Network Layer Protocols and IP Addressing

Foreword

- Internet Protocol Version 4 (IPv4) is the core protocol suite in the TCP/IP protocol suite. It works at the network layer in the TCP/IP protocol stack and this layer corresponds to the network layer in the Open System Interconnection Reference Model (OSI RM).
- The network layer provides connectionless data transmission services. A network does not need to establish a connection before sending data packets. Each IP data packet is sent separately.
- This presentation describes the basic concepts of IPv4 addresses, subnetting, network IP address planning, and basic IP address configuration.

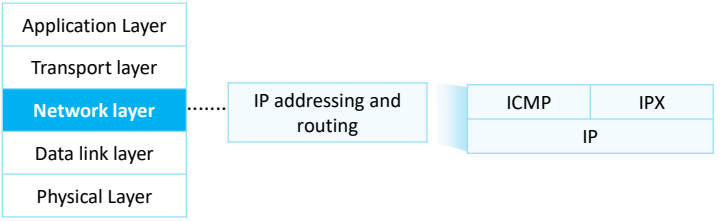
Objectives

- On completion of this course, you will be able:
  - Describe main protocols at the network layer.
  - Describe the concepts and classification of IPv4 addresses and special IPv4 addresses.
  - Calculate IP networks and subnets.
  - Use the IP network address planning method.

Contents

Network Layer Protocols

- The network layer is often called the IP layer. Network layer protocols include Internet Control Message Protocol (ICMP) and Internet Packet Exchange (IPX), in addition to IP.



Equivalent TCP/IP model

-

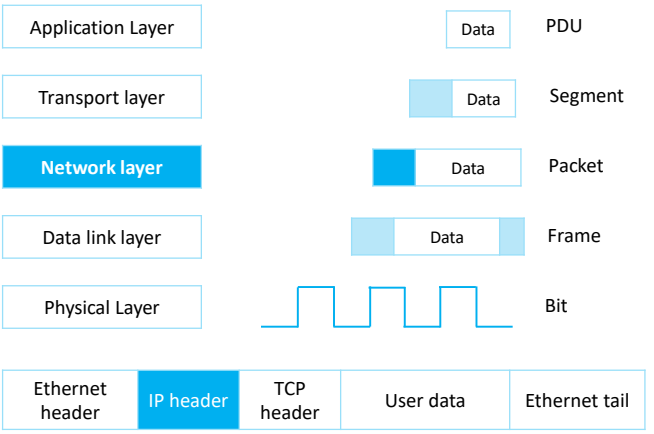
Internet Protocol

- IP is short for the Internet Protocol. IP is the name of a protocol file with small content. It defines and describes the format of IP packets.
- The frequently mentioned IP refers to any content related directly or indirectly to the Internet Protocol, instead of the Internet Protocol itself.

Function	Version
• Provides logical addresses for devices at the network layer. • Is responsible for addressing and forwarding data packets.	• IP Version 4 (IPv4) • IP Version 6 (IPv6)

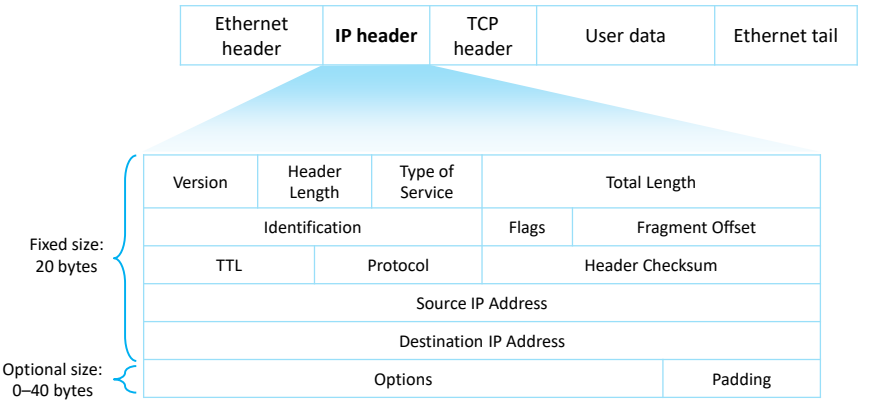
- IP has two versions: IPv4 and IPv6. IPv4 packets prevail on the Internet, and the Internet is undergoing the transition to IPv6. Unless otherwise specified, IP addresses mentioned in this presentation refer to IPv4 addresses.
  - IPv4 is the core protocol in the TCP/IP protocol suite. It works at the network layer in the TCP/IP protocol stack and this layer corresponds to the network layer in the Open System Interconnection Reference Model (OSI RM).
  - IPv6, also called IP Next Generation (IPng), is the second-generation standard protocol of network layer protocols. Designed by the Internet Engineering Task Force (IETF), IPv6 is an upgraded version of IPv4.

Data Encapsulation



- Application data can be transmitted to the destination end over the network only after being processed at each layer of the TCP/IP protocol suite. Each layer uses protocol data units (PDUs) to exchange information with another layer. PDUs at different layers contain different information. Therefore, PDUs at each layer have a particular name.
  - For example, after a TCP header is added to the upper-layer data in a PDU at the transport layer, the PDU is called a segment. The data segment is transmitted to the network layer. After an IP header is added to the PDU at the network layer, the PDU is called a packet. The data packet is transmitted to the data link layer. After the data link layer header and tailer are encapsulated into the PDU, the PDU becomes a frame. Ultimately, the frame is converted into bits and transmitted through network media.
  - The process in which data is delivered following the protocol suite from top to bottom and is added with headers and tails is called encapsulation.
- This presentation describes how to encapsulate data at the network layer. If data is encapsulated with IP, the packets are called IP packets.

IPv4 Packet Format

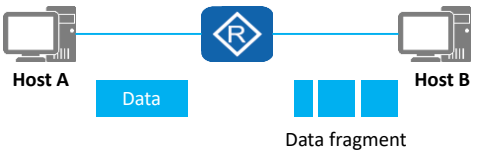


- The IP packet header contains the following information:
  - Version: 4 bits long. Value 4 indicates IPv4. Value 6 indicates IPv6.
  - Header Length: 4 bits long, indicating the size of a header. If the Option field is not carried, the length is 20 bytes. The maximum length is 60 bytes.
  - Type of Service: 8 bits long, indicating a service type. This field takes effect only when the QoS differentiated service (DiffServ) is required.
  - Total Length: 16 bits long. It indicates the total length of an IP data packet.
  - Identification: 16 bits long. This field is used for fragment reassembly.
  - Flags: 3 bits long.
  - Fragment Offset: 12 bits long. This field is used for fragment reassembly.
  - Time to Live: 8 bits long.

Data Packet Fragmentation

- The process of dividing a packet into multiple fragments is called fragmentation.
- The sizes of IP packets forwarded on a network may be different. If the size of an IP packet exceeds the maximum size supported by a data link, the packet needs to be divided into several smaller fragments before being transmitted on the link.

Version	Header Length	Type of Service	Total Length	
Identification			**Flags**	**Fragment Offset**
TTL	Protocol	Header Checksum		
Source IP Address				
Destination IP Address				
Options				Padding

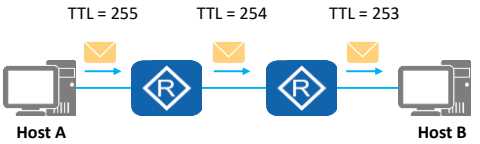


- Identification: 16 bits long. This field carries a value assigned by a sender host and is used for fragment reassembly.
- Flags: 3 bits long.
  - Reserved Fragment: 0 (reserved).
  - Don't Fragment: Value 1 indicates that fragmentation is not allowed, and value 0 indicates that fragmentation is allowed.
  - More Fragment: Value 1 indicates that there are more segments following the segment, and value 0 indicates that the segment is the last data segment.
- Fragment Offset: 12 bits long. This field is used for fragment reassembly. This field indicates the relative position of a fragment in an original packet that is fragmented. This field is used together with the More Fragment bit to help the receiver assemble the fragments.

Time to Live

- The TTL field specifies the number of routers that a packet can pass through.
- Once a packet passes through a router, the TTL is reduced by 1. If the TTL value is reduced to 0, a data packet is discarded.

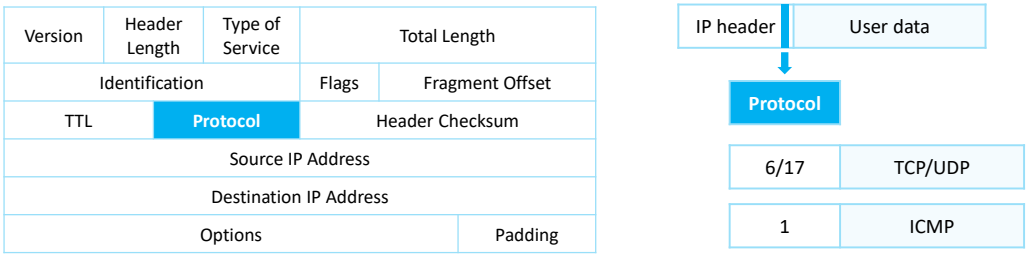
Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding



- Time to Live: 8 bits long. It specifies the maximum number of routers that a packet can pass through on a network.
  - When packets are forwarded between network segments, loops may occur if routes are not properly planned on network devices. As a result, packets are infinitely looped on the network and cannot reach the destination. If a loop occurs, all packets destined for this destination are forwarded cyclically. As the number of such packets increases, network congestion occurs.
  - To prevent network congestion induced by loops, a TTL field is added to the IP packet header. The TTL value decreases by 1 each time a packet passes through a Layer 3 device. The initial TTL value is set on the source device. After the TTL value of a packet decreases to 0, the packet is discarded. In addition, the device that discards the packet sends an ICMP error message to the source based on the source IP address in the packet header. (Note: A network device can be disabled from sending ICMP error messages to the source ends.)

Protocol

- The Protocol field in the IP packet header identifies a protocol that will continue to process the packet.
- This field identifies the protocol used by the data carried in the data packet so that the IP layer of the destination host sends the data to the process mapped to the Protocol field.

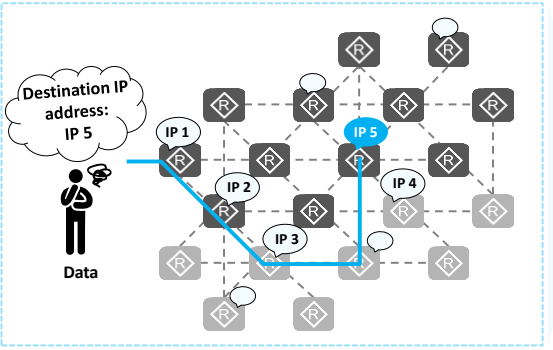


- After receiving and processing the packet at the network layer, the destination end needs to determine which protocol is used to further process the packet. The Protocol field in the IP packet header identifies the number of a protocol that will continue to process the packet.
- The field may identify a network layer protocol (for example, ICMP of value 0x01) or an upper-layer protocol (for example, Transmission Control Protocol [TCP] of value 0x06 or the User Datagram Protocol [UDP] of value 0x11).

Contents

What Is an IP Address?

- An IP address identifies a node (or an interface on a network device) on a network.
- IP addresses are used to forward IP packets on the network.



IP Address

An IP address identifies a node on a network and is used to find the destination for data.

- On an IP network, if a user wants to connect a computer to the Internet, the user needs to apply for an IP address for the computer. An IP address identifies a node on a network and is used to find the destination for data. We use IP addresses to implement global network communication.
- An IP address is an attribute of a network device interface, not an attribute of the network device itself. To assign an IP address to a device is to assign an IP address to an interface on the device. If a device has multiple interfaces, each interface needs at least one IP address.

- Note: The interface that needs to use an IP address is usually the interface of a router or computer.

IP address Notation

- An IPv4 address is 32 bits long.
- It is in dotted decimal notation.

Dotted decimal notation

	192.	168.	10.	1	
Decimal					4 bytes
Binary	**11000000**	10101000	00001010	00000001	32 bits

Conversion between decimal and binary systems

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Power	128	64	32	16	8	4	2	1
Bit	1	1	0	0	0	0	0	0

= 128 + 64 = 192

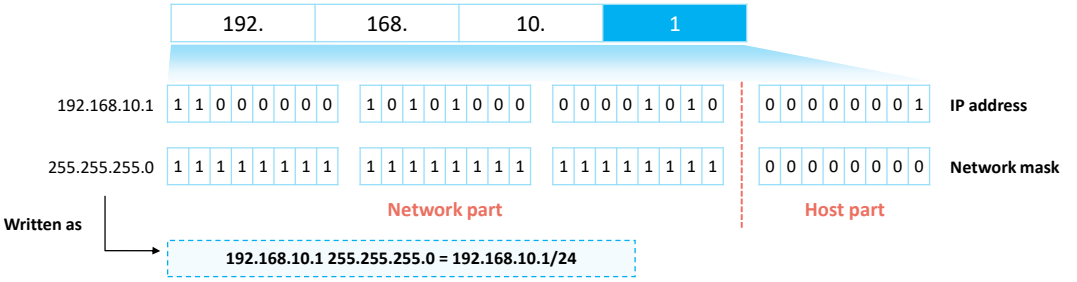
- IPv4 address range is 0.0.0.0–255.255.255.255.

- IP address notation
  - An IP address is 32 bits long and consists of 4 bytes. It is in dotted decimal notation, which is convenient for reading and writing.
- Dotted decimal notation
  - The IP address format helps us better use and configure a network. However, a communication device uses the binary mode to operate an IP address. Therefore, it is necessary to be familiar with the decimal and binary conversion.
- IPv4 address range
  - 00000000.00000000.00000000.00000000–11111111.11111111.11111111.11111111, that is, 0.0.0.0–255.255.255.255

IP Address Structure

- **Network part:** identifies a network.
- **Host part:** identifies a host and is used to differentiate hosts on a network.

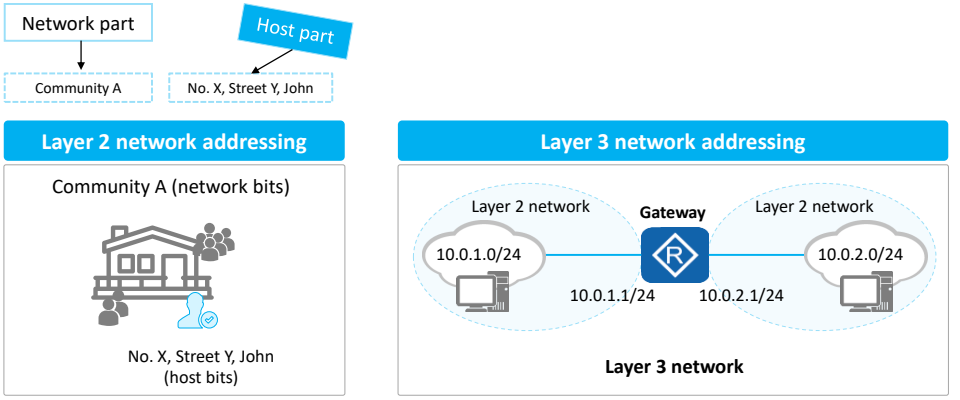
- **Network mask:** is used to distinguish the network part from the host part in an IP address.



- An IPv4 address is divided into two parts:
  - **Network part** (network ID): identifies a network.
    - IP addresses do not show any geographical information. The network ID represents the network to which a host belongs.
    - Network devices with the same network ID are located on the same network, regardless of their physical locations.
  - **Host part:** identifies a host and is used to differentiate hosts on a network.
- A network mask is also called a subnet mask:
  - A network mask is 32 bits long, which is also represented in dotted decimal notation, like bits in an IP address.
  - The network mask is not an IP address. The network mask consists of consecutive 1s followed by consecutive 0s in binary notation.
  - Generally, the number of 1s indicates the length of a network mask. For example, the length of mask 0.0.0.0 is 0, and the length of mask 252.0.0.0 is 6.
  - The network mask is generally used together with the IP address. Bits of 1 correspond to network bits in the IP address. Bits of 0 corresponds to host bits in the IP address. In other words, in an IP address, the number of 1s in a network mask is the number of bits of the network ID, and the number of 0s is the number of bits in the host ID.

IP Addressing

- **Network part (network ID):** identifies a network.
- **Host part:** identifies a host and is used to differentiate hosts on a network.



- A network ID indicates the network where a host is located, which is similar to the function of "Community A in district B of City X in province Y."
- A host ID identifies a specific host interface within a network segment defined by the network ID. The function of host ID is like a host location "No. A Street B".
- Network addressing:
  - Layer 2 network addressing: A host interface can be found based on an IP address.
  - Layer 3 network addressing: A gateway is used to forward data packets between network segments.
- Gateway:
  - During packet forwarding, a device determines a forwarding path and an interface connected to a destination network segment. If the destination host and source host are on different network segments, packets are forwarded to the gateway and then the gateway forwards the packets to the destination network segment.
  - A gateway receives and processes packets sent by hosts on a local network segment and forwards the packets to the destination network segment. To implement this function, the gateway must know the route of the destination network segment. The IP address of the interface on the gateway connected to the local network segment is the gateway address of the network segment.

IP Address Classification (Classful Addressing)

- To facilitate IP address management and networking, IP addresses are classified into the following classes:

Class A	0NNNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	0.0.0.0–127.255.255.255	Assigned to hosts
Class B	10NNNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	128.0.0.0–191.255.255.255	
Class C	110NNNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	192.0.0.0–223.255.255.255	
Class D	1110NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	224.0.0.0–239.255.255.255	Used for multicast
Class E	1111NNNN	NNNNNNNN	NNNNNNNN	NNNNNNNN	240.0.0.0–255.255.255.255	Used for research

- Default subnet masks of classes A, B, and C
  - Class A: 8 bits, 0.0.0.0–127.255.255.255/8
  - Class B: 16 bits, 128.0.0.0–191.255.255.255/16
  - Class C: 24 bits, 192.0.0.0-223.255.255.255/24

Network part

Host part

HUAWEI

- To facilitate IP address management and networking, IP addresses are classified into the following classes:
  - The easiest way to determine the class of an IP address is to check the most significant bits in a network ID. Classes A, B, C, D, and E are identified by binary digits 0, 10, 110, 1110, and 1111, respectively.
  - Class A, B, and C addresses are unicast IP addresses (except some special addresses). Only these addresses can be assigned to host interfaces.
  - Class D addresses are multicast IP addresses.
  - Class E addresses are used for special experiment purposes.
  - This presentation only focuses on class A, B, and C addresses.
- Comparison of class A, B, and C addresses:
  - A network using class A addresses is called a class A network. A network using class B addresses is called a class B network. A network that uses class C addresses is called a class C network.
  - The network ID of a class A network is 8 bits, indicating that the number of network IDs is small and a large number of host interfaces are supported. The leftmost bit is fixed at 0, and the address space is 0.0.0.0–127.255.255.255.
  - The network ID of class B network is 16 bits, which is between class A and class C networks. The leftmost two bits are fixed at 10, and the address space is 128.0.0.0–191.255.255.255.
  - The network ID of a class C network is 24 bits, indicating that a large number of network IDs are supported, and the number of host interfaces is small. The leftmost three bits are fixed at 110, and the address space is 192.0.0.0–223.255.255.255.

IP Address Types

- A network range defined by a network ID is called a network segment.
- **Network address**: identifies a network.

  Example: 192.168.10.0/24

192.	168.	10.	00000000

- **Broadcast address**: a special address used to send data to all hosts on a network.

  Example: 192.168.10.255/24

192.	168.	10.	11111111

- **Available addresses**: IP addresses that can be allocated to device interfaces on a network.

  Example: 192.168.10.1/24

192.	168.	10.	00000001

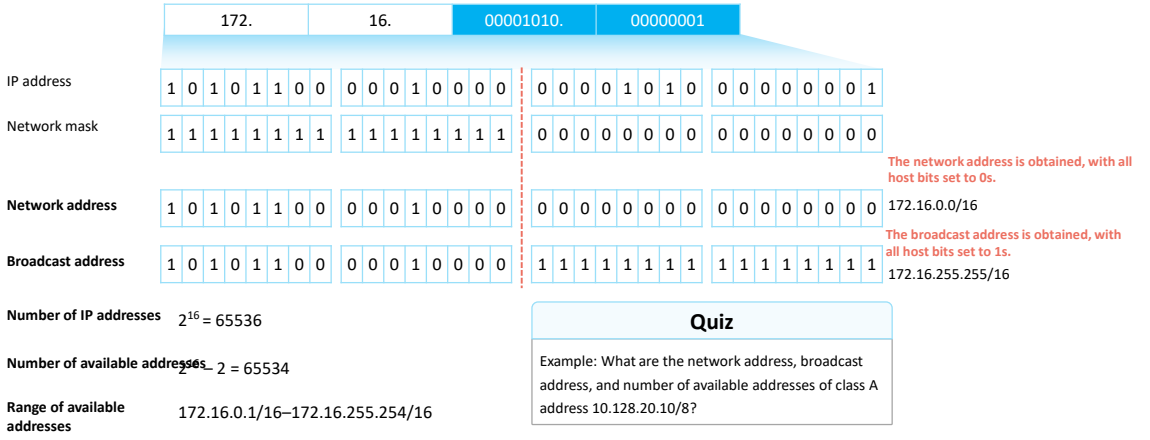
Note

- Network and broadcast addresses cannot be directly used by devices or their interfaces.
- Number of available addresses on a network segment is $2^n - 2$ (n is the number of bits in the host part).

- Network address
  - The network ID is X, and each bit in the host ID is 0.
  - It cannot be assigned to a host interface.
- Broadcast address
  - The network ID is X, and each bit in the host ID is 1.
  - It cannot be assigned to a host interface.
- Available address
  - It is also called a host address. It can be assigned to a host interface.
- The number of available IP addresses on a network segment is calculated using the following method:
  - Given that the host part of a network segment is n bits, the number of IP addresses is 2^n, and the number of available IP addresses is $2^n - 2$ (one network address and one broadcast address).

IP Address Calculation

- Example: What are the network address, broadcast address, and number of available addresses of class B address 172.16.10.1/16?

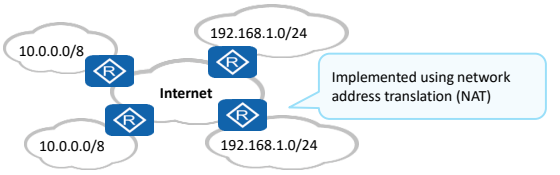


- Network address: After the host part of this address is set to all 0s, the obtained result is the network address of the network segment where the IP address is located.
- Broadcast address: After the host part of this address is set to all 1s, the obtained result is the broadcast address used on the network where the IP address is located.
- Number of IP addresses: 2^n, where n indicates the number of host bits.
- Number of available IP addresses: $2^n - 2$, where n indicates the number of host bits.

- Answers to the quiz:
  - Network address: 10.0.0.0/8
  - Broadcast address: 10.255.255.255
  - Number of addresses: 2^{24}
  - Number of available addresses: $2^{24} - 2$
  - Range of available addresses: 10.0.0.1/8–10.255.255.254/8

Private IP Addresses

- **Public IP address:** An IP address is assigned by the Internet Assigned Numbers Authority (IANA), and this address allocation mode ensures that each IP address is unique on the Internet. Such an IP address is a public IP address.
- **Private IP address:** In practice, some networks do not need to connect to the Internet. For example, on a network of a lab in a college, IP addresses of devices need to avoid conflicting with each other only within the same network. In the IP address space, some IP addresses of class A, B, and C addresses are reserved for the preceding situations. These IP addresses are called private IP addresses.
  - Class A: 10.0.0.0–10.255.255.255
  - Class B: 172.16.0.0–172.31.255.255
  - Class C: 192.168.0.0–192.168.255.255



Connecting a private network to the Internet

- Private IP addresses are used to relieve the problem of IP address shortage. Private addresses are used on internal networks and hosts, and cannot be used on the public network.
  - Public IP address: A network device connected to the Internet must have a public IP address allocated by the IANA.
  - Private IP address: The use of a private IP address allows a network to be expanded more freely, because a same private IP address can be repeatedly used on different private networks.
- Connecting a private network to the Internet: A private network is not allowed to connect to the Internet because it uses a private IP address. Driven by requirements, many private networks also need to connect to the Internet to implement communication between private networks and the Internet, and between private networks through the Internet. The interconnection between the private network and Internet must be implemented using the NAT technology.

- Note: Network Address Translation (NAT) is used to translate addresses between private and public IP address realms.

Special IP Addresses

- Some IP addresses in the IP address space are of special meanings and functions.
- For example:

Special IP Address	Address Scope	Function
Limited broadcast address	255.255.255.255	It can be used as a destination address and traffic destined for it is sent to all hosts on the network segment to which the address belongs. (Its usage is restricted by a gateway).
Any IP address	0.0.0.0	It is an address of any network. Addresses in this block refer to source hosts on "this" network.
Loopback address	127.0.0.0/8	It is used to test the software system of a test device.
Link-local address	169.254.0.0/24	If a host fails to automatically obtain an IP address, the host can use an IP address in this address block for temporary communication.

- 255.255.255.255
  - This address is called a limited broadcast address and can be used as the destination IP address of an IP packet.
  - After receiving an IP packet whose destination IP address is a limited broadcast address, the router stops forwarding the IP packet.
- 0.0.0.0
  - If this address is used as a network address, it means the network address of any network. If this address is used as the IP address of a host interface, it is the IP address of a source host interface on "this" network.
  - For example, if a host interface does not obtain its IP address during startup, the host interface can send a DHCP Request message with the destination IP address set to a limited broadcast address and the source IP address set to 0.0.0.0 to the network. The DHCP server is expected to allocate an available IP address to the host interface after receiving the DHCP Request message.
- 127.0.0.0/8
  - This address is called a Loopback address and can be used as the destination IP address of an IP packet. It is used to test the software system of a test device.
  - The IP packets that are generated by a device and whose destination IP address is set to a Loopback address cannot leave the device itself.
- 169.254.0.0/16
  - If a network device is configured to automatically obtain an IP address but no DHCP server is available on the network, the device uses an IP address in the 169.254.0.0/16 network segment for temporary communication.
- Note: The Dynamic Host Configuration Protocol (DHCP) is used to dynamically allocate network

configuration parameters, such as IP addresses.

IPv4 vs. IPv6

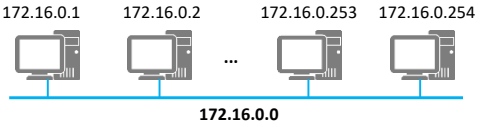
- IPv4 addresses managed by the IANA were exhausted in 2011. As the last public IPv4 address was allocated and more and more users and devices access the public network, IPv4 addresses were exhausted. This is the biggest driving force for IPv6 to replace IPv4.

IPv4	IPv6

• Address length: 32 bits
• Address types: unicast address, broadcast address, and multicast address
• Characteristics:
  ▫ IPv4 address depletion
  ▫ Inappropriate packet header design
  ▫ ARP dependency-induced flooding
  ▫ ...
	• Address length: 128 bits
	• Address types: unicast address, multicast address, and anycast address
	• Characteristics:
	  ▫ Unlimited number of addresses
	  ▫ Simplified packet header
	  ▫ Automatic IPv6 address allocation
	  ▫ ...

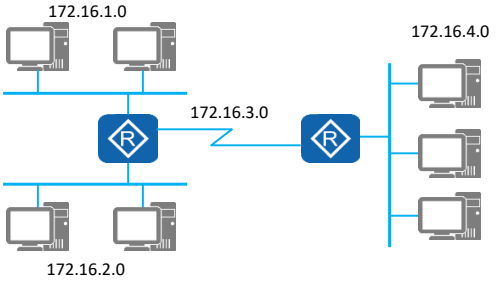
Contents

Why Subnetting?



2^{16} = 65536 IP addresses

- A class B address is used for a broadcast domain, wasting addresses.
- The broadcast domain is too large. Once broadcast occurs, an internal network is overloaded.

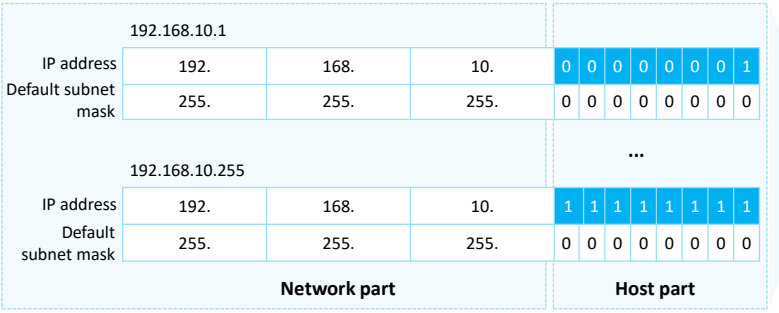


- A network number is divided into multiple subnets, and each subnet is allocated to a separate broadcast domain.
- In this way, the broadcast domain is smaller, and the network planning is more reasonable.
- IP addresses are properly used.

- Classful addressing is too rigid and the granularity of address division is too large. As a result, a large number of host IDs cannot be fully used, wasting IP addresses.
- Therefore, subnetting can be used to reduce address waste through the variable length subnet mask (VLSM) technology. A large classful network is divided into several small subnets, which makes the use of IP addresses more scientific.

Subnetting - Analyzing the Original Network Segment

- Example: 192.168.10.0/24



One class C network:

192.168.10.0/24

Default subnet mask:

255.255.255.0

Network address: 192.168.10.0/24

Broadcast address: 192.168.10.255

Total IP addresses: $2^8 = 256$

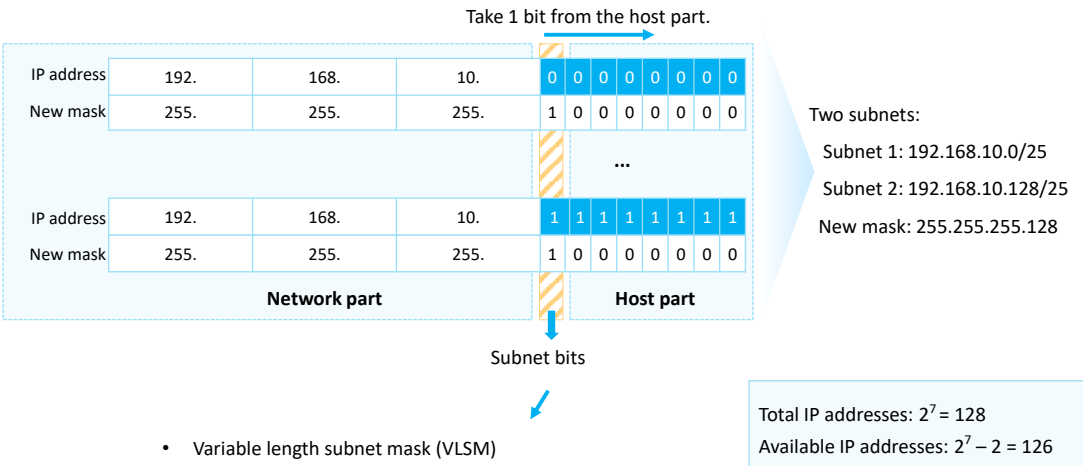
Available IP addresses: $2^8 - 2 = 254$

HUAWEI

- Assume that a class C network segment is 192.168.10.0. By default, the network mask is 24 bits, including 24 network bits and 8 host bits.
- As calculated, there are 256 IP addresses on the network.

Subnetting - Taking Bits from the Host Part

- Bits can be taken from the host part to create subnets.



- Variable length subnet mask (VLSM)

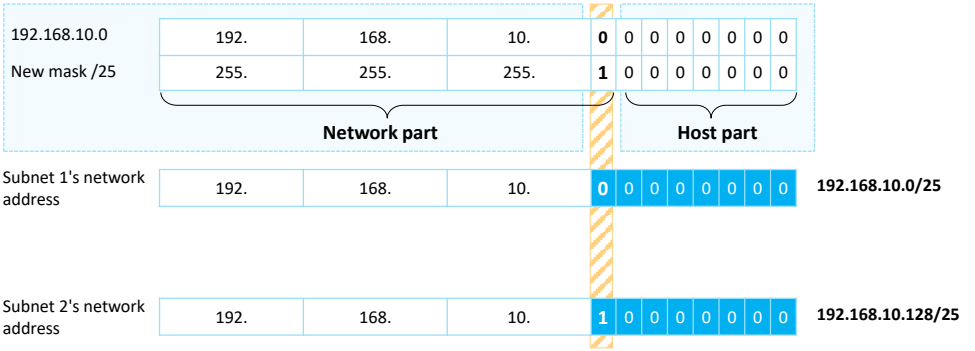
Total IP addresses: $2^7 = 128$
Available IP addresses: $2^7 - 2 = 126$

HUAWEI

- Now, for the original 24-bit network part, a host bit is taken to increase the network part to 25 bits. The host part is reduced to 7 bits. The taken 1 bit is a subnet bit. In this case, the network mask becomes 25 bits, that is, 255.255.255.128, or /25.
- Subnet bit: The value can be 0 or 1. Two new subnets are obtained.
- As calculated, there are 128 IP addresses on the network.

Subnetting - Calculating the Subnet Network Address

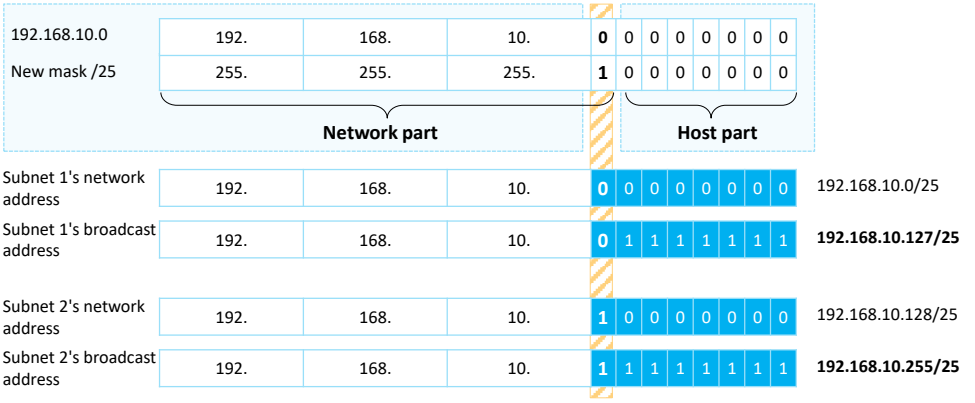
- The network address is obtained, with all host bits set to 0s.



- Calculate a network address, with all host bits set to 0s.
  - If the subnet bit is 0, the network address is 192.168.10.0/25.
  - If the subnet bit is 1, the network address is 192.168.10.128/25.

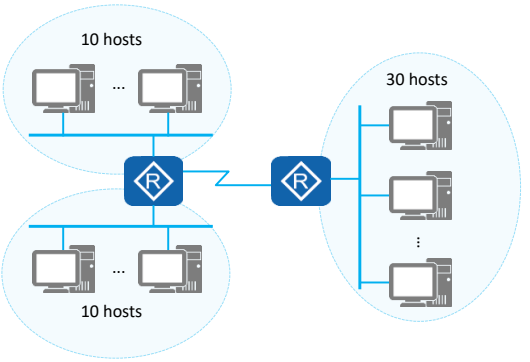
Subnetting - Calculating the Subnet Broadcast Address

- The broadcast address is obtained, with all host bits set to 1s.



- Calculate a broadcast address, with all host bits set to 1s.
  - If the subnet bit is 0, the network address is 192.168.10.127/25.
  - If the subnet bit is 1, the network address is 192.168.10.255/25.

Practice: Computing Subnets (1)



- **Question:** An existing class C network segment is 192.168.1.0/24. Use the VLSM to allocate IP addresses to three subnets.

- **Answer:** (Use a network with 10 hosts as an example.)

  Step 1: Calculate the number of host bits to be taken.

  $2^n - 2 \geq 10$

  $n \geq 4$, host bits

  Step 2: Take bits from the host part.

Take 4 bits from the host part.

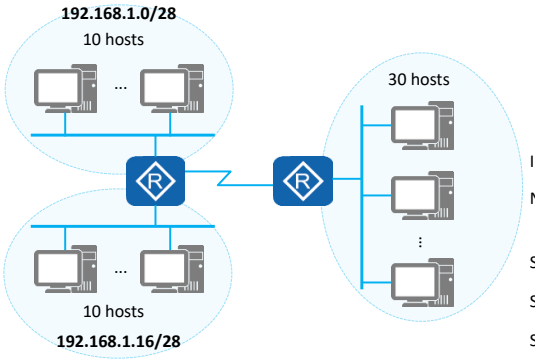
IP address	192.	168.	1.	**0**	**0**	**0**	**0**	0	0	0	0
Subnet mask	255.	255.	255.	1	1	1	1	0	0	0	0

Subnet bits

Number of subnets: $2^4 = 16$ subnets

- In actual network planning, the subnet with more hosts is planned first.

Practice: Computing Subnets (2)



- **Question:** An existing class C network segment is 192.168.1.0/24. Use the VLSM to allocate IP addresses to three subnets.
- **Answer:** (Use a network with 10 hosts as an example.)

Step 3: Calculate subnet network addresses.

IP address	192.	168.	1.	**0**	**0**	**0**	**0**	0	0	0	0
New mask	255.	255.	255.	1	1	1	1	0	0	0	0
											Network address
Subnet 1	192.	168.	1.	0	0	0	0	0	0	0	192.168.1.0/28
Subnet 2	192	168.	1.	0	0	0	1	0	0	0	192.168.1.16/28
Subnet 3	192.	168.	1.	0	0	1	0	0	0	0	192.168.1.32/28
⋮											
Subnet 16	192.	168.	1.	1	1	1	1	0	0	0	192.168.1.240/28

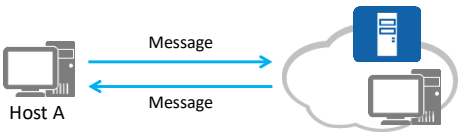
HUAWEI

- Subnet network addresses are:
  - 192.168.1.0/28
  - 192.168.1.16/28
  - 192.168.1.32/28
  - 192.168.1.48/28
  - 192.168.1.64/28
  - 192.168.1.80/28
  - 192.168.1.96/28
  - 192.168.1.112/28
  - 192.168.1.128/28
  - 192.168.1.144/28
  - 192.168.1.160/28
  - 192.168.1.176/28
  - 192.168.1.192/28
  - 192.168.1.208/28
  - 192.168.1.224/28
  - 192.168.1.240/28

Contents

ICMP

- The Internet Control Message Protocol (ICMP) is an auxiliary protocol of the IP protocol.
- ICMP is used to transmit error and control information between network devices. It plays an important role in collecting network information, diagnosing and rectifying network faults.



Ethernet header	IP header	**ICMP message**	Ethernet tail

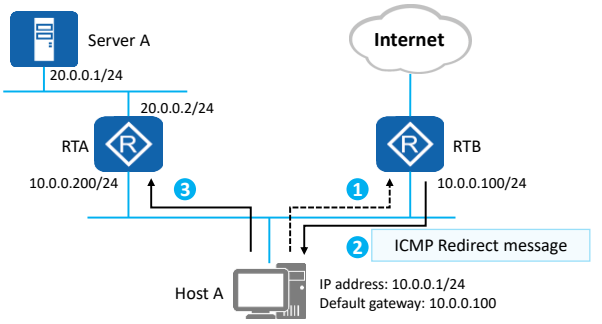
Type	**Code**	Checksum
ICMP message content		

Type	Code	Description
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
5	0	Redirect
8	0	Echo Request

- To improve the efficiency of IP data packet forwarding and success rate of packet exchanges, ICMP is used at the network layer. ICMP allows hosts and devices to report errors during packet transmission.
- ICMP message:
  - ICMP messages are encapsulated in IP packets. Value 1 in the Protocol field of the IP packet header indicates ICMP.
  - Explanation of fields:
    - The format of an ICMP message depends on the Type and Code fields. The Type field indicates a message type, and the Code field contains a parameter mapped to the message type.
    - The Checksum field is used to check whether a message is complete.
    - A message contains a 32-bit variable field. This field is not used and is usually set to 0.
      - In an ICMP Redirect message, this field indicates the IP address of a gateway. A host redirects packets to the specified gateway that is assigned this IP address.
      - In an Echo Request message, this field contains an identifier and a sequence number. The source associates the received Echo Reply message with the Echo Request message sent by the local end based on the identifiers and sequence numbers carried in the messages. Especially, when the source sends multiple Echo Request messages to the destination, each Echo Reply message must carry the same identifier and sequence number as those carried in the Echo Request message.

ICMP Redirection

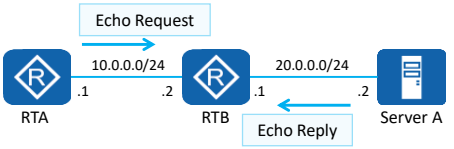
- ICMP Redirect messages are a type of ICMP control message. When a router detects that a host uses a non-optimal route in a specific scenario, the router sends an ICMP Redirect message to the host, requesting the host to change the route.



- ICMP redirection process:
  1. Host A wants to send packets to server A. Host A sends packets to the default gateway address that is assigned to the gateway RTB.
  2. After receiving the packet, RTB checks packet information and finds that the packet should be forwarded to RTA. RTA is the other gateway on the same network segment as the source host. This forwarding path through RTA is better than that through RTB. Therefore, RTB sends an ICMP Redirect message to the host, instructing the host to send the packet to RTA.
  3. After receiving the ICMP Redirect message, the host sends a packet to RTA. Then RTA forwards the packet to server A.

ICMP Error Detection

- ICMP Echo messages are used to check network connectivity between the source and destination and provide other information, such as the round-trip time.



Function: Ping

Ping is a command used on network devices, Windows OS, Unix OS, and Linux OS. Ping is a small and useful application based on the ICMP protocol.

A ping tests the reachability of a destination node.

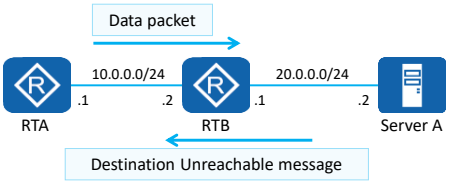
```
[RTA]ping 20.0.0.2
  PING 20.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 20.0.0.2: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 20.0.0.2: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 20.0.0.2: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 20.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/40/70 ms
```


- A typical ICMP application is ping. Ping is a common tool used to check network connectivity and collect other related information. Different parameters can be specified in a ping command, such as the size of ICMP messages, number of ICMP messages sent at a time, and the timeout period for waiting for a reply. Devices construct ICMP messages based on the parameters and perform ping tests.

ICMP Error Report

- ICMP defines various error messages for diagnosing network connectivity problems. The source can determine the cause for a data transmission failure based on the received error messages. For example, after a network device receives a packet, it cannot access the network where the destination device resides, the network device automatically sends an ICMP Destination Unreachable message to the source.



[RTA]tracert 20.0.0.2

traceroute to 20.0.0.2(20.0.0.2), max hops: 30 ,packet length: 40,press CTRL_C
to break

1 10.0.0.2	80 ms	10 ms	10 ms
2 20.0.0.2	30 ms	30 ms	20 ms

Function: Tracert

Tracert checks the reachability of each hop on a forwarding path based on the TTL value carried in the packet header.

Tracert is an effective method to detect packet loss and delay on a network and helps administrators discover routing loops on the network.

- ICMP defines various error messages for diagnosing network connectivity problems. The source can determine the cause for a data transmission failure based on the received error messages.
  - If a loop occurs on the network, packets are looped on the network, and the TTL times out, the network device sends a TTL timeout message to the sender device.
  - If the destination is unreachable, the intermediate network device sends an ICMP Destination Unreachable message to the sender device. There are a variety of cases for unreachable destination. If the network device cannot find the destination network, the network device sends an ICMP Destination Network Unreachable message. If the network device cannot find the destination host on the destination network, the network device sends an ICMP Destination Host Unreachable message.
- Tracert is a typical ICMP application. Tracert checks the reachability of each hop on a forwarding path based on the TTL value carried in the packet header. In a tracert test for a path to a specific destination address, the source first sets the TTL value in a packet to 1 before sending the packet. After the packet reaches the first node, the TTL times out. Therefore, the first node sends an ICMP TTL Timeout message carrying a timestamp to the source. Then, the source sets the TTL value in a packet to 2 before sending the packet. After the packet reaches the second node, the TTL times out. The second node also returns an ICMP TTL Timeout message. The process repeats until the packet reaches the destination. In this way, the source end can trace each node through which the packet passes based on the information in the returned packet, and calculate the round-trip time based on timestamps.

Contents

Basic IP Address Configuration Commands

1. Enter the interface view.

   [Huawei] **interface** *interface-type interface-number*

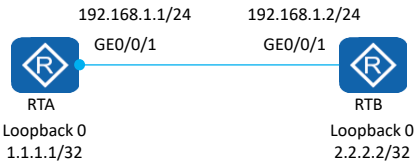
   You can run this command to enter the view of a specified interface and configure attributes for the interface.
   - *interface-type interface-number*: specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.

2. Configure an IP address for the interface.

   [Huawei-GigabitEthernet0/0/1] **ip address** *ip-address* { *mask* | *mask-length* }

   You can run this command in the interface view to assign an IP address to the interface on the network devices to implement network interconnection.
   - *ip-address*: specifies the IP address of an interface. The value is in dotted decimal notation.
   - *mask*: specifies a subnet mask. The value is in dotted decimal notation.
   - *mask-length*: specifies a mask length. The value is an integer ranging from 0 to 32.

Case: Configuring an IP address for an Interface



On the preceding network where the two routers are interconnected, configure IP addresses for the interconnected physical interfaces and logical IP addresses.

Configure an IP address for a physical interface.

```
[RTA] interface gigabitethernet 0/0/1
[RTA-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
                Or,
[RTA-GigabitEthernet0/0/1] ip address 192.168.1.1 24
```

Configure an IP address for a logical interface.

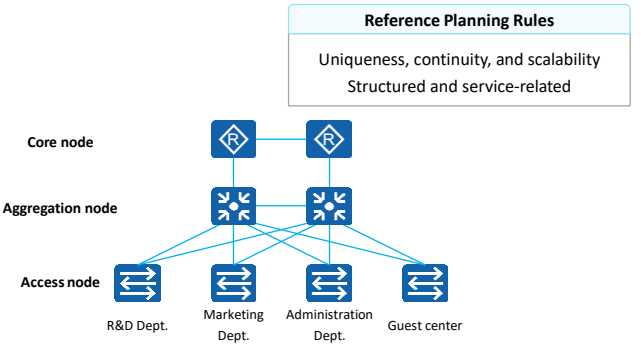
```
[RTA] interface LoopBack 0
[RTA-LoopBack0] ip address 1.1.1.1 255.255.255.255
                Or,
[RTA-LoopBack0] ip address 1.1.1.1 32
```


- Physical interface: is an existing port on a network device. A physical interface can be a service interface transmitting services or a management interface managing the device. For example, a GE service interface and an MEth management interface are physical interfaces.
- Logical interface: is a physically nonexistent interface that can be created using configuration and need to transmit services. For example, a VLANIF interface and Loopback interfaces are logical interfaces.
    - Loopback interface: is always in the up state.
        - Once a Loopback interface is created, its physical status and data link protocol status always stay up, regardless of whether an IP address is configured for the Loopback interface.
        - The IP address of a Loopback interface can be advertised immediately after being configured. A Loopback interface can be assigned an IP address with a 32-bit mask, which reduces address consumption.
        - No data link layer protocols can be encapsulated on a Loopback interface. No negotiation at the data link layer is performed for the Loopback interface. Therefore, the data link protocol status of the Loopback interface is always up.
        - The local device directly discards a packet whose destination address is not the local IP address but the outbound interface is the local Loopback interface.

Network IP Address Planning

- IP address planning must be considered together with the network structure, routing protocols, traffic planning, and service rules. In addition, IP address planning should be corresponding to the network hierarchy and performed in a top-bottom way.
- In conclusion, IP address planning objectives are to achieve easy management, easy scalability, and high utilization.
- **IP Address Planning Example**

Background	Address Type	Address Scope
Example: A company is assigned 192.168.0.0/16 as a network segment address.	Network segment of the R&D department	192.168.1.0/24
	Network segment of the marketing department	192.168.2.0/24
	Network segment of the administrative department	192.168.3.0/24
	Network segment of the guest center	192.168.4.0/24
	Others	...



- Planning rules:
  - Uniqueness: Each host on an IP network must have a unique IP address.
  - Continuity: Contiguous addresses can be summarized easily in the hierarchical networking. Route summarization reduces the size of the routing table and speeds up route calculation and route convergence.
  - Scalability: Addresses need to be properly reserved at each layer, ensuring the contiguous address space for route summarization when the network is expanded. Re-planning of addresses and routes induced by network expansion is therefore prevented.
  - Combination of topology and services: Address planning is combined with the network topology and network transport service to facilitate route planning and quality of service (QoS) deployment. Appropriate IP address planning helps you easily determine the positions of devices and types of services once you read the IP addresses.

Quiz

1. (Multiple) Which class does 201.222.5.64 belong? ( )
   A. Class A
   B. Class B
   C. Class C
   D. Class D
2. (Multiple) A company is assigned a class C network segment 192.168.20.0/24. One of its departments has 40 hosts. Which of the following subnets can be allocated? ( )
   A. 192.168.20.64/26
   B. 192.168.20.64/27
   C. 192.168.20.128/26
   D. 192.168.20.190/26

1. C
2. AC

Summary

- To connect a PC to the Internet, apply an IP address from the Internet Service Provider (ISP).
- This presentation provides an overview of the IP protocol and describes concepts related to IPv4 addresses and subnetting.
- This presentation also describes the planning and basic configuration of IP addresses.


Thank You
www.huawei.com