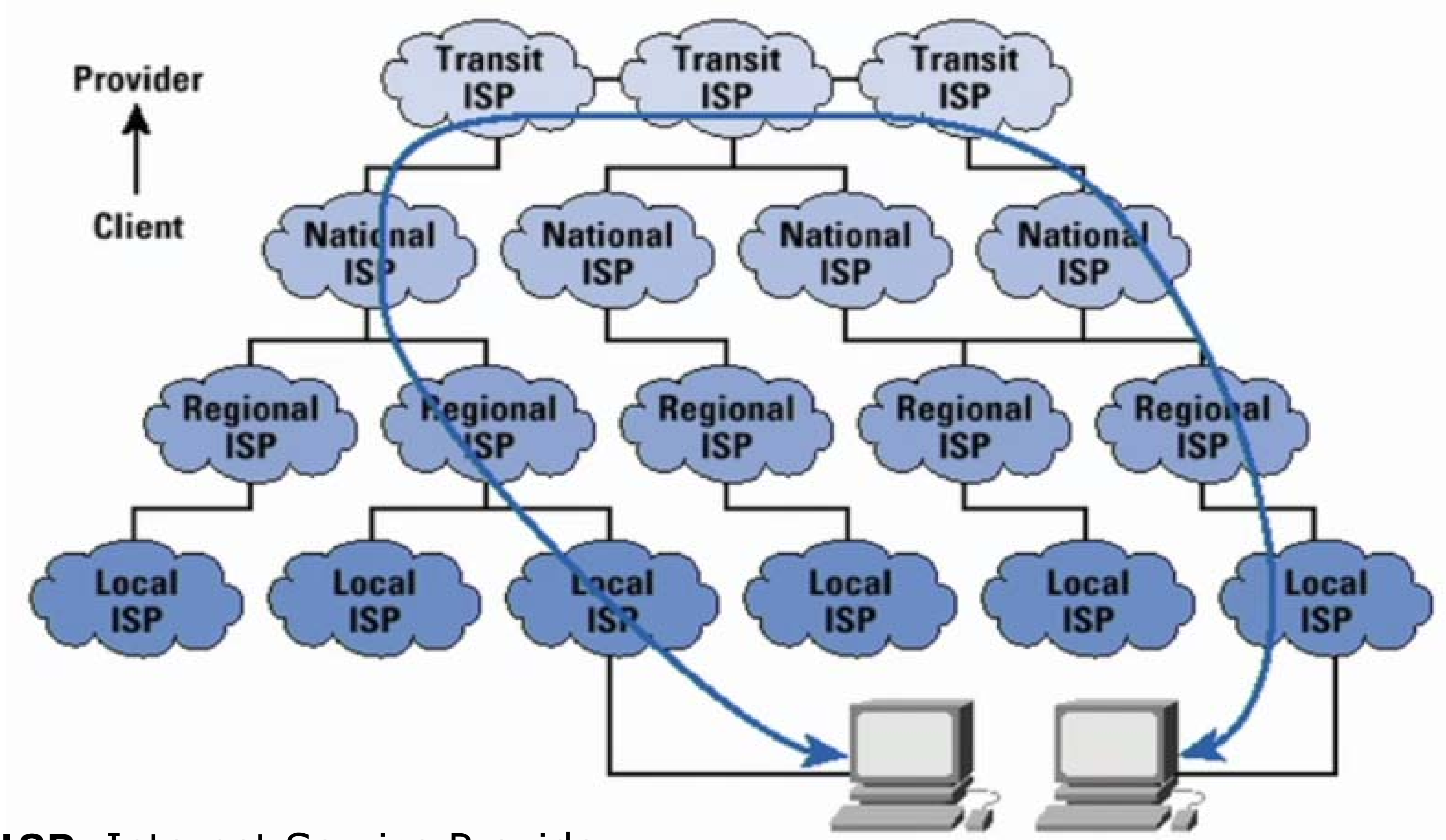
CS 302 Data Communication and Networks

Lecture 29-30: IP Addressing (IPv4)

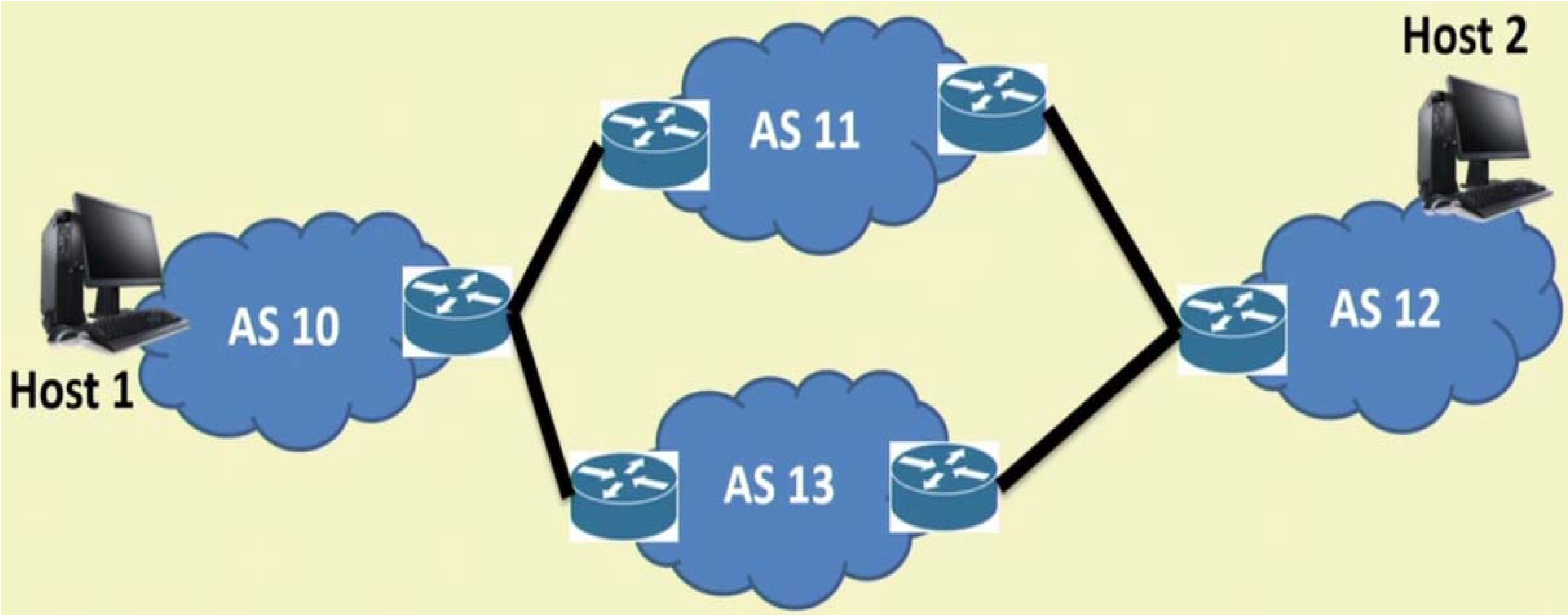
Communication between Two Nodes over ISPs



ISP: Internet Service Provider

IP Addressing: Basic Principles

- We need to forward data packets from one network to another network via different intermediate networks
- Therefore, we require an address that identifies a network as well as a host inside the network



AS: Autonomous System

What is an IP Address?

- An IP address is a unique global address for a network interface
- An IP address uniquely and universally defines the connection of a host or a router to the Internet
- IP addresses are unique in the sense that each address defines one, and only one, connection to the Internet
  - If a device has two connections to the Internet, via two networks, it has two IP addresses
- An IPv4 address:
  - is a **32 bit long** identifier
  - encodes a **network number** (network prefix) and a **host number**

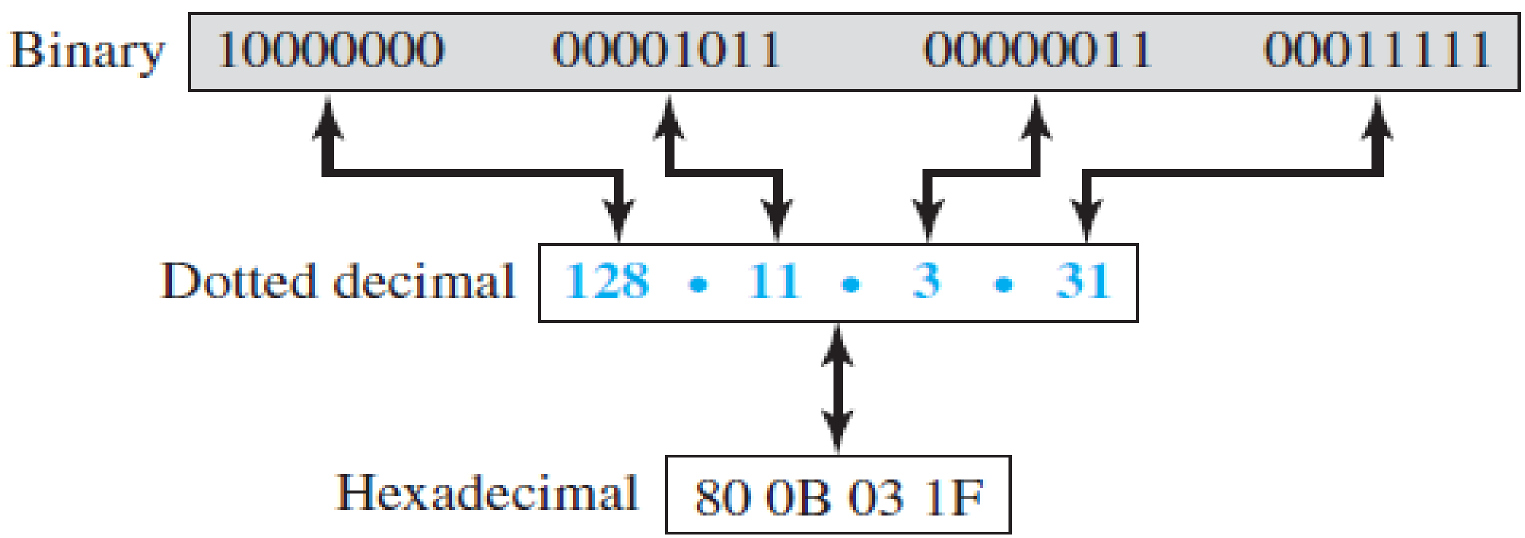
IPv4 Addresses

- **Address Space:**
  - A protocol like IPv4 that defines addresses has an address space
  - An **address space** is the total number of addresses used by the protocol
  - If a protocol uses ***b*** bits to define an address, the address space is $\boldsymbol{2^b}$ because each bit can have two different values (0 or 1)
  - IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion)
- There are three common notations to show an IPv4 address:
  - Binary notation
  - Dotted-decimal notation
  - Hexadecimal notation

Notations in IPv4 addressing

- Binary and dotted-decimal notations are popular and commonly used
- Hexadecimal notation is not very common. It is often used in network programming

Three different notations in IPv4 addressing



Network prefix and Host number

- The network prefix identifies a network and the host number identifies a specific host (actually, an interface on the network)

network prefix	host number

- When Internet addresses were standardized (early 1980s), the Internet address space was divided into classes. For example:
  - **Class A:** Network prefix is 8 bits long
  - **Class B:** Network prefix is 16 bits long
  - **Class C:** Network prefix is 24 bits long

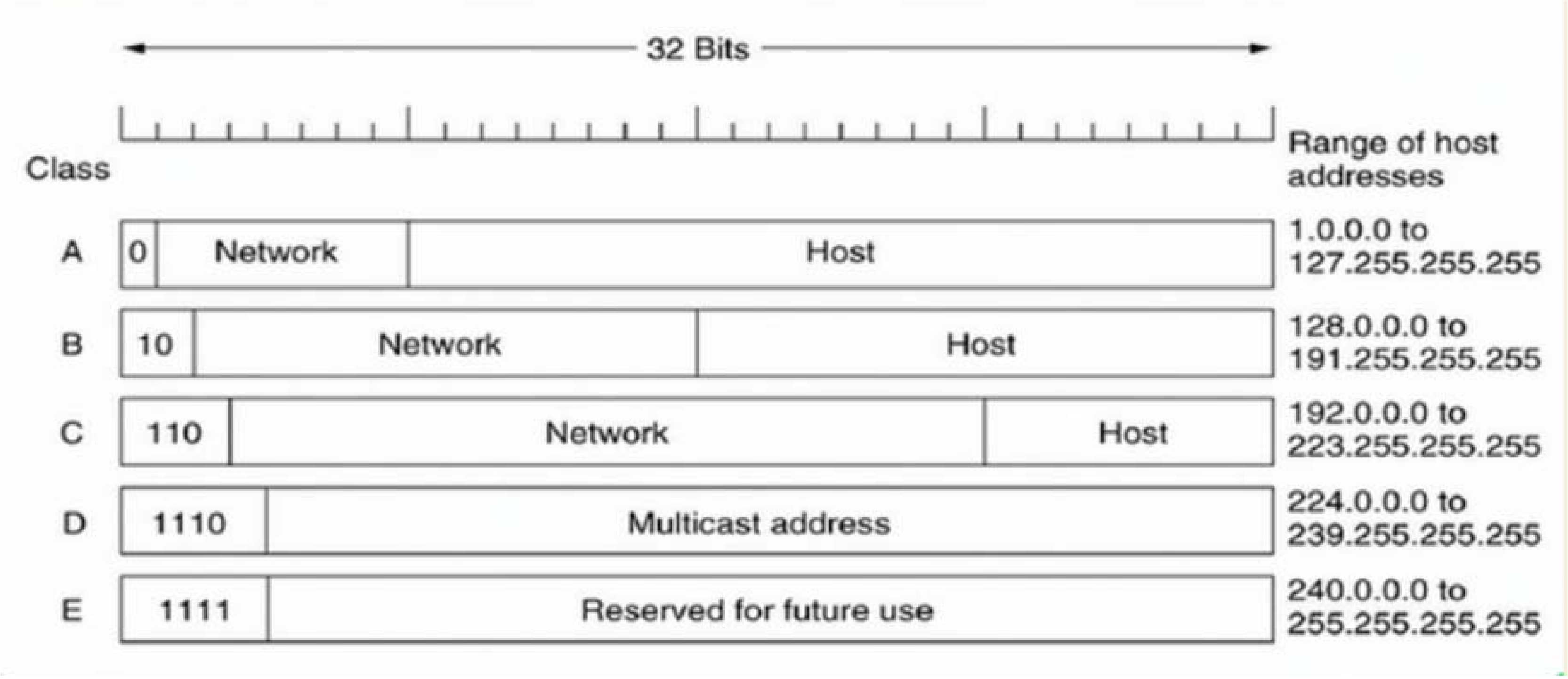
IP Addressing: IPv4

- Divide the address space (32 bit in IPv4) among network address and host address
- **The old age – Classful addressing:** Fixed number of bits for network address and host address

IP Addressing: IPv4

- When the Internet started, an IPv4 address was designed with a fixed-length prefix
  - To accommodate both small and large networks, three fixed-length prefixes were designed (n = 8, n = 16, and n = 24)
- The whole address space was divided into five classes (class A, B, C, D, and E)
- This scheme is referred to as **classful addressing** (shown in the next slide)

Classful Addressing



- How to identify a class? – Use the first few bits
  - 0 – Class A; 10 – Class B; 110 – Class C; 1110 – Class D; 1111 – Class E

IP Addresses

- **Class A:**
  - Starts with binary 0
  - In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can use only seven bits as the network identifier
  - Therefore, only $2^7 = 128$ (0 to 127) networks are possible in class A
    - All 0 reserved (will be discussed later)
    - 01111111 (127) is also reserved for loopback (will be discussed later)
    - Hence, range: 1.x.x.x to 126.x.x.x

IP Addresses

- **Class B:**
  - Starts with binary 10
  - In class B, the network length is 16 bits, but since the first two bits, which are (10), define the class, we can use only 14 bits as the network identifier
  - Therefore, only 2^{14} = 16,384 networks are possible in class B
  - Range: 128.x.x.x to 191.x.x.x
- **Class C:**
  - Starts with binary 110
  - The network length is 24 bits
  - Since first three bits define the class, we can use only 21 bits as the network identifier
  - There are 2^{21} = 2,097,152 networks possible in class C
  - Range: 192.x.x.x to 223.x.x.x

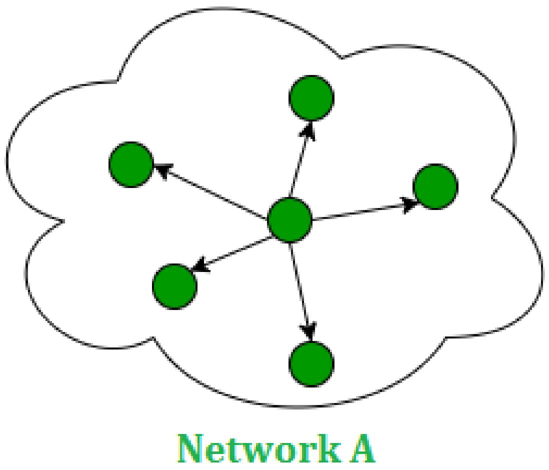
IP Addresses

- **Class D:**
  - Starts with binary 1110
  - Class D is not divided into prefix and suffix
  - It is used for multicast addresses
- **Class E:**
  - Starts with binary 1111
  - As in Class D, Class E is not divided into prefix and suffix
  - Reserved for future use

Broadcast

- Broadcast can be classified into two types:
  - Limited Broadcast
  - Directed Broadcast
- **Limited Broadcast:**
  - It is used when we have to send stream of packets to all the devices over the network that we reside
  - For this to achieve, we append 255.255.255.255 (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header

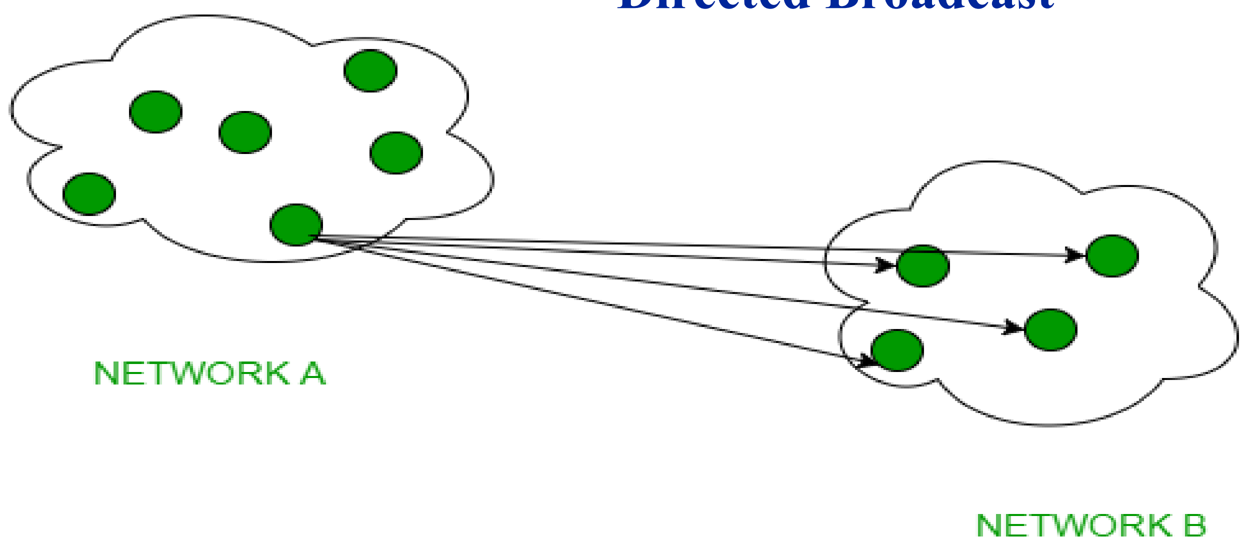
Limited Broadcast



Broadcast

- **Directed Broadcast:**
  - This is useful when a device in one network wants to transfer packets to all the devices over the other network
  - This is achieved by translating all the host ID part bits of the destination address to 1, referred as **Directed Broadcast Address** in the datagram header
  - For example, see next slide

Directed Broadcast



Network Address and Broadcast Address

- **Network address:** Identify a network
  - All 0's in the host address part
  - **Ex-1 (Class A):** 01111110.00000000.00000000.00000000 (126.0.0.0)
  - **Ex-2 (Class B):** 10111101.11101001.00000000.00000000 (189.233.0.0)
- **Directed broadcast address:** Send the data to **all the hosts** of a network
  - All 1's in the host address part
  - **Ex-1 (Class A):** 01111110.11111111.11111111.11111111 (126.255.255.255)
  - **Ex-2 (Class B):** 10111101.11101001.11111111.11111111 (189.233.255.255)
- How many valid hosts can be there in a Class A, in a Class B and in a Class C IP address?

Classful Addressing

- Maximum possible hosts in a Class A IP address:
  - 24 bits in the host address
  - Hence, total possible hosts = $2^{24} – 2$
  - Here, it is important to note that we have total 2^{24} IP addresses available but we can configure only $2^{24} – 2$ hosts
  - Two addresses cannot be assigned to any host because we require one address for network address (all zeros in the host id part) and one for directed broadcast address (all 1's in the host id part)
- Maximum possible hosts in a Class B IP address:
  - 16 bits in the host address
  - Hence, total possible hosts = $2^{16} – 2$ (minus 2 is due to the same reason as in class A)
- Maximum possible hosts in a Class C IP address:
  - 8 bits in the host address
  - Hence, total possible hosts = $2^{8} – 2$ (minus 2 is due to the same reason as in class A and class B)

Subnetting, Supernetting, and Classless Inter-domain Routing (CIDR)

- Suppose, you have to configure a network with 255 hosts. Which IPv4 address class will you use – Class C or Class B?
  - Class C – Not possible
  - Class B – Huge address space is unutilized (using only 255 addresses out of possible $2^{16} - 2$ addresses)

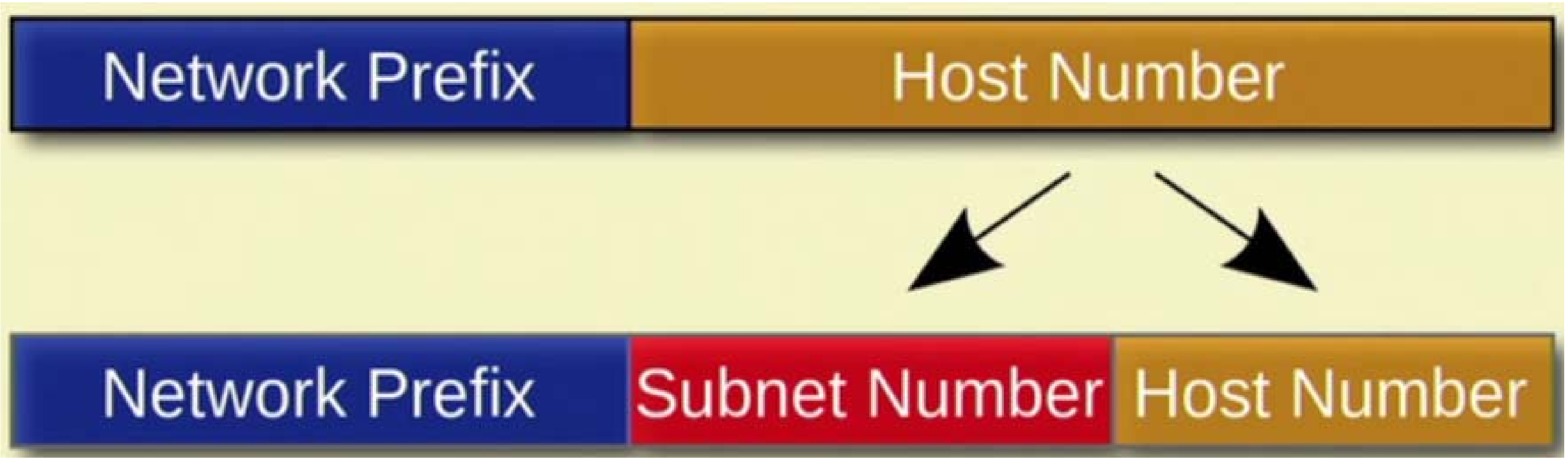
Subnetting, Supernetting, and CIDR

- Split a large network or combine multiple small networks for efficient use of address space
  - **Subnetting:** Divide a large network into multiple small networks
  - **Supernetting:** Combine multiple small networks into a single large network
- **Subnet mask:** Denote the number of bits in the network address part

Subnetting, Supernetting, and CIDR

- **Subnet mask: (Contd…)**
  - An IP address is divided into two parts: network and host parts
  - For example, an IP class A address consists of 8 bits identifying the network and 24 bits identifying the host
  - Like an IP address, a subnet mask also consists of 32 bits. We use it to determine the network part and the host part of an address
  - The 1s in the subnet mask represent a network part, and the 0s represent a host part
  - A subnet mask must always be a series of 1s followed by a series of 0s
  - For example, the default subnet mask for a class A IP address in dotted decimal notation is 255.0.0.0

Divide a Network into Subnets

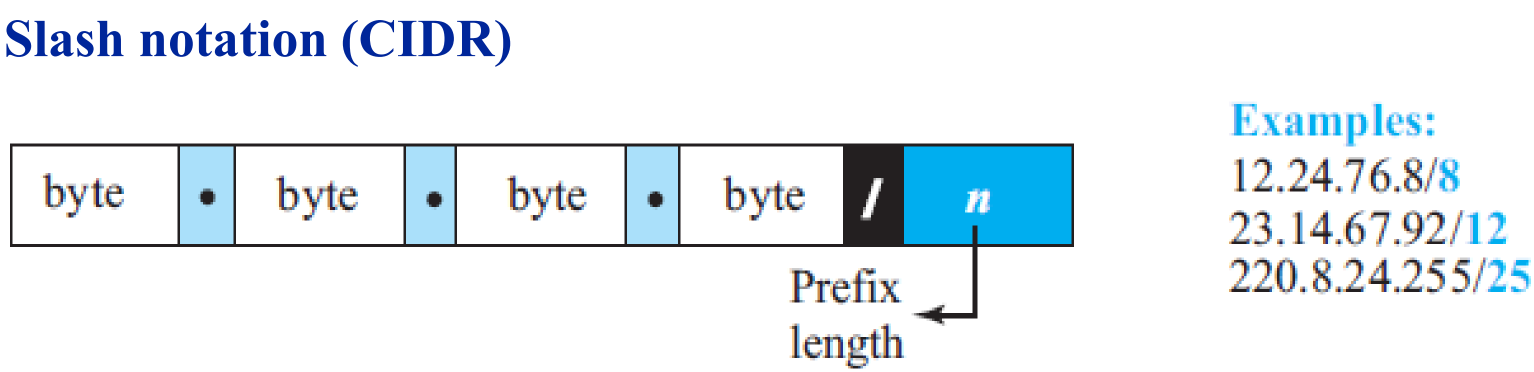


Classless Addressing

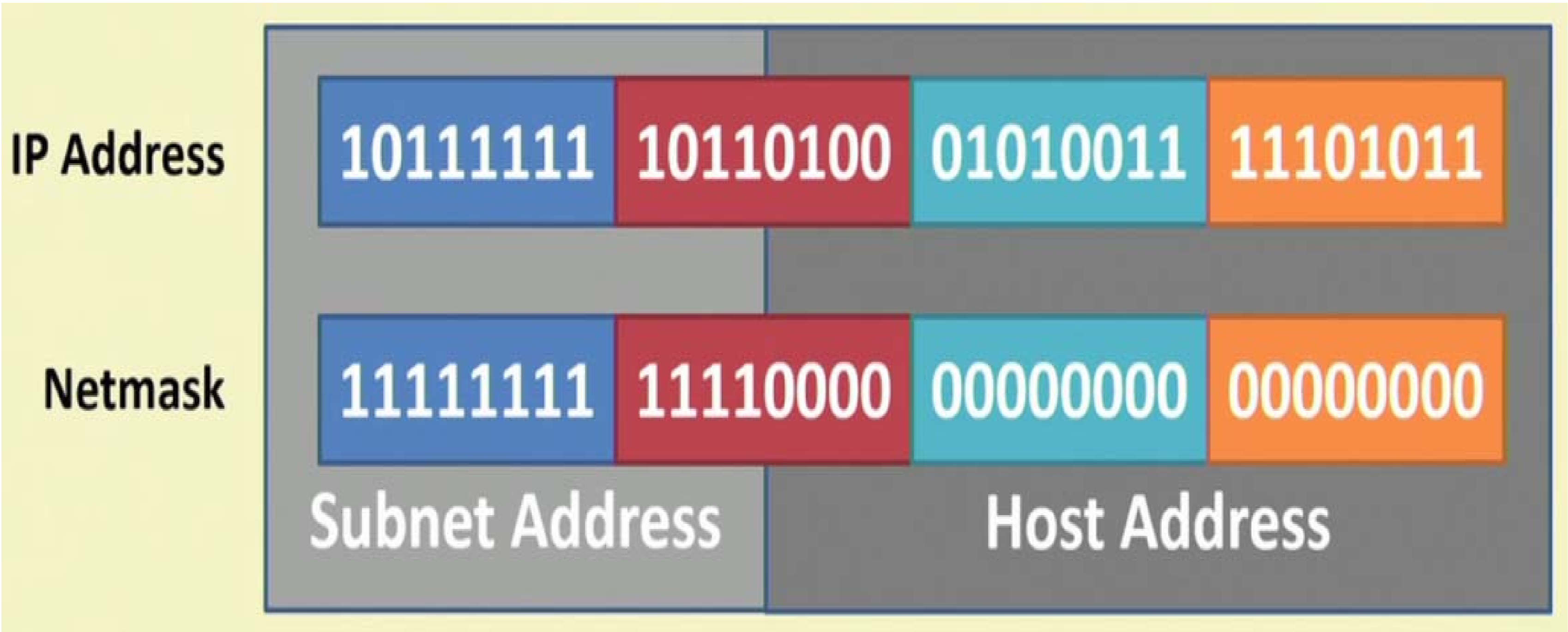
- In classless addressing, the class privilege was removed
- In classless addressing, variable-length blocks are used that belong to no classes
  - We can have a block of 1 address, 2 addresses, 4 addresses,128 addresses, and so on
- In classless addressing, the whole address space is divided into variable length blocks
- The prefix in an address defines the block (network); the suffix defines the node (device)
- One of the restrictions is that the number of addresses in a block needs to be a power of 2
- Unlike classful addressing, the prefix length in classless addressing is variable
  - We can have a prefix length that ranges from 0 to 32

Classless Addressing

- **Prefix Length: Slash Notation:**
  - The first question that we need to answer in classless addressing is how to find the prefix length if an address is given
  - In classless addressing, the prefix length is added to the address, separated by a slash
  - The notation is informally referred to as slash notation and formally as classless interdomain routing (CIDR)



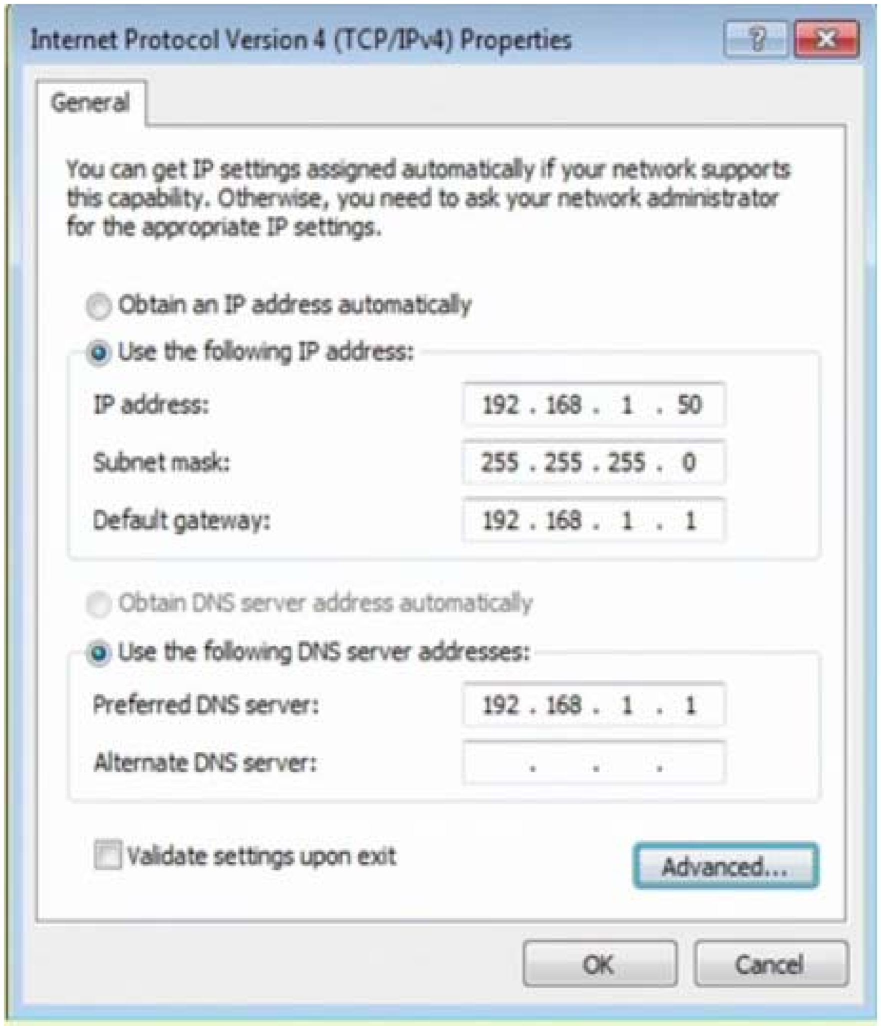
CIDR: Addressing Format

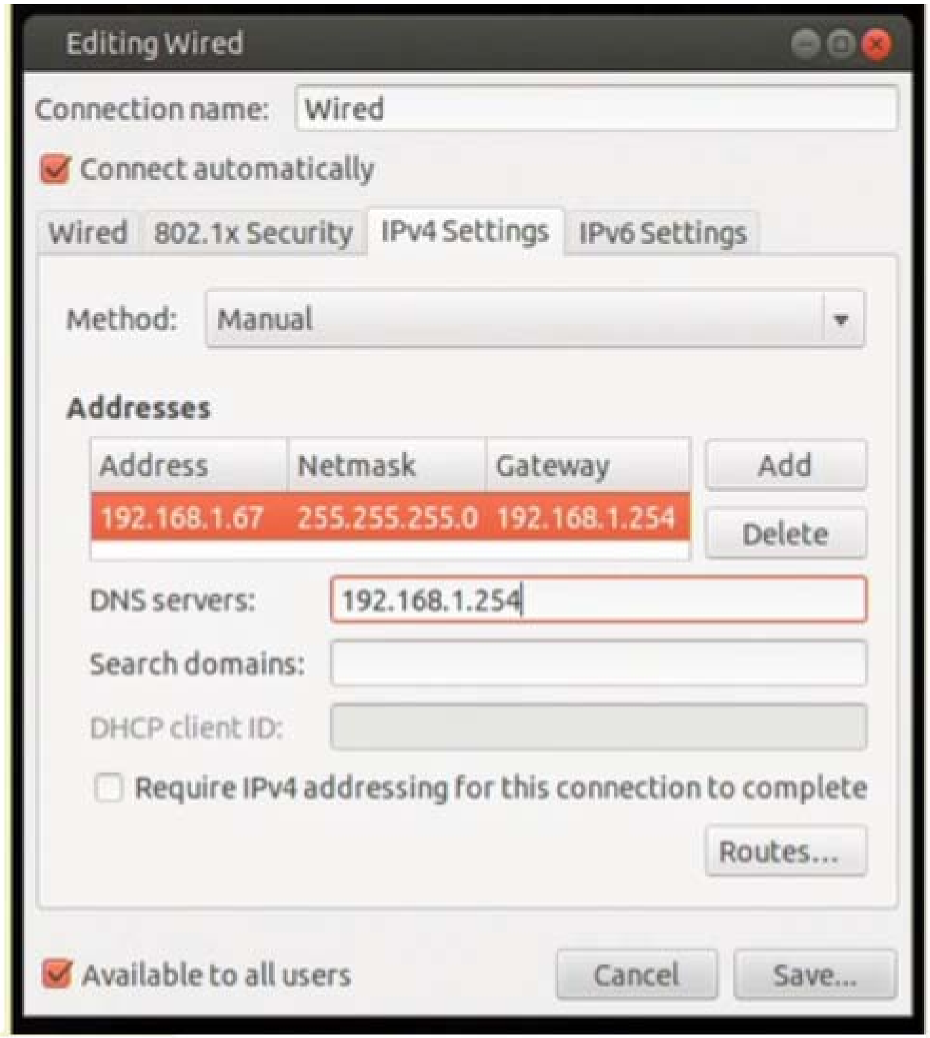


CIDR: Addressing Format

- We write the IP address as 192.180.83.235/12 in CIDR notation
  - The first 12 bits are the network address and rest (32 - 12) = 20 bits are for host address
  - The subnet mask is 255.240.0.0

CIDR: Manual IP Setting in the OS



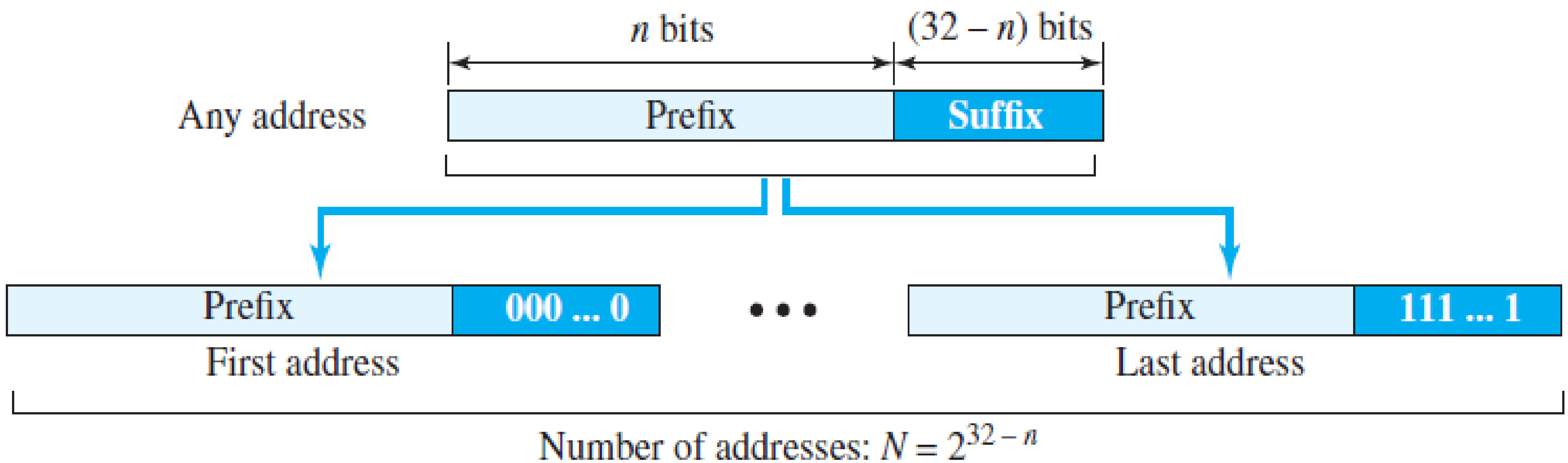


Extracting Information from an Address

- Given any address in the block, we normally like to know three pieces of information about the block to which the address belongs:
  - The number of addresses, the first address in the block, and the last address
- We can easily find these three pieces of information as (also shown in Figure in the next slide):
  1. The number of addresses in the block is found as $N = 2^{32 - n}$ where n is the prefix length
  2. To find the first address, we keep the n leftmost bits and set the (32 – n) rightmost bits all to 0s
  3. To find the last address, we keep the n leftmost bits and set the (32 – n) rightmost bits all to 1s

Extracting Information from an Address

Information extraction in classless addressing



Extracting Information from an Address

- **Example:** A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows:
  - The number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses
  - The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s as:

Address: 167.199.170.82/27 10100111 11000111 10101010 01010010

First address: 167.199.170.64/27 10100111 11000111 10101010 01000000

  - The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s as:

Address: 167.199.170.82/27 10100111 11000111 10101010 01010010

Last address: 167.199.170.95/27 10100111 11000111 10101010 01011111

CIDR: Block Allocation

- One issue in classless addressing is block allocation
- The ultimate responsibility of block allocation is given to a global authority called the Internet Corporation for Assigned Names and Numbers (ICANN)
- However, ICANN does not normally allocate addresses to individual Internet users
- It assigns a large block of addresses to an ISP (or a larger organization), which further allocate addresses to individual Internet users

CIDR: Block Allocation

- For the proper operation of the CIDR, two restrictions need to be applied to the allocated block
  1. The number of requested addresses, N, needs to be a power of 2. The reason is that $N = 2^{32-n}$ or $n = 32 - \log_2 N$. If N is not a power of 2, we cannot have an integer value for n (prefix length)
  2. The requested block needs to be allocated where there is an adequate number of contiguous addresses available in the address space
- **Example:** An ISP has requested a block of 1000 addresses. Since 1000 is not a power of 2, 1024 addresses are granted. The prefix length is calculated as $n = 32 - \log_2 1024 = 22$
  - An available block, 18.14.12.0/22, is granted to the ISP

CIDR: Subnetting

- More levels of hierarchy can be created using subnetting
- An organization (or an ISP) that is granted a range of addresses may divide the range into several subranges and assign each subrange to a subnetwork (or subnet)
- Nothing stops the organization from creating more levels
  - A subnetwork can be divided into several sub-subnetworks
  - A sub-subnetwork can be divided into several sub-sub-subnetworks, and so on

CIDR: Designing Subnets

- The subnetworks in a network should be carefully designed to enable the routing of packets
- Suppose, the total number of addresses granted to the organization is N, the prefix length is n, the assigned number of addresses to each subnetwork is N_{sub}, and the prefix length for each subnetwork is n_{sub}
- Then the following steps need to be carefully followed to guarantee the proper operation of the subnetworks:
  - All IP addresses corresponding to a subnet should be contiguous
  - The number of addresses in each subnetwork should be a power of 2
  - The prefix length for each subnetwork should be found using the following formula:

$$n_{sub} = 32 - \log_2 N_{sub}$$

  - The starting address in each subnetwork should be divisible by the number of addresses in that subnetwork. This can be achieved if we first assign addresses to larger subnetworks

CIDR: Finding Information about Each Subnetwork

- It can be found by using the process we described to find the information about each network in the Internet
- **Example:** An organization is granted a block of addresses with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks
- **Solution:** There are $2^{32-24} = 256$ addresses in this block. The first address is 14.24.74.0/24; the last address is 14.24.74.255/24. To satisfy the last requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one
  a. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. Hence, we allocate 128 addresses. The subnet mask (prefix length) for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$. The first address in this block is 14.24.74.0/25; the last address is 14.24.74.127/25

CIDR: Finding Information about Each Subnetwork

- **Solution: (Contd….)**

  b. The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. Hence, we allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$. The first address in this block is 14.24.74.128/26; the last address is 14.24.74.191/26

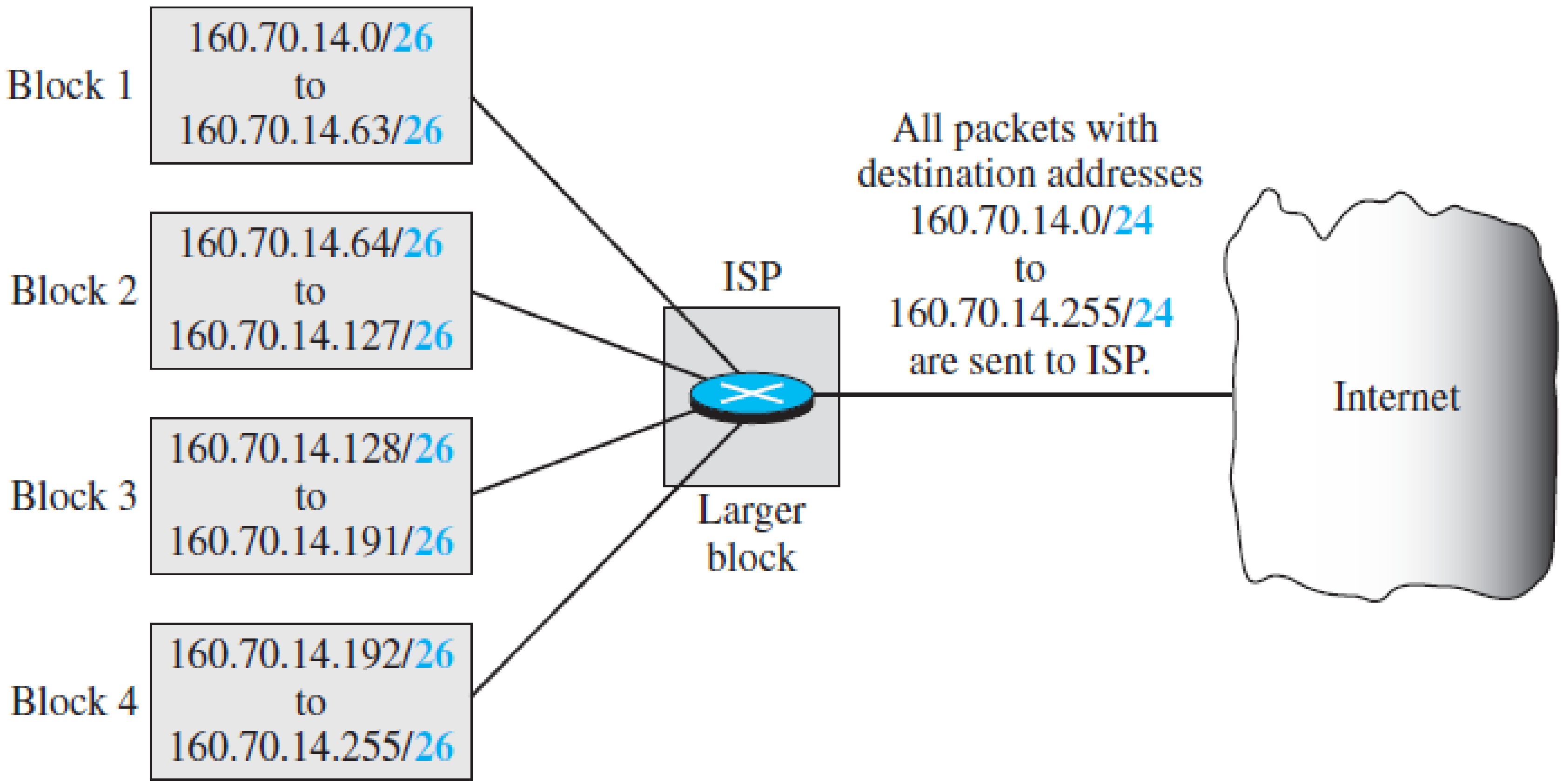
  c. The number of addresses in the smallest subblock, which requires 10 addresses, is not a power of 2 either. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_3 = 32 - \log_2 16 = 28$. The first address in this block is 14.24.74.192/28; the last address is 14.24.74.207/28

CIDR: Address Aggregation

- One of the advantages of the CIDR strategy is address aggregation (sometimes called address summarization or route summarization)
- When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block
- ICANN assigns a large block of addresses to an ISP. Each ISP in turn divides its assigned block into smaller subblocks and grants the subblocks to its customers
- **Example:** Figure in the next slide shows how four small blocks of addresses are assigned to four organizations by an ISP. The ISP combines these four blocks into one single block and advertises the larger block to the rest of the world. Any packet destined for this larger block should be sent to this ISP. It is the responsibility of the ISP to forward the packet to the appropriate organization. This is similar to routing we can find in a postal network. All packages coming from outside a country are sent first to the capital and then distributed to the corresponding destination

CIDR: Address Aggregation

Example of address aggregation



Special Addresses

- **This-host Address:**
  - The only address in the block 0.0.0.0/32 is called the this-host address
  - It is used whenever a host needs to send an IP datagram but it does not know its own address. Such host uses it as the source address
- **Limited-broadcast Address:**
  - The only address in the block 255.255.255.255/32 is called the limited-broadcast address
  - It is used whenever a router or a host needs to send a datagram to all devices in its own network
  - The routers in the network, however, block the packet having this address as the destination; the packet cannot travel outside the network

Special Addresses

- **Loopback Address:**
  - The block 127.0.0.0/8 is called the loopback address
  - A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host
  - Any address in the block is used to test a piece of software in the machine
  - For example, we can write a client and a server program in which one of the addresses in the block is used as the server address. We can test the programs using the same host to see if they work before running them on different computers

Special Addresses

- **Private Addresses:**
  - Four blocks are assigned as private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 169.254.0.0/16
  - We use any one of these address blocks when we use NAT (Network Address Translation) method for setting up an organization network

End