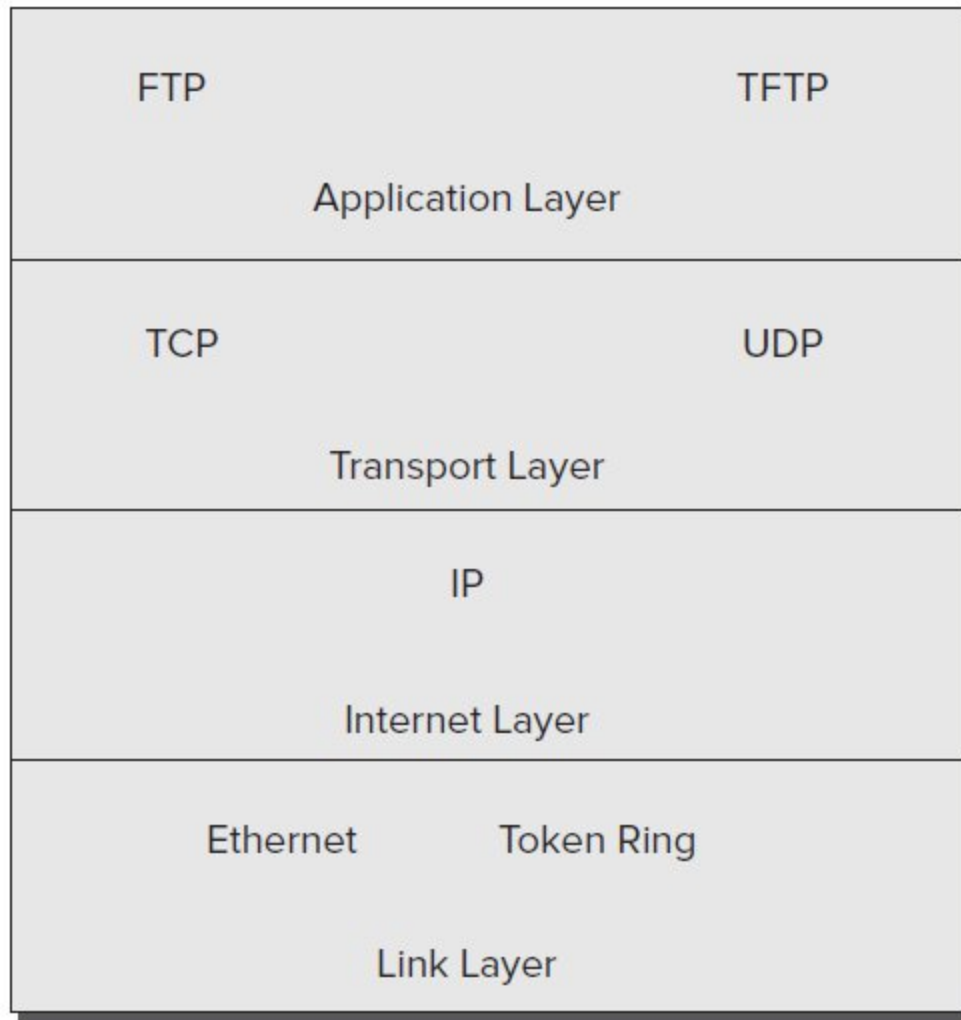


# MCA: Windows Server Hybrid Administrator Study Guide: AZ-800 & AZ-801

## Chapter 4: Understanding IP

# Understanding TCP/IP



# Application Layer

- The Application layer is where the applications that use the protocol stack reside
- These applications include
  - File Transfer Protocol (FTP)
  - Trivial File Transfer Protocol (TFTP)
  - Simple Mail Transfer Protocol (SMTP)
  - Hypertext Transfer Protocol (HTTP).

# Transport Layer

- Two Transport Layer protocols reside:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- TCP is a connection oriented protocol
  - Delivery is guaranteed.
- UDP is a connectionless protocol
  - Does its best job to deliver the message but there is no guarantee

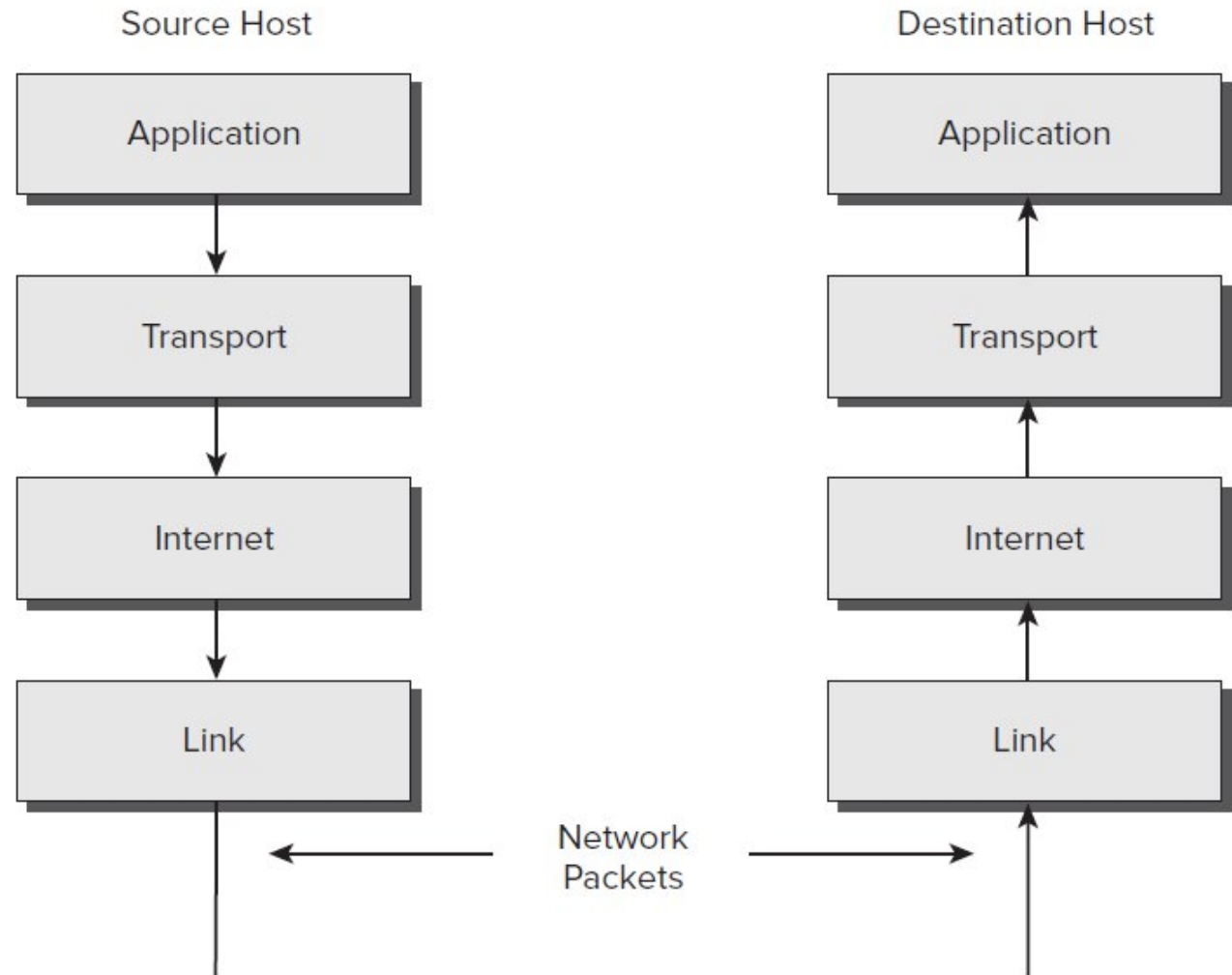
# Internet Layer

- Where the IP protocol resides
- The IP protocol is a connectionless protocol that relies on the upper layer (Transport Layer) for guarantee of delivery
- Address Resolution Protocol (ARP) also resides on this layer
- ARP turns an IP address into a Media Access Control (MAC) address
- All upper and lower layers travel through the IP protocol.

# Link Layer

- The data link protocols like Ethernet and Token Ring reside in the Link layer
- This layer is also referred to as the Network Access Layer

# How TCP/IP Layers Communicate



# Common Port Numbers

Port Number	Description
20	FTP data
21	FTP control
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP), Web
88	Kerberos Network Authentication
110	Post Office Protocol v3 (POP3)
443	Secure HTTP (HTTPS)
464	Kerberos Changes (for example, setting a password)
902	VMware ESXi



# Understanding IP Addressing

- Dotted-decimal
  - 130.57.30.56
- Binary
  - 10000010.00111001.00011110.00111000
- Hexadecimal
  - 82 39 1E 38

# Understanding Network Classes

- Class A Networks
  - Network.Node.Node.Node
- Class B Networks
  - Network.Network.Node.Node
- Class C Networks
  - Network.Network.Network.Node

## Network Address Classes

Class	Mask Bits	Leading Bit Pattern	Decimal Range of First Octet of IP Address	Assignable Networks	Maximum Nodes per Network
A	8	0	1–126	126	16,777,214
B	16	10	128–191	16,384	65,534
C	24	110	192–223	2,097,152	254

# Special Network Addresses

Address	Function
Entire IP address set to all 0s	Depending on the mask, this network (that is, the network or subnet of which you are currently a part) or this host on this network.
A routing table entry of all 0s with a mask of all 0s	Used as the default gateway entry. Any destination address masked by all 0s produces a match for the all 0s reference address. Because the mask has no 1s, this is the least desirable entry, but it will be used when no other match exists.
Network address 127	Reserved for loopback tests. Designates the local node, and it allows that node to send a test packet to itself without generating network traffic.
Node address of all 0s	Used when referencing a network without referring to any specific nodes on that network. Usually used in routing tables.
Node address of all 1s	Broadcast address for all nodes on the specified network, also known as a <i>directed broadcast</i> . For example, 128.2.255.255 means all nodes on the Class B network 128.2. Routing this broadcast is configurable on certain routers.
169.254.0.0 with a mask of 255.255.0.0	The “link-local” block used for autoconfiguration and communication between devices on a single link. Communication cannot occur across routers. Microsoft uses this block for Automatic Private IP Addressing (APIPA).
Entire IP address set to all 1s (same as 255.255.255.255) 10.0.0.0/8 172.16.0.0 to 172.31.255.255	Broadcast to all nodes on the current network; sometimes called a limited broadcast or an all-1s broadcast. <i>This broadcast is not routable.</i>
192.168.0.0/16	The private-use blocks for Classes A, B, and C. As noted in RFC 1918, the addresses in these blocks must never be allowed into the Internet, making them acceptable for simultaneous use behind NAT servers and non-Internet-connected IP networks.

# Class A Networks

- The first byte is the network address, and the three remaining bytes are used for the node addresses. The Class A format is Network.Node.Node.Node.
- There are 126 possible Class A network addresses.
- Each Class A network has 3 bytes (24 bit positions) for the node address of a machine, which means that there are 224, or 16,777,216, unique combinations.

# Class B Networks

- The first 2 bytes are assigned to the network address, and the remaining 2 bytes are used for node addresses. The format is Network.Network.Node.Node.
- The network address is 2 bytes, so there would be 216 unique combinations.
- There are 16,384 (or  $2^{14}$ ) unique Class B networks. For a total of 65,534 possible node addresses for each Class B network.

# Class C Networks

- The first 3 bytes of a Class C network are dedicated to the network portion of the address, with only 1 byte remaining for the node address. The format is Network.Network.Network.Node.
- The first three bit positions are always binary 110. Three bytes, or 24 bits, minus 3 reserved positions leaves 21 positions. There are therefore 2<sup>21</sup> (or 2,097,152) possible Class C networks.
- Each unique Class C network has 1 byte to use for node addresses. This leads to 2<sup>8</sup>, or 256, minus the two special patterns of all 0s and all 1s, for a total of 254 node addresses for each Class C network.

# Subnetting a Network

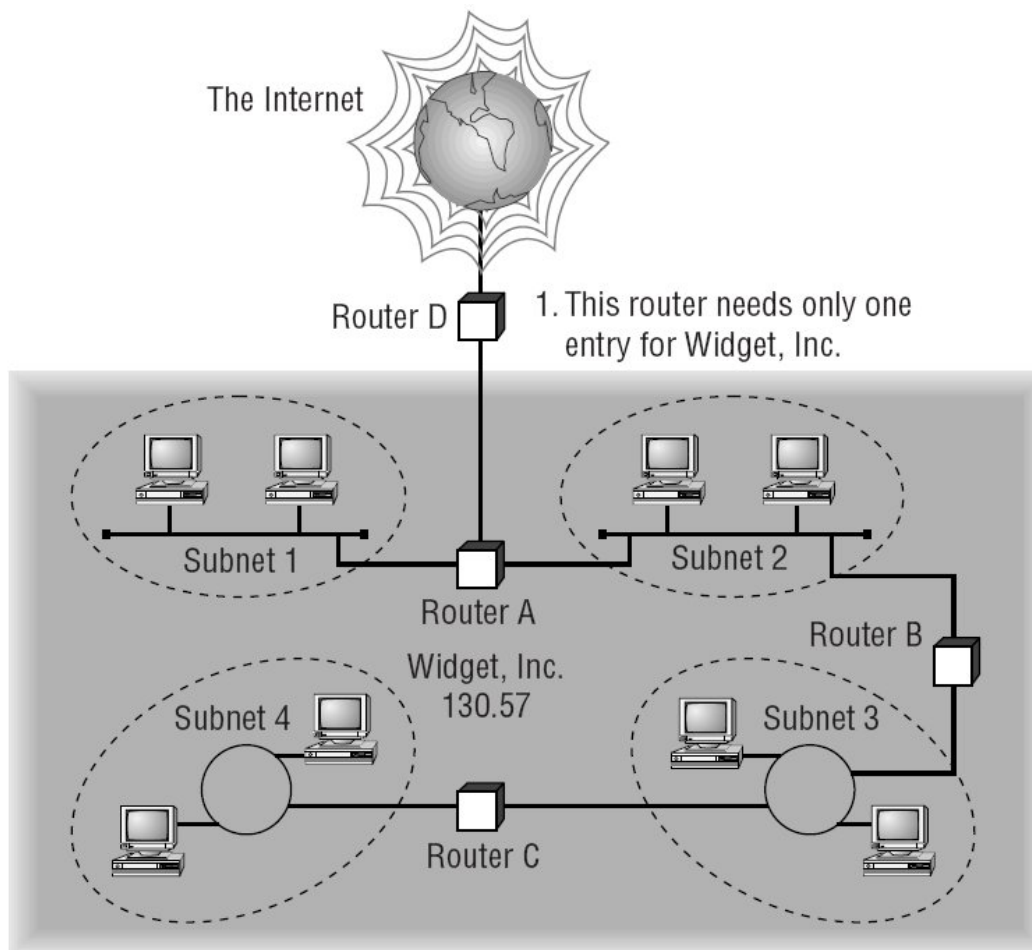
- Reduced network traffic
- Simplified management
- Not enough addresses
- Gigantic routing tables

# Determine Your Subnetting Requirements

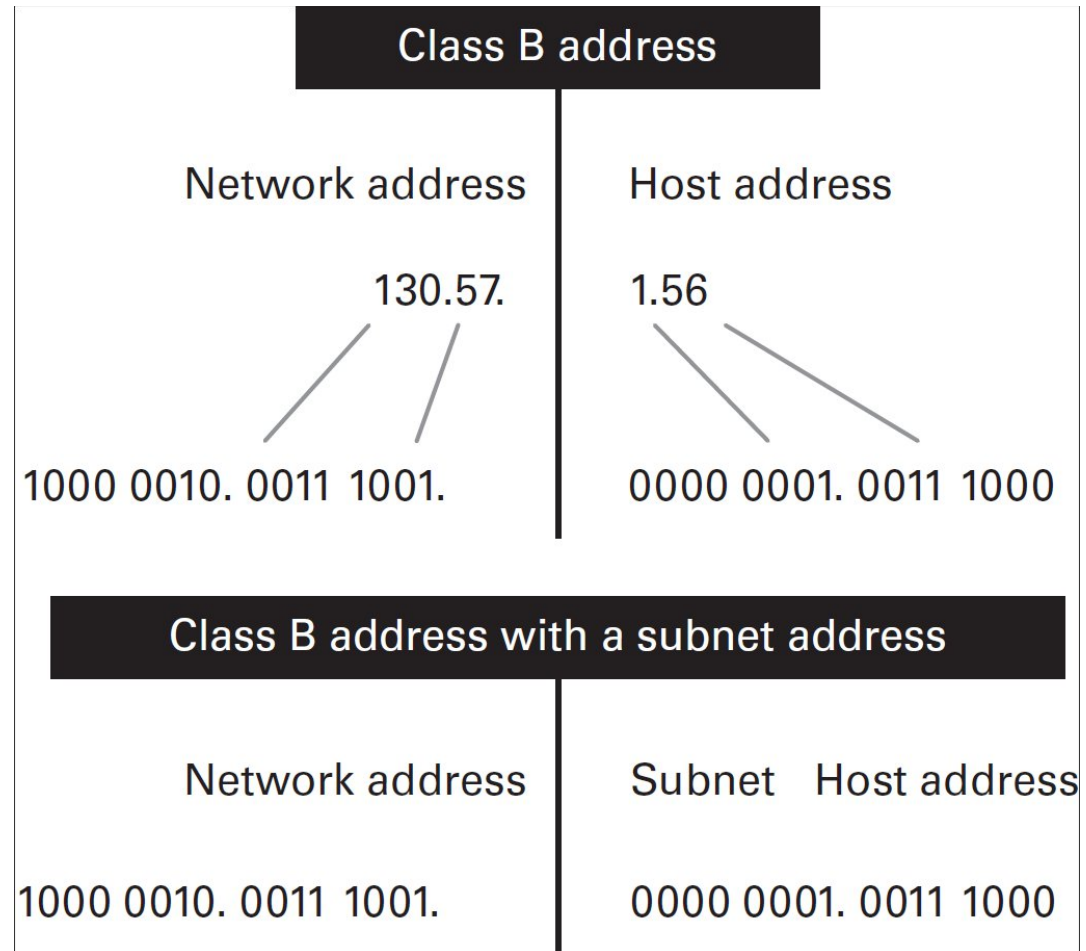
1. Determine the number of required network IDs: one for each subnet and one for each wide area network (WAN) connection.
2. Determine the number of required host IDs per subnet: one for each TCP/IP device, including, for example, computers, network printers, and router interfaces.
3. Based on these two data points, create the following:
  - One subnet mask for your entire network
  - A unique subnet ID for each physical segment
  - A range of host IDs for each unique subnet



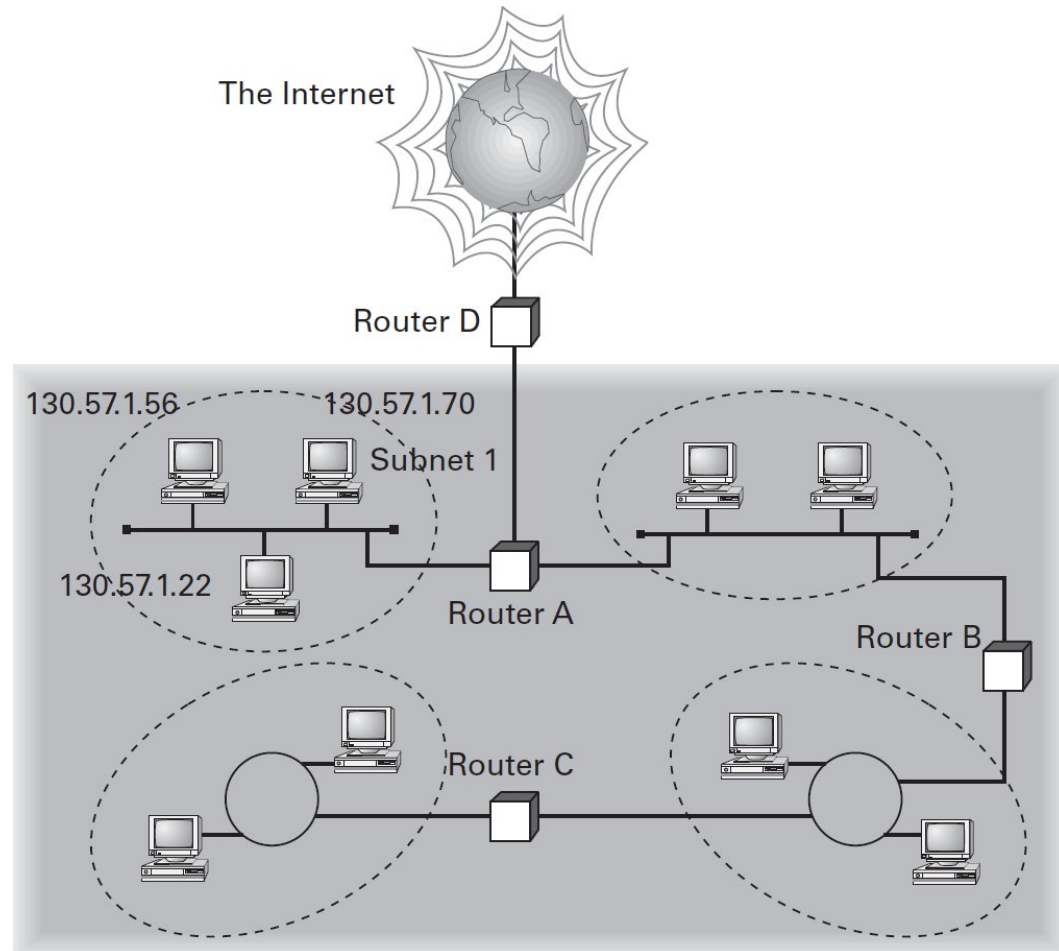
# Implement Subnetting



# Network vs. Host Addresses



# Network Address and Its Subnet



# How to Use Subnet Masks

- Every machine on the network must know which part of the host address will be used as the network address.
- The administrator creates a 32-bit subnet mask comprising 1s and 0s. The 1s in the subnet mask represent the positions in the IP address that refer to the network and subnet addresses. The 0s represent the positions that refer to the host part of the address.

# Subnet Mask

Subnet mask code

---

1s = Positions representing network or subnet addresses

0s = Positions representing the host address

Subnet mask for Widget, Inc.

---

1111 1111. 1111 1111.	1111 1111.	0000 0000
<div style="border: 1px solid black; width: 200px; height: 40px; margin: 5px 0;"></div>	<div style="border: 1px solid black; width: 100px; height: 40px; margin: 5px 0;"></div>	<div style="border: 1px solid black; width: 100px; height: 40px; margin: 5px 0;"></div>
Network address positions	Subnet positions	Host positions

# Different Ways to Represent the Same Mask

- The subnet mask can also be expressed using the decimal equivalents of the binary patterns.

Subnet mask in binary: 1111 1111. 1111 1111. 1111 1111. 0000 0000

Subnet mask in decimal: 255 . 255 . 255 . 0

(The spaces in the above example are only for illustrative purposes.  
The subnet mask in decimal would actually appear as 255.255.255.0.)

# Default Subnet Masks

Class	Format	Default Subnet Mask
A	Network.Node.Node.Node	255.0.0.0
B	Network.Network.Node.Node	255.255.0.0
C	Network.Network.Network.Node	255.255.255.0

# Applying the Subnet Mask

Subnet mask code

---

1s = Positions representing network or subnet addresses

0s = Positions representing the host address

Positions relating to the subnet address

Subnet mask:

1111 1111. 1111 1111. 1111 1111. 0000 0000

IP address of a machine on subnet 1: 1000 0010. 0011 1001. 0000 0001. 0011 1000  
(Decimal: 130.57.1.56)

Bits relating to the subnet address



# Converting the Subnet Mask to Decimal

Binary numbering convention

---

Position/value: ← (continued)	128	64	32	16	8	4	2	1
Widget third byte:	0	0	0	0	0	0	0	1
Decimal equivalent:								$0 + 1 = 1$
Subnet address:								1

# Calculate the Number of Subnets

The formulas for calculating the maximum number of subnets and the maximum number of hosts per subnet are as follows:

- $2^{\times \text{number of masked bits in subnet mask}}$  = maximum number of subnets
- $2^{\times \text{number of unmasked bits in subnet mask}} - 2$  = maximum number of hosts per subnet

# An Easier Way to Apply Subnetting

$2^{(X)} - 2 = Y$	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

**0 = HOSTS    1 = SUBNETS**

**Will Panek Chart**

	X (Power)		X		Y
2 x	3	=	8	-2	6
2 x	4	=	16	-2	14
2 x	5	=	32	-2	30
2 x	6	=	64	-2	62
2 x	7	=	128	-2	126
2 x	8	=	256	-2	254
2 x	9	=	512	-2	510
2 x	10	=	1024	-2	1022
2 x	11	=	2048	-2	2046
2 x	12	=	4096	-2	4094
2 x	13	=	8192	-2	8190
2 x	14	=	16384	-2	16382
2 x	15	=	32768	-2	32766
2 x	16	=	65536	-2	65534
2 x	17	=	131072	-2	131070

# Classless Inter-Domain Routing (CIDR)<sup>(1/2)</sup>

- CIDR is a shorthand version of the subnet mask.
- CIDR represents the number of 1s turned on in a subnet mask.
- For example, a CIDR number of /16 stands for 255.255.0.0 (11111111.11111111.00000000.00000000).

# Classless Inter-Domain Routing (CIDR)<sup>(2/2)</sup>

CIDR	Mask	CIDR	Mask	CIDR	Mask
/8	255.0.0.0	/17	255.255.128.0	/25	255.255.255.128
/9	255.128.0.0	/18	255.255.192.0	/26	255.255.255.192
/10	255.192.0.0	/19	255.255.224.0	/27	255.255.255.224
/11	255.224.0.0	/20	255.255.240.0	/28	255.255.255.240
/12	255.240.0.0	/21	255.255.248.0	/29	255.255.255.248
/13	255.248.0.0	/22	255.255.252.0	/30	255.255.255.252
/14	255.252.0.0	/23	255.255.254.0	/31	255.255.255.254
/15	255.254.0.0	/24	255.255.255.0	/32	255.255.255.255
/16	255.255.0.0				

# Supernetting

- Supernetting allows you to have two or more blocks of contiguous subnetwork addresses.
- Example, a Class C addresses give you 254 usable addresses. So, if you needed 1,000 users, you could set up Supernetting of 4 Class C addresses that are contiguous using a Class B subnet mask.

# IPv6

- Larger address space (128bit vs. 32bit)
- Autoconfiguration of Internet-accessible addresses with or without DHCP (without DHCP it's called stateless autoconfiguration)
- More efficient IP header (fewer fields and no checksum)
- Fixed length IP header (IPv4 header is variable length) with extension headers beyond the standard fixed length to provide enhancements
- Built-in IP mobility and security (although available in IPv4, the IPv6 implementation is much better implementation)
- Built-in transition schemes to allow integration of the IPv4 and IPv6 spaces
- ARP broadcast messages are replaced with multicast request

# IPv6 Address Format

IPv4

ddd ddd ddd ddd

ddd = 8 Bits in Dotted Decimal Notation  
32 Bits Total

IPv6

hhhh hhhh hhhh hhhh hhhh hhhh hhhh hhhh

hhhh = 16 Bits in Hexadecimal Notation  
128 Bits Total



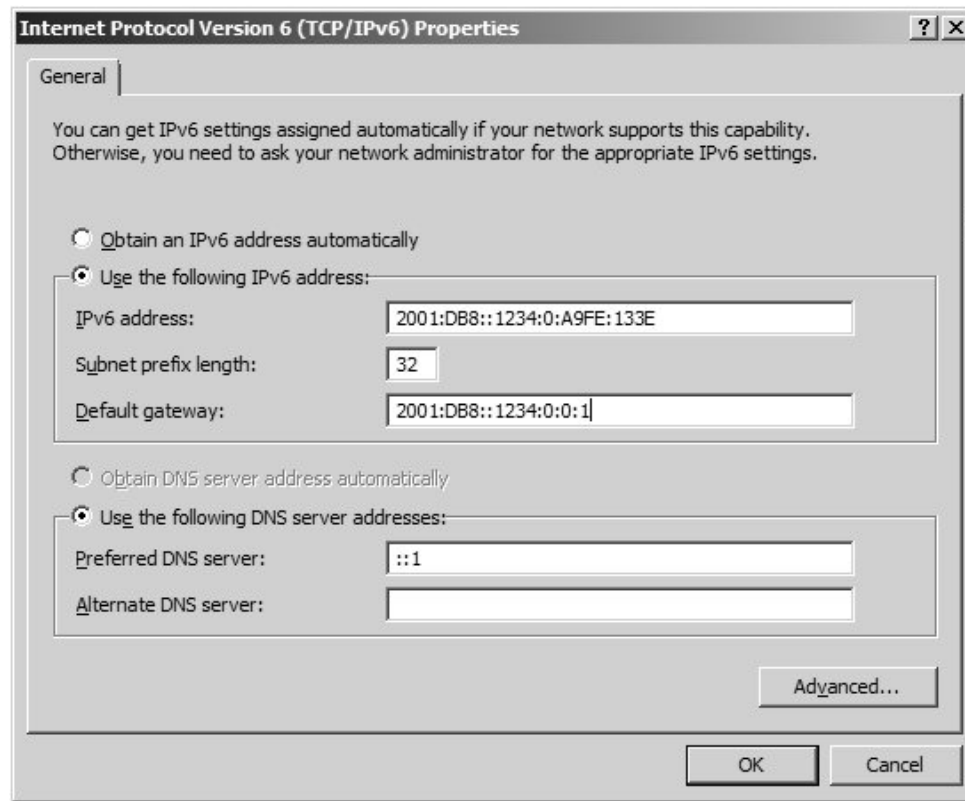
# IPv6 Address Shortcuts

There are several shortcuts for writing an IPv6 address:

- :0: stands for :0000:.
- Can omit preceding 0s in any 16-bit word. For example, :DB8: and :0DB8: are equivalent.
- :: is a variable standing for enough zeroes to round out the address to 128 bits. :: can be used only once in an address.

# IPv6 Address Assignment

## TCP/IPv6 Properties Window



**Internet Protocol Version 6 (TCP/IPv6) Properties**

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:DB8::1234:0:A9FE:133E

Subnet prefix length: 32

Default gateway: 2001:DB8::1234:0:0:1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: ::1

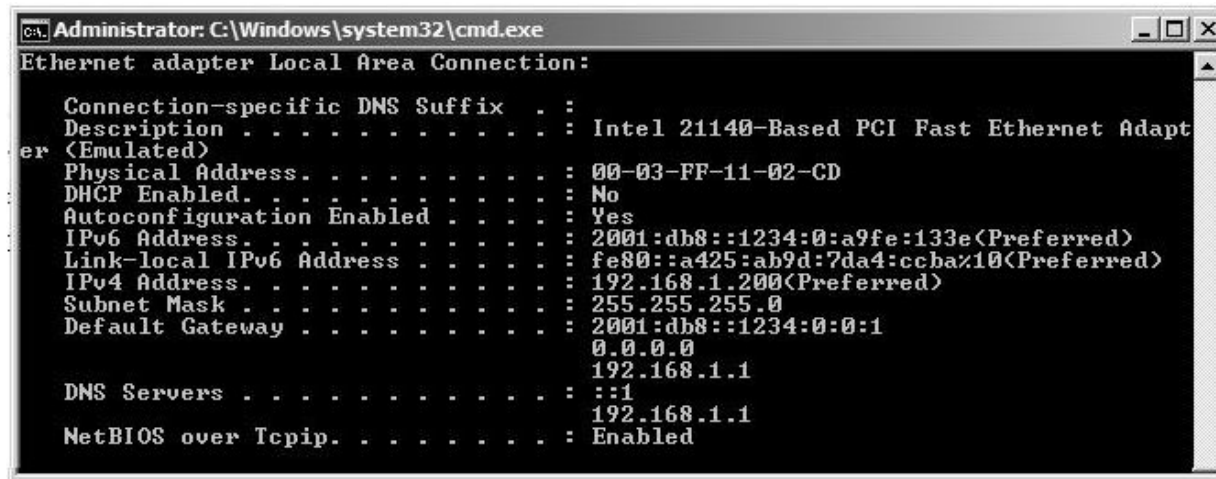
Alternate DNS server:

Advanced...

OK Cancel

# IPv6 Configuration From the Command Prompt

- To see your configured IP addresses (IPv4 and IPv6), you can still use the **ipconfig** command.



```
C:\Administrator: C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel 21140-Based PCI Fast Ethernet Adapt
er (Emulated)
    Physical Address. . . . . : 00-03-FF-11-02-CD
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2001:db8::1234:0:a9fe:133e(Preferred)
    Link-local IPv6 Address . . . . . : fe80::a425:ab9d:7da4:ccbaz10(Preferred)
    IPv4 Address. . . . . : 192.168.1.200(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 2001:db8::1234:0:0:1
                                0.0.0.0
                                192.168.1.1
    DNS Servers . . . . . : ::1
                                192.168.1.1
    NetBIOS over Tcpip. . . . . : Enabled
```

# IPv6 Address Types

- Anycase Addresses
- Unicast Addresses
  - Global unicast address
  - Link-local address
  - AnonymousAddress
  - Unique local address
- Multicast address

# IPv6 Known Prefixes and Addresses

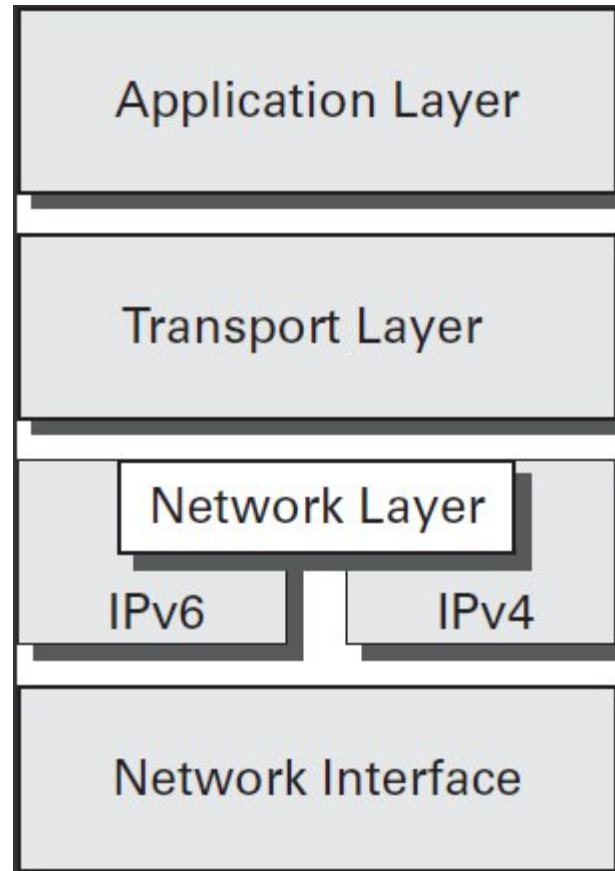
Address Prefix	Scope of Use
2000:: /3	Global unicast space prefix
FE80:: /10	Link-local address prefix
FC00:: /7	Unique local unicast prefix
FD00:: /8	Unique local unicast prefix
FF00:: /8	Multicast prefix
2001:DB8:: /32	Global unicast prefix used for documentation
::1	Reserved local loopback address
2001:0000: /32	Teredo prefix (discussed later in this chapter)
2002:: /16	6to4 prefix

# IPv6 Integration/Migration

The process of integration/migration consists of several mechanisms:

- Dual Stack
- Tunneling
- Address Translation

# IPv6 Dual Stack



# IPv6 Tunneling

Windows Server 2022 includes several tunneling mechanisms for tunneling IPv6 through the IPv4 address space. They include:

- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), used for unicast IPv6 communication across an IPv4 infrastructure. Enabled by default in Windows Server 2022.
- 6to4, used for unicast IPv6 communication across an IPv4 infrastructure.
- Teredo, used for unicast IPv6 communication with an IPv4 NAT implementation across an IPv4 infrastructure.



# Useful IPv6 Information Commands

Can use numerous commands to view, verify, and configure the network parameters of Windows Server 2022:

- netsh
- route print
- ping
- tracert