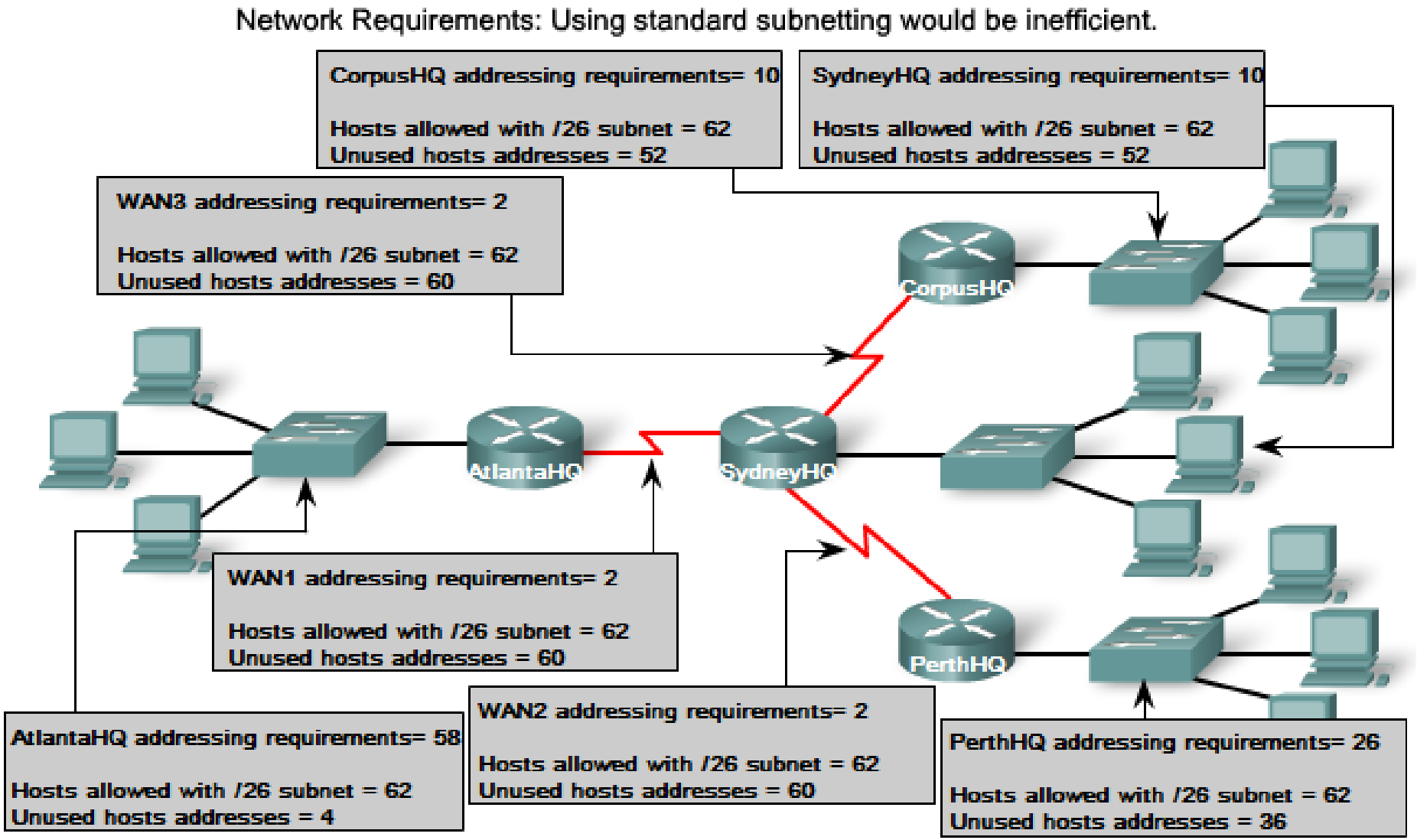
6.5.3 Subnetting a Subnet



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	192.168.20.220/30

6.5.3 Subnetting a Subnet



6.5.3 Subnetting a Subnet

ORIGINAL ADDRESS 192.168.15.0/24
ADDRESS RANGE 192.168.15.0 TO 256
NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

	Actual Requirements	Total Wasted Addresses
AtlantaHQ	58 host addresses	4 addresses
PerthHQ	26 host addresses	36 addresses
SydneyHQ	10 host addresses	52 addresses
CorpusHQ	10 host addresses	52 addresses
WAN links	2 host addresses (each)	60 addresses

6.5.3 Subnetting a Subnet

ORIGINAL ADDRESS 192.168.15.0/24
NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Name -required addresses	Subnet address	Address range	Broadcast Address	Network /prefix
AtlantaHQ - 58				
PerthHQ - 28				
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

STEP 1
Sort the networks according to the required host addresses
Largest to smallest number of hosts

On your documentation list your requirements in descending order.

6.5.3 Subnetting a Subnet

ATLANTA ADDRESS 192.168.15.0/26
192.168.15.0 TO 63
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNHHHHHH

Name -required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28				
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Calculate the subnet mask to meet largest requirement - AtlantaHQ

6.5.3 Subnetting a Subnet

PERTH ADDRESS 192.168.15.64/27
192.168.15.64 TO 95
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNHHHHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Use the next available Address .64 to calculate a subnet mask for the next largest requirement - PerthHQ.

6.5.3 Subnetting a Subnet

SYDNEY ADDRESS 192.168.15.96/28
192.168.15.96 TO 111
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNNHHHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Sydney needs 12 addresses. Use the next available address .96 to calculate a subnet for SydneyHQ requirement of 10 hosts.

6.5.3 Subnetting a Subnet

CORPUS ADDRESS 192.168.15.112/28
192.168.15.112 TO 127
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNNHHHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Use the next available address .112 to calculate a subnet for CorpusHQ which also requires 10 hosts.

6.5.3 Subnetting a Subnet

WAN1 ADDRESS 192.168.15.128/30
192.168.15.128 TO 131
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNNNNHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2				
WAN3 - 2				

WAN links require 2 addresses each

6.5.3 Subnetting a Subnet

WAN2 ADDRESS 192.168.15.132/30
192.168.15.132 TO 135
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNNNNHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2	192.168.15.132	.133 - 134	.135	192.168.15.132 /30
WAN3 - 2				

6.5.3 Subnetting a Subnet

WAN3 ADDRESS 192.168.15.136/30
192.168.15.136 TO 139
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNNNNNHH

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2	192.168.15.132	.133 - 134	.135	192.168.15.132 /30
WAN3 - 2	192.168.15.136	.137 - .138	.139	192.168.15.136 /30

The networking problem is solved

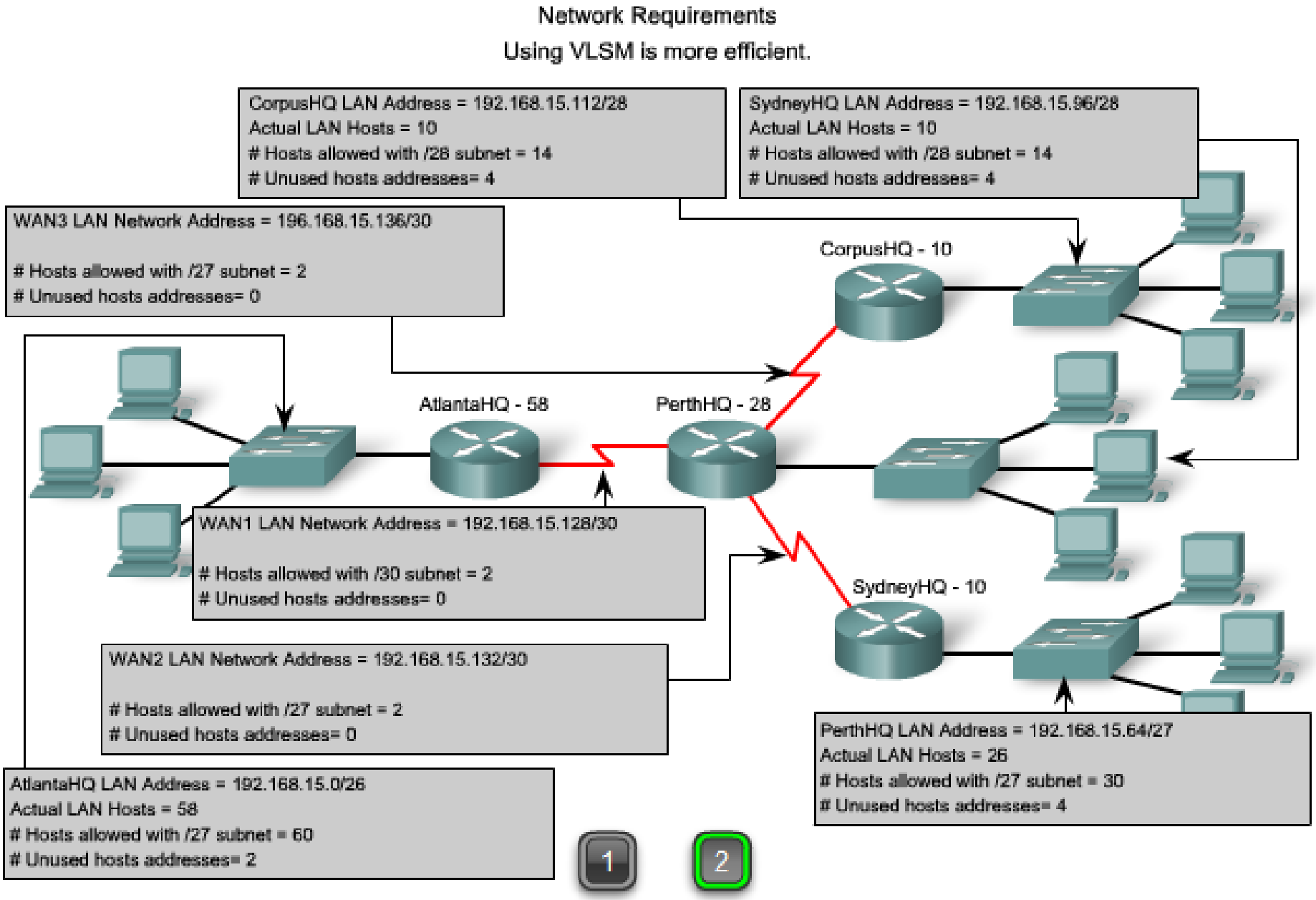
6.5.3 Subnetting a Subnet

Network Requirements

Using VLSM is more efficient.

Name -required addresses	Subnet address	Address range	Broadcast Address	Network /prefix
AtlantaHQ - 58	192.168.15.0	.1-.62	.63	192.168.15.0/26
PerthHQ - 28	192.168.15.64	.65-.94	.95	192.168.15.64/27
SydneyHQ - 10	192.168.15.96	.97-.110	.111	192.168.15.96/28
CorpusHQ - 10	192.168.15.112	.113-.126	.127	192.168.15.112/28
WAN1 - 2	192.168.15.128	.129-.130	.131	192.168.15.128/30
WAN2 - 2	192.168.15.132	.133-.134	.135	192.168.15.132/30
WAN3 - 2	192.168.15.136	.137-.138	.139	192.168.15.136/30

6.5.3 Subnetting a Subnet



6.5.3 Subnetting a Subnet

Using VLSM to allocate the addresses made it possible to apply the subnetting guidelines for grouping hosts based on:

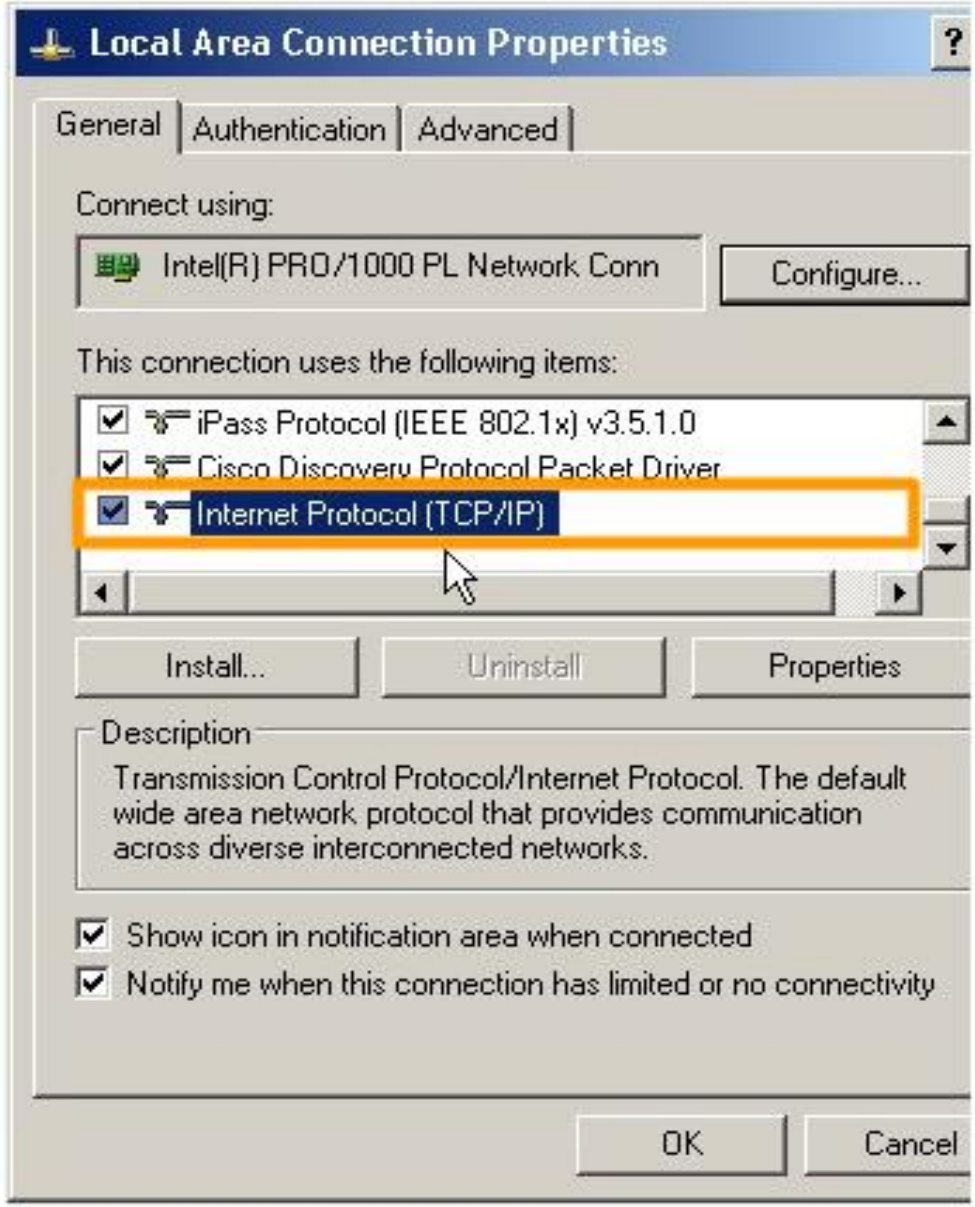
- Grouping based on common geographic location
- Grouping hosts used for specific purposes
- Grouping based on ownership

6.6.1 Ping

Testing Local TCP/IP Stack

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

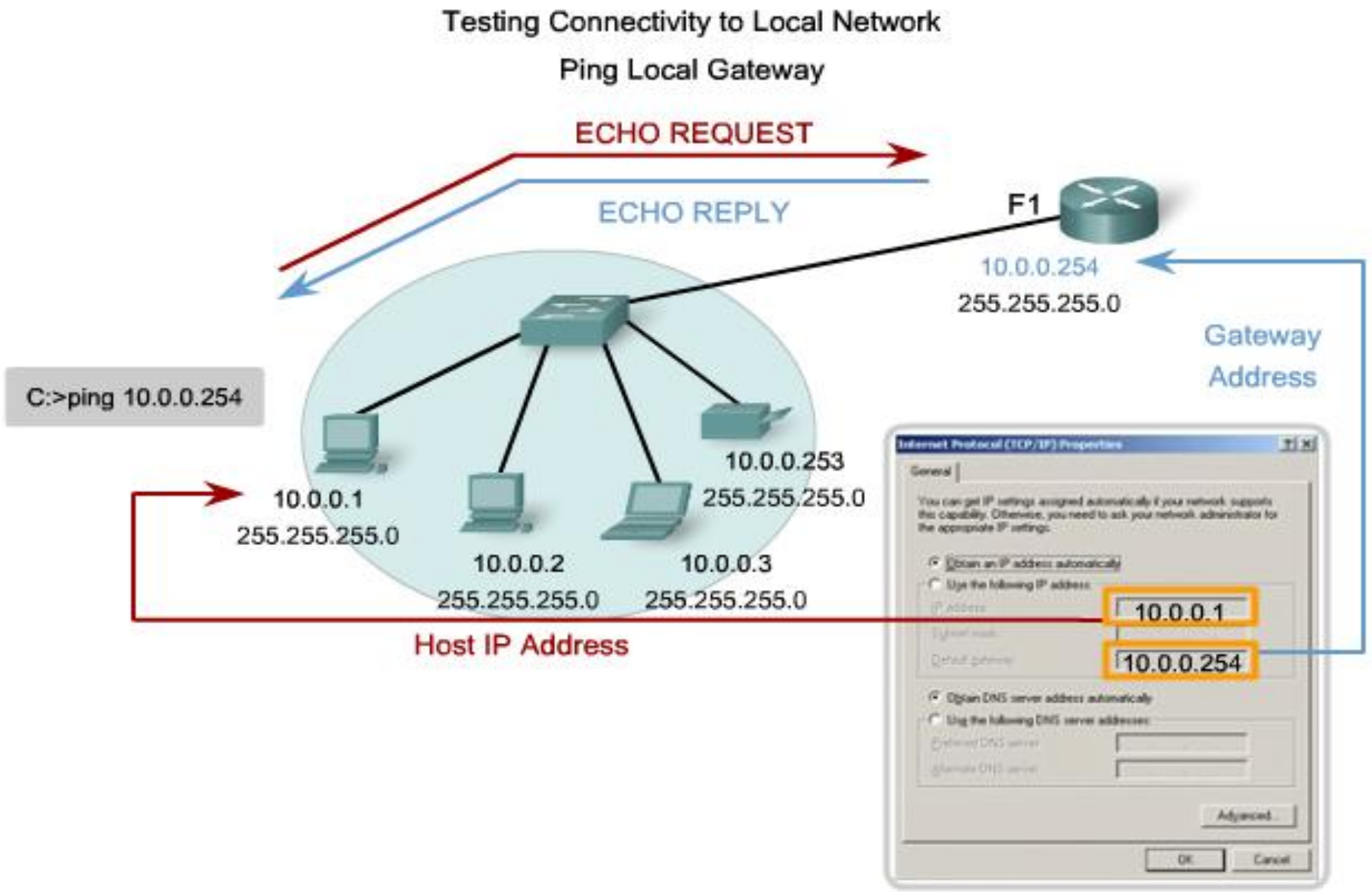
Pinging 127.0.0.1 causes a device to ping itself.



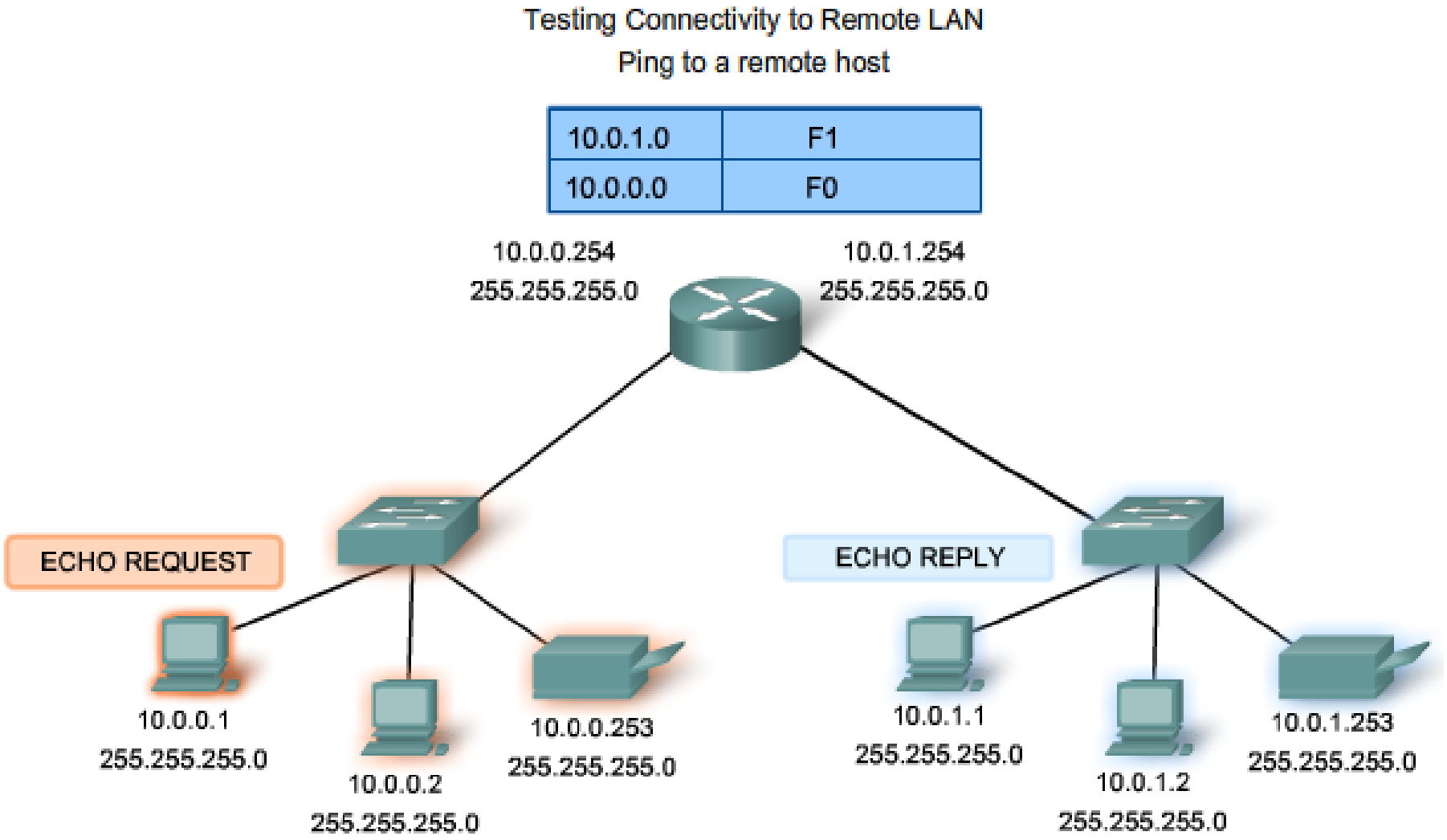
6.6.1 Ping

- A response from 127.0.0.1 indicates that IP is properly installed on the host.
- This response comes from the Network layer.
- This response is not an indication that the addresses, masks, or gateways are properly configured.
- Does not indicate anything about the status of the lower layer of the network stack.
- Simply tests IP down through the Network layer of the IP protocol.
- If we get an error message, it is an indication that TCP/IP is not operational on the host.

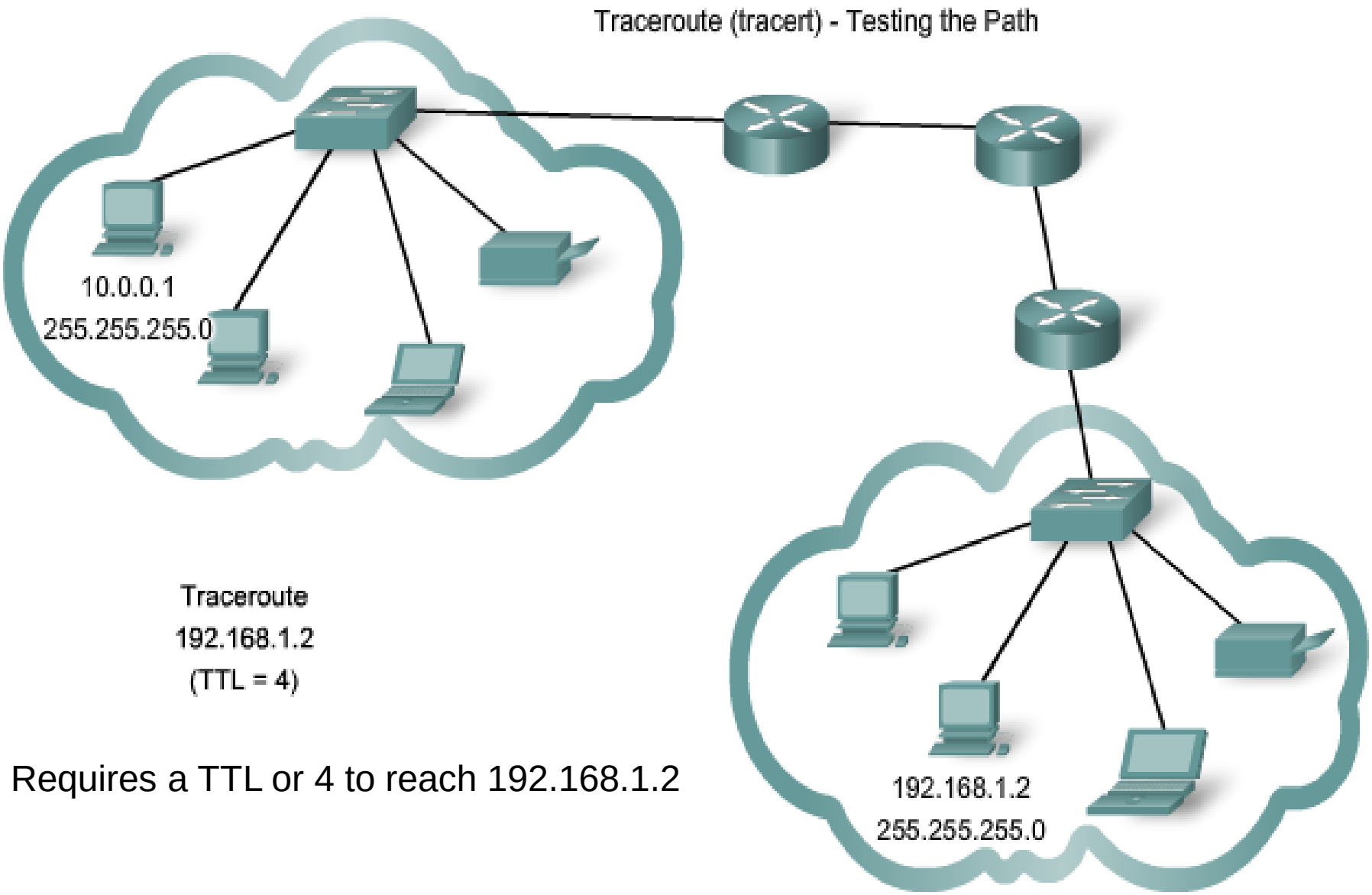
6.6.2 Pinging the Gateway



6.6.3 Pinging a remote host

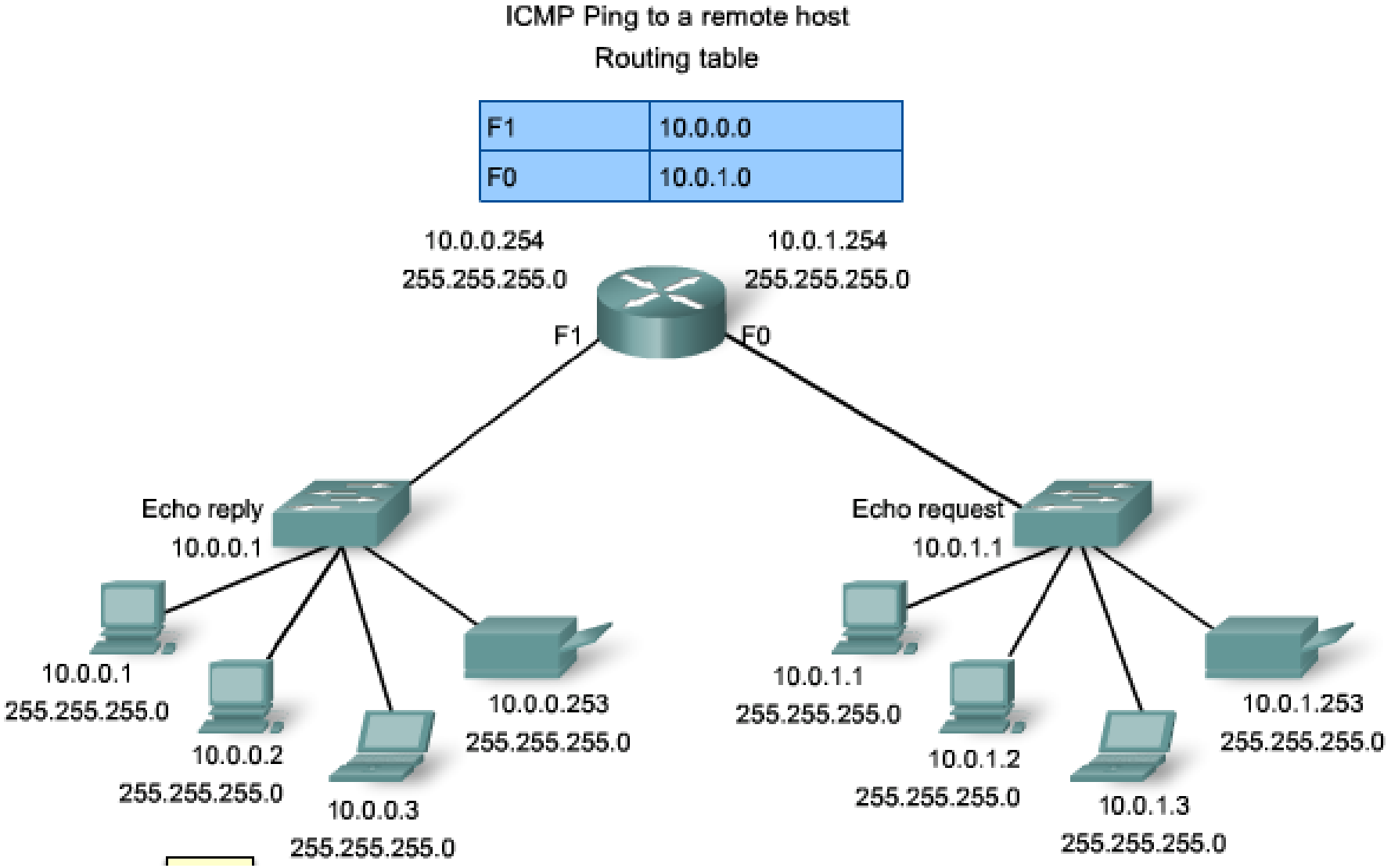


6.6.4 Tracert (Testing the Path)



Requires a TTL or 4 to reach 192.168.1.2

6.6.5 ICMP testing



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.