Summer Network Package

Dongqi Guo

05/16/2017

At Northeastern University

Wireless Network 02

Ethernet 05

Protocols 06

General 22

Algorithm 29

Top Brief Interview Questions 30

Interview Test Questions 40

Wireless Network

1: What are wireless LANs?

Wireless LANs involve a collection of machines which communicate with each other using radio links. In the former case, base station is called an access point, in the latter case, communication take place directly among machines and such a network is known as an “ad hoc network”.

2: What is a hidden station problem in wireless LANs?

In a wireless LAN, problem arises when a station is not able to detect a transmission which is already going on because it is out of range.

3: What is an exposed station problem in wireless LANs?

When a station senses the channel and knows that there is an ongoing transmission, it does not transmit to its destination even though the destination may be located at a place where frames can be easily received.

4: What is the structure of IEEE 802.3 frame?

An IEEE802.3 frame(CSMA/CD) is composed of following fields:

a) Preamble: It is a 8-byte field where each byte is composed of 10101010 pattern and it is used to synchronize the receiver with the sender.

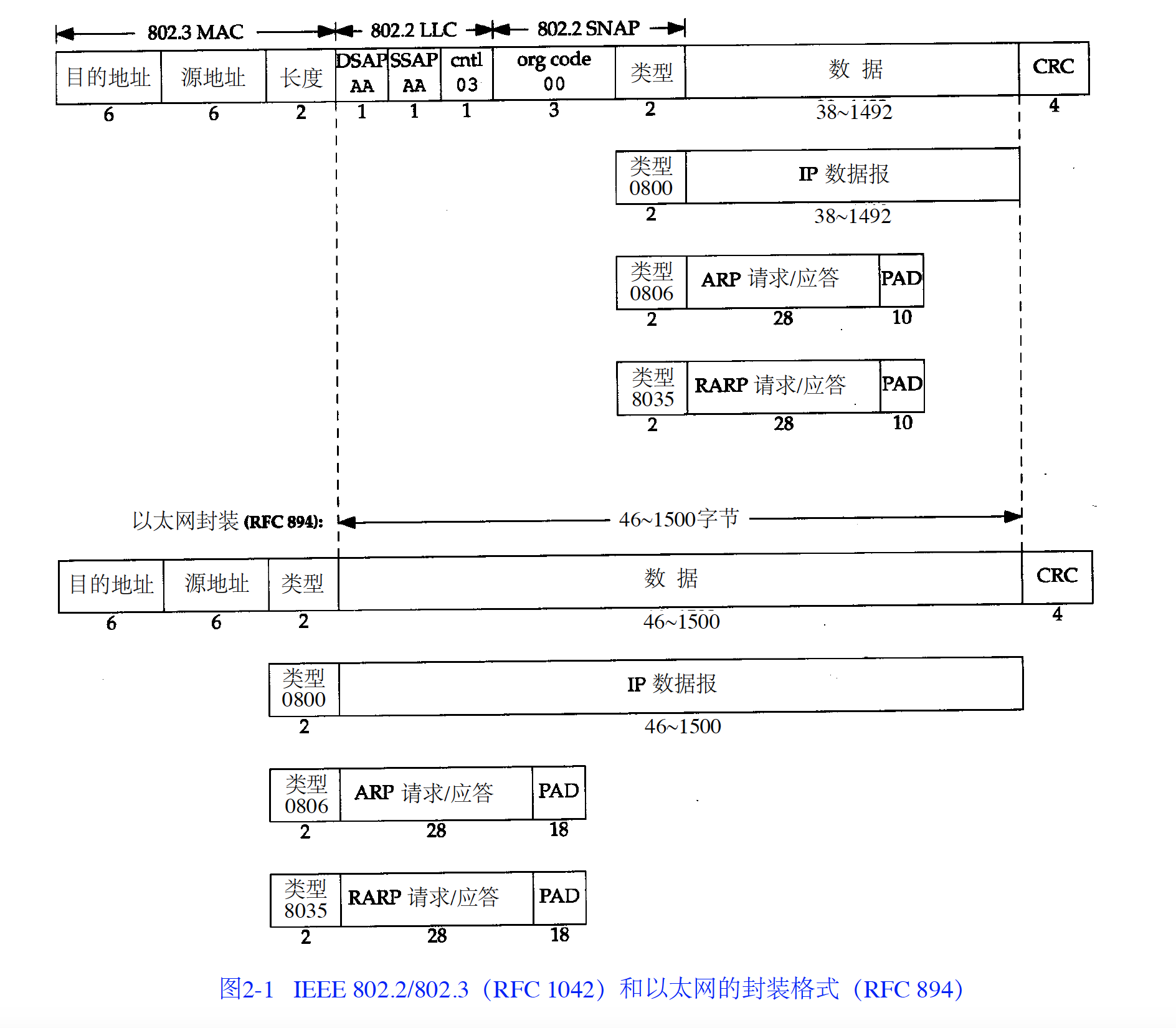
b) Destination: It is a 6-byte field and contains the address of the destination.

c) Source: It is a 6-byte field and contains the address of the source machine.

d) Length: It is 2-byte field and is used to specify the maximum frame length.

e) Data: This field contains the data to be transmitted. The maximum size of data is 1500 bytes. f) Pad: It is a 46 bytes field and is used to fill the frame when data field contains less than 46 bytes so that frame must have minimum length.

g) Checksum: It is a 4-byte field and it is the count of binary bits of the data.



CRC checksum addition:

1. IP packet check only IP header
2. ICMP packet check header and data
3. Transport layer packet check header and data
4. TCP CRC check is required, UDP is optional
5. Transport layer check will add a fake IP header (4B IP source, 4B IP destination, 2B protocol type, 2B length)
6. If TCP or UDP packet is odd length, padding 0 to tail

CRC checksum method:

1. Set checksum to zero
2. split all checked data 16bits(2Bytes) as a group
3. add them in binary format or hex format
4. ~ the previous result



5: What is Bluetooth?

It is an IEEE 802.15 wireless standard in which short radio waves are used to interconnect various computing and communication devices with each other. For example, a mobile phone can be connected to a PDA using Bluetooth. The maximum range of a Bluetooth network is 10 meters.

6: What is an ad hoc network?

An ad hoc network consists of a collection of machines in which both nodes and routers are mobile and each machine can be a node as well as a router.

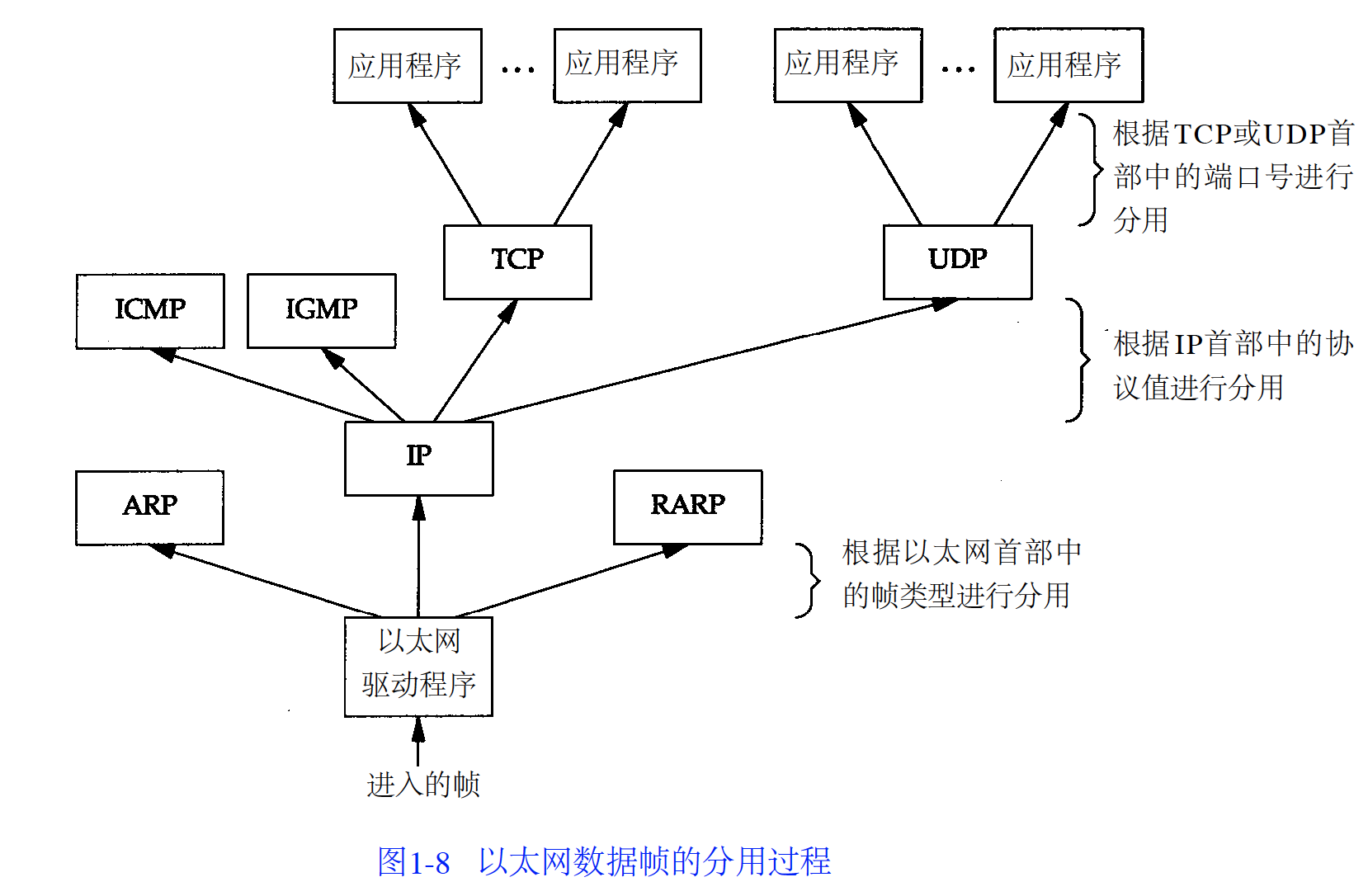
Ethernet

1: What do you mean by the term “Ethernet”?

Ethernet is a network in which multiple machines are connected by a thick coaxial cable (ether). In Ethernet, if a machine wants to send packets over the cable then it first listens to the cable. If another machine is already transmitting a packet then it waits until transmission is over so that there are no collisions and hence no interference. An example of Ethernet is IEEE 802.3 (LAN) standard. The speed of the Ethernet is usually 100 Mbps and more.

2: What is fast Ethernet?

To increase the speed of 802.3 from 10Mbps to 100Mbps, a new standard was approved known as 802.3u which is called fast Ethernet.



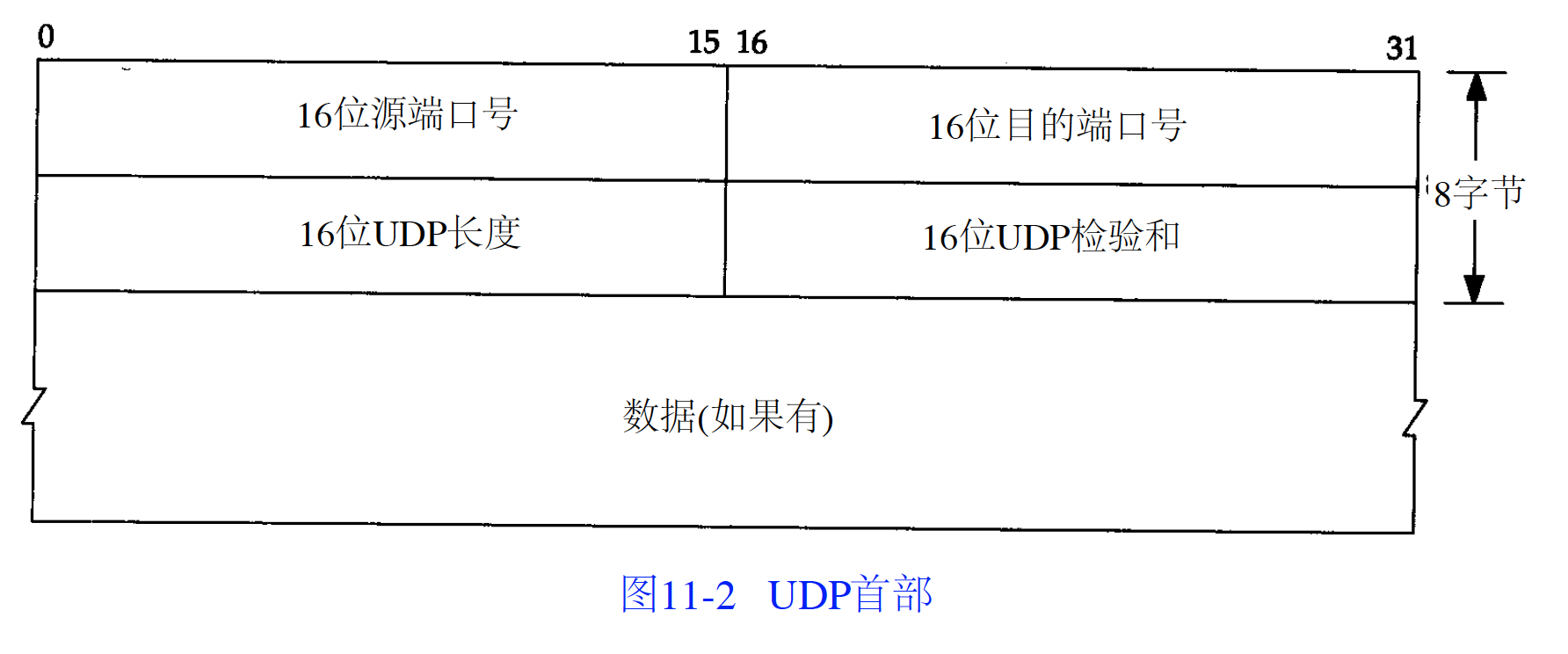
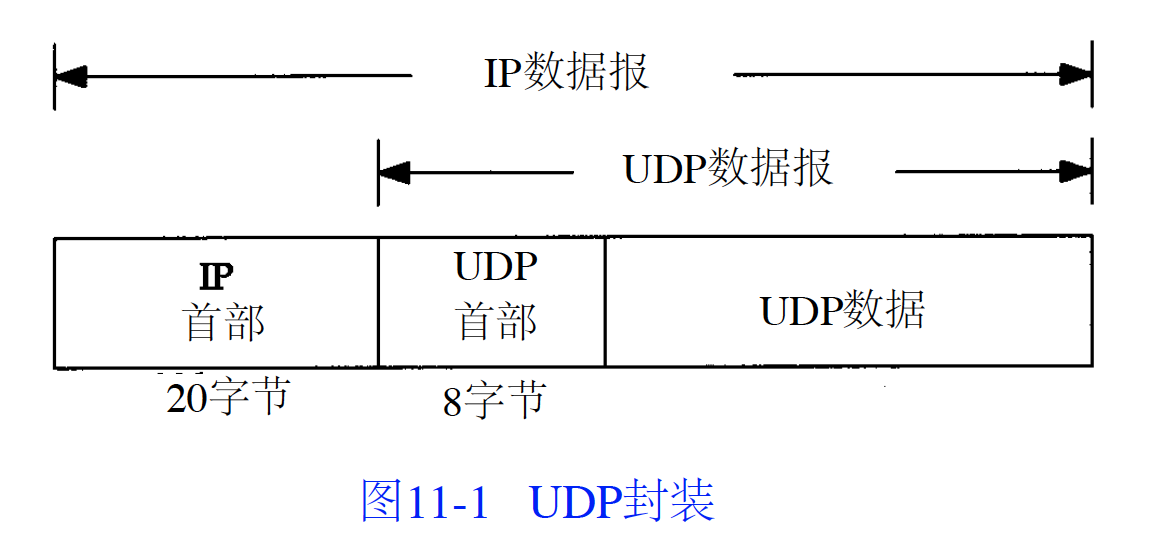
Protocols

1: What is the difference between Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?

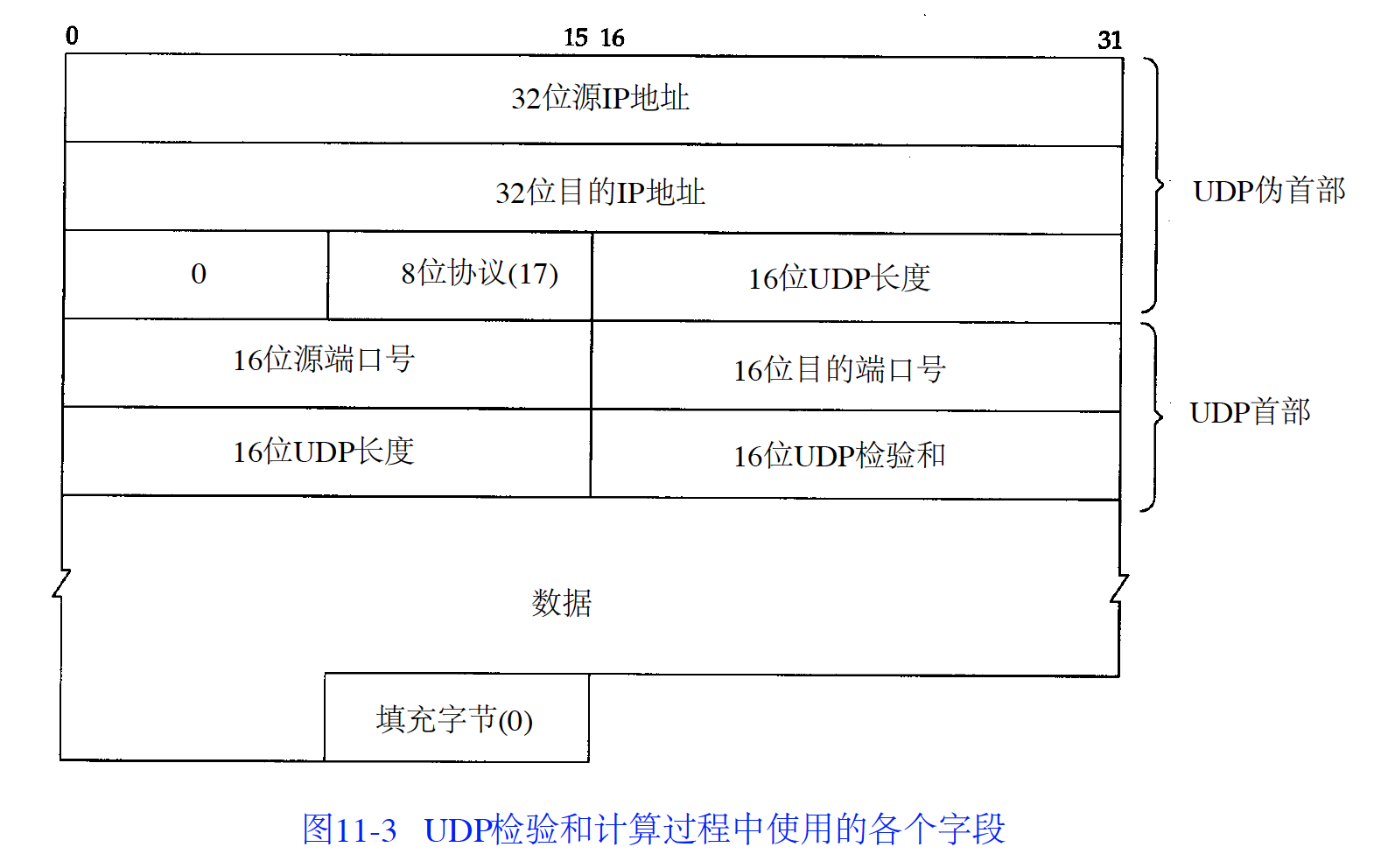
TCP is a reliable and connection-oriented protocol. It delivers data to any machine on the network without any error. It breaks the incoming message into small packets and sends the packets sequentially over the network to the destination.

UDP is an unreliable and connection-less protocol. It does not guarantee the correct delivery of the packets. UDP is used for applications which require immediate delivery and may not require correct delivery of packets such as audio or video streaming.

UDP addition:

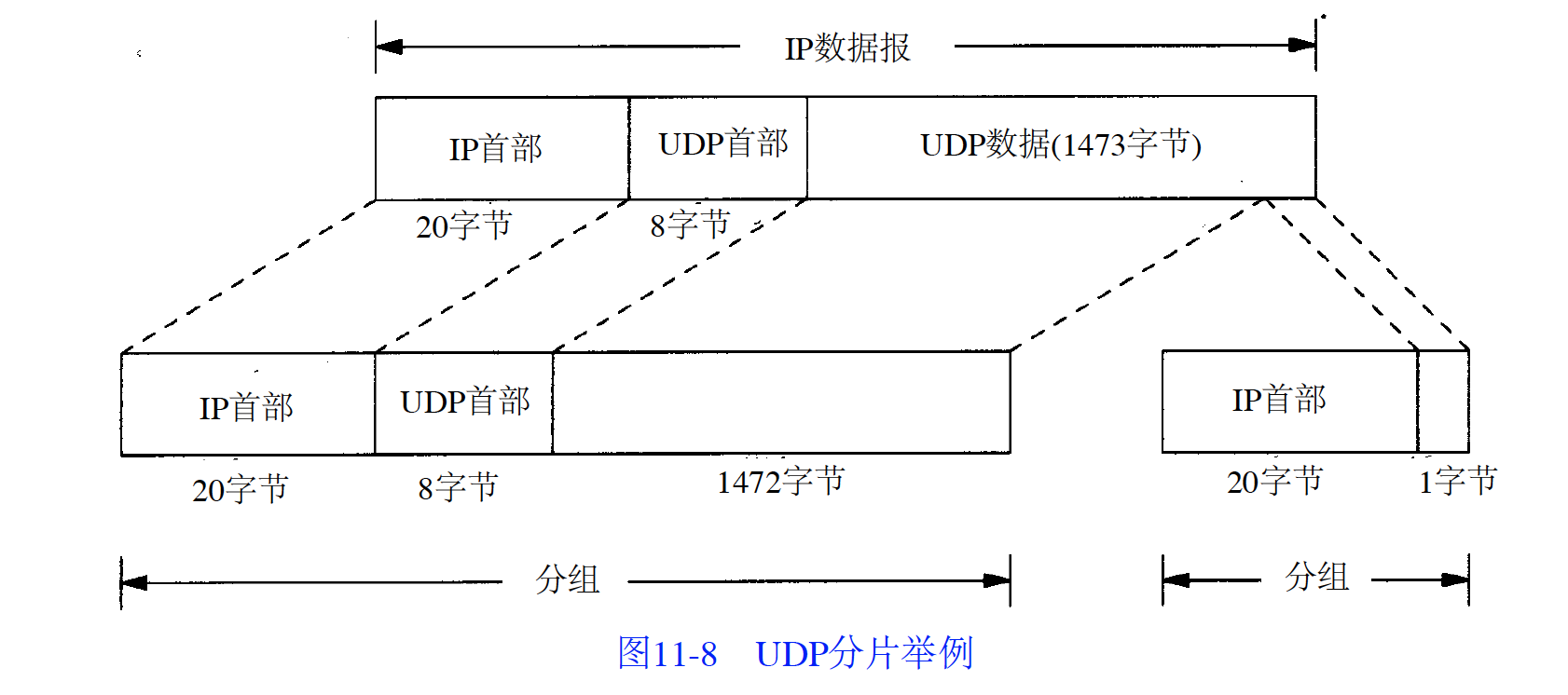


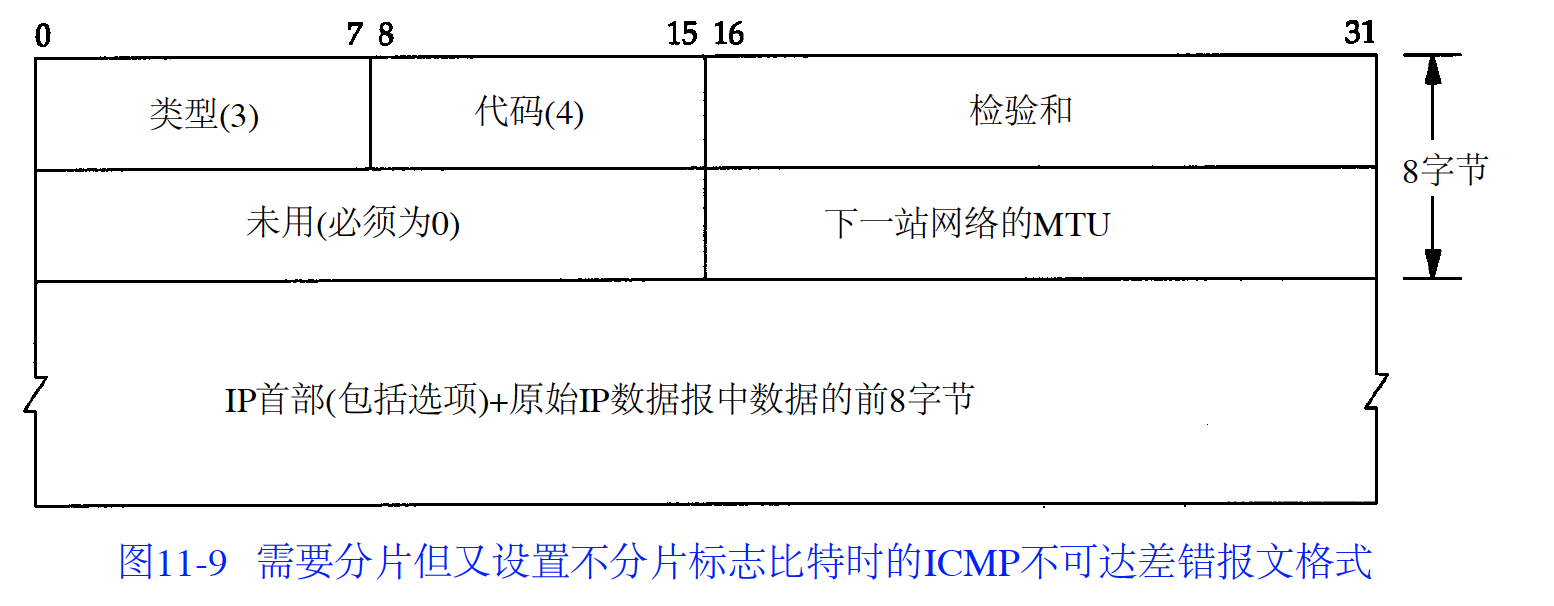
TCP ports and UDP ports are independent. Identified by IP packet’s protocol attribute value.



TCP and UDP include a fake 12 bytes’ header to do checksum

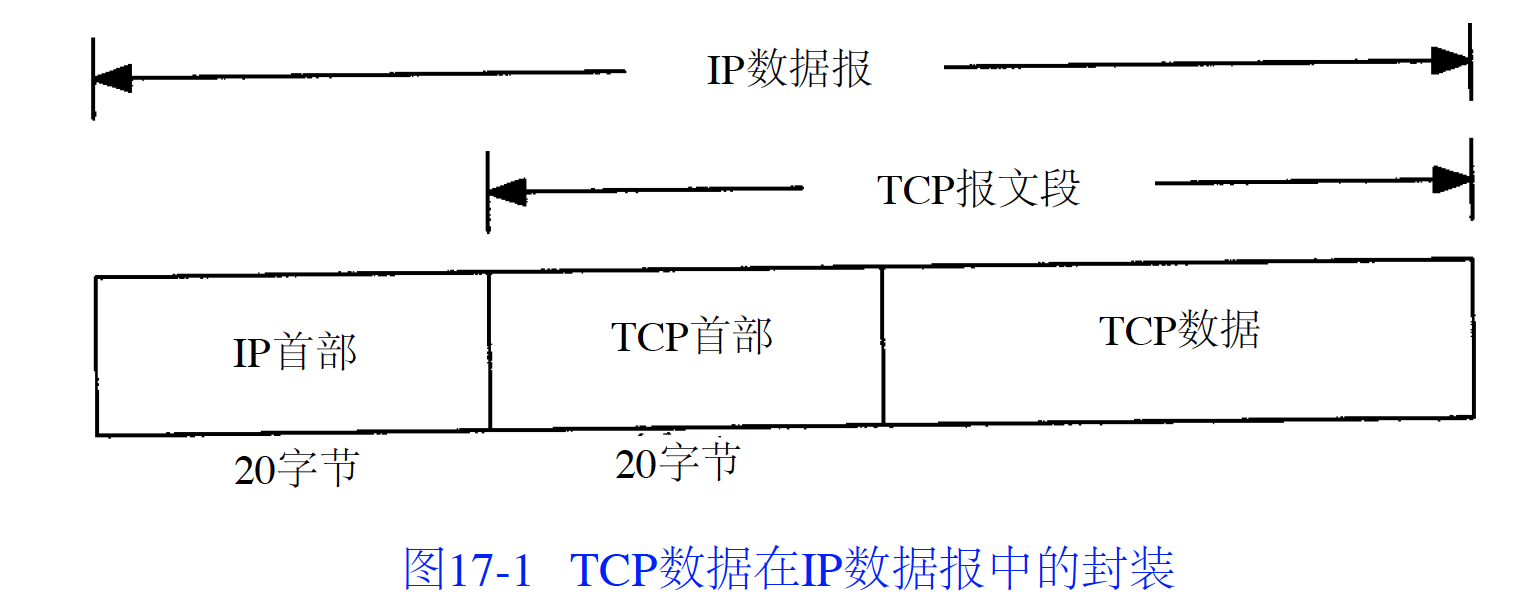
Checksum method is adding 16bits, could not identify swap 16 bits’ errors





TCP addition:

1. data are split to many optimal segment send to another end.
2. After send a segment, sender will start a timer to wait receiver get the segment, timer is out of range, the segment will be sent again.
3. If the segment has been checked error, receiver will drop the segment.
4. Recevicer tcp will resort all segments and then hand to application layer.
5. Receiver tcp will drop all repeat data.
6. TCP flow control
7. TCP don’t know what are the data, application layer explain the data.

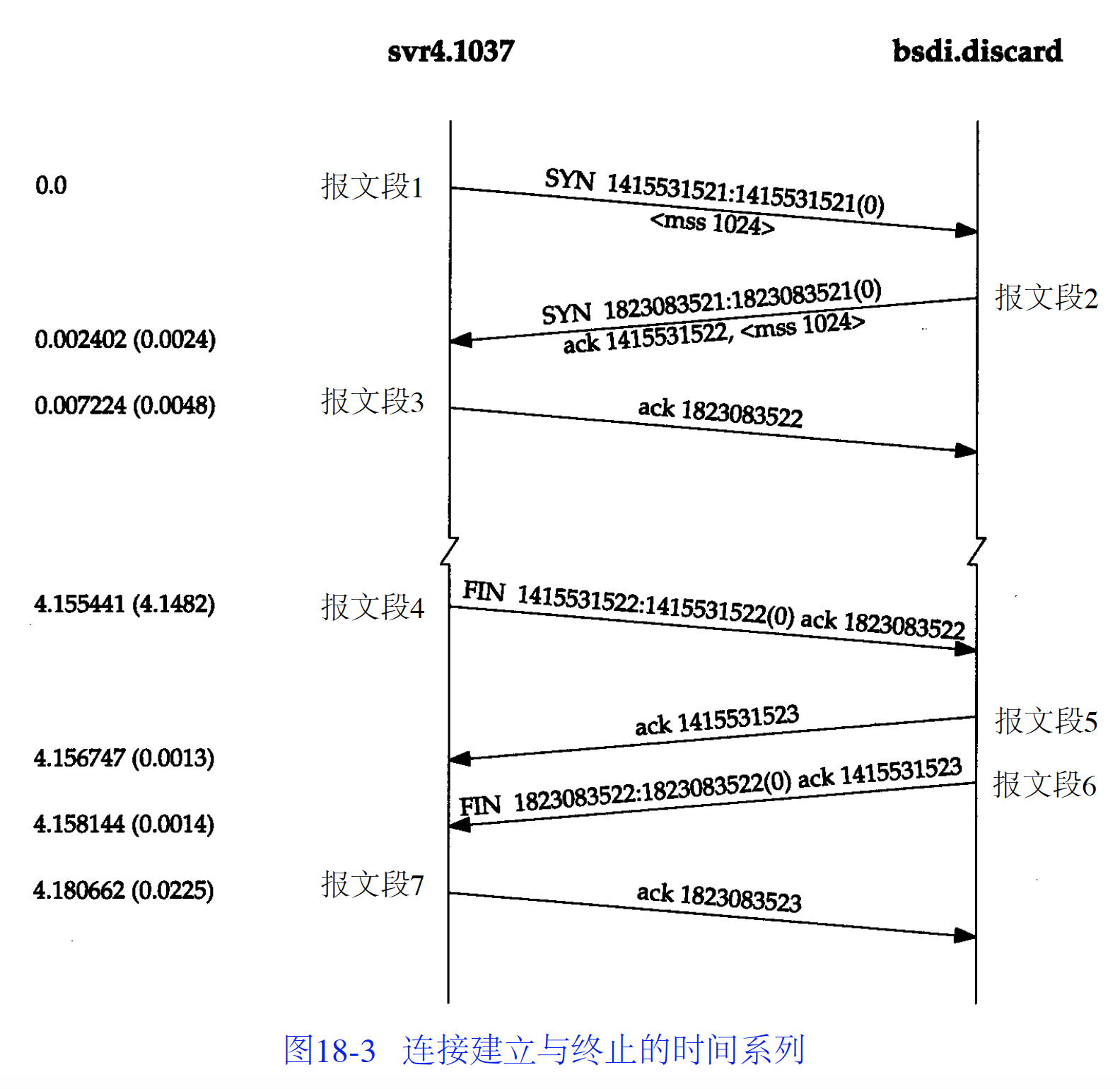




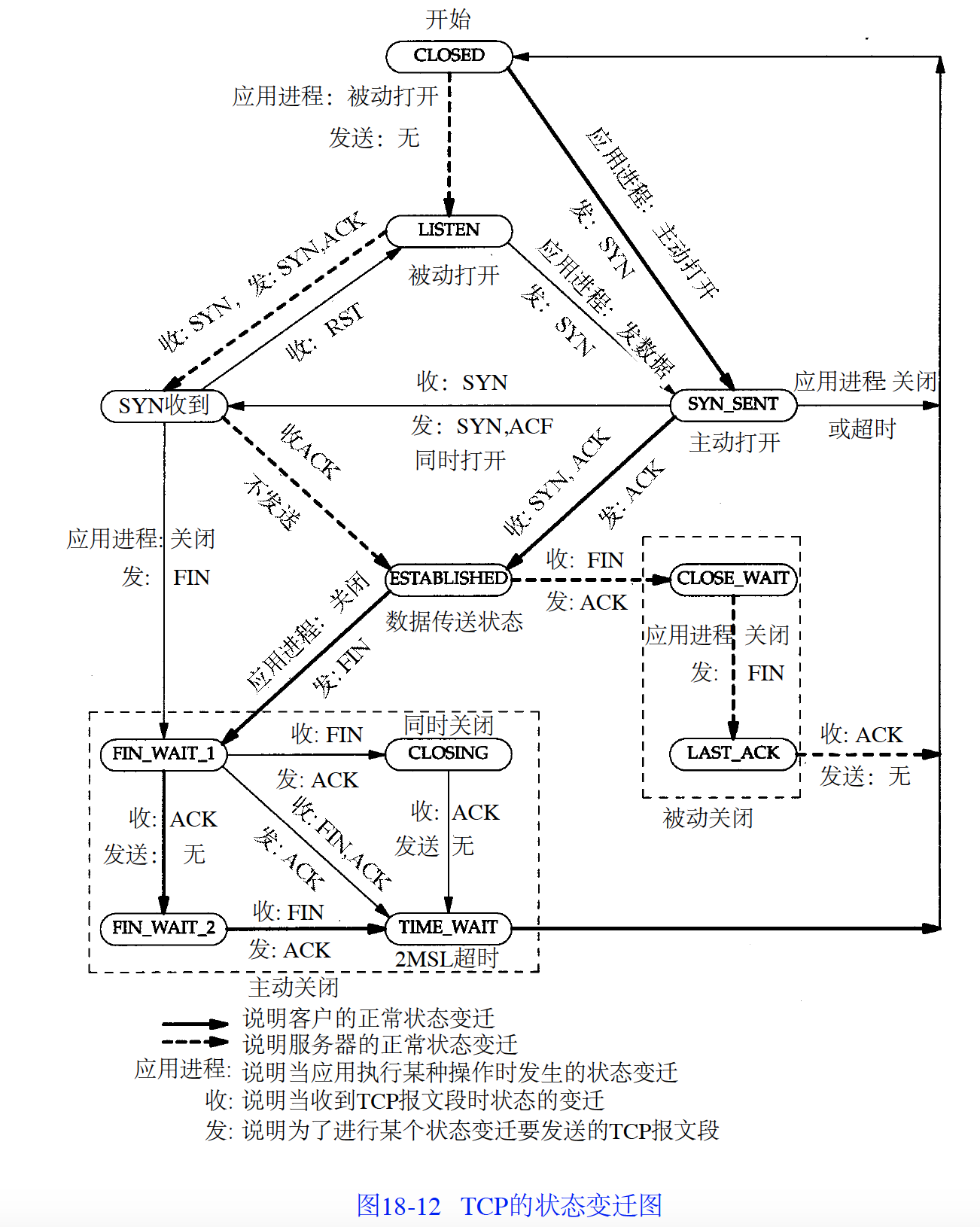
TCP provide two directions data transport

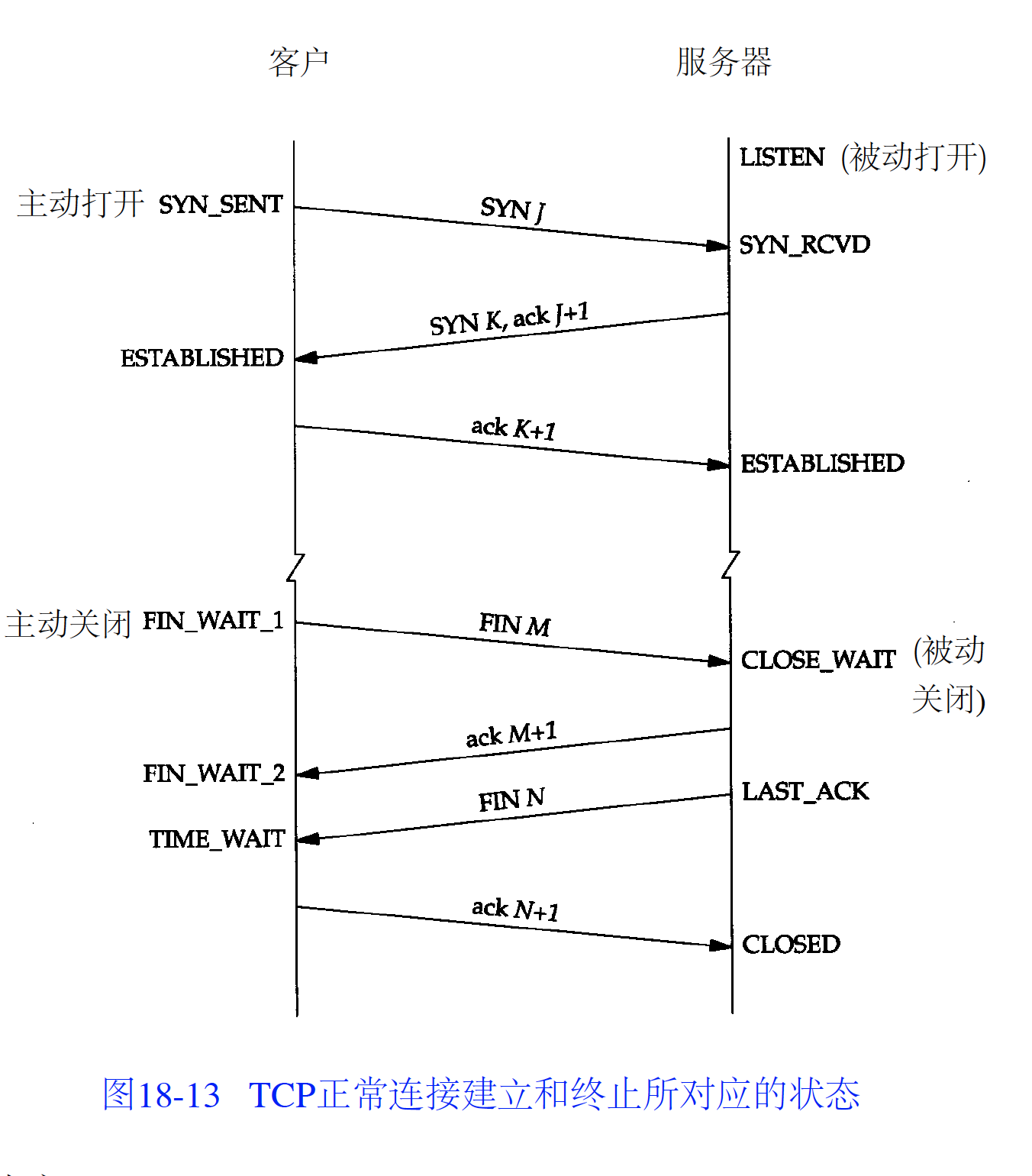
Flag bits:

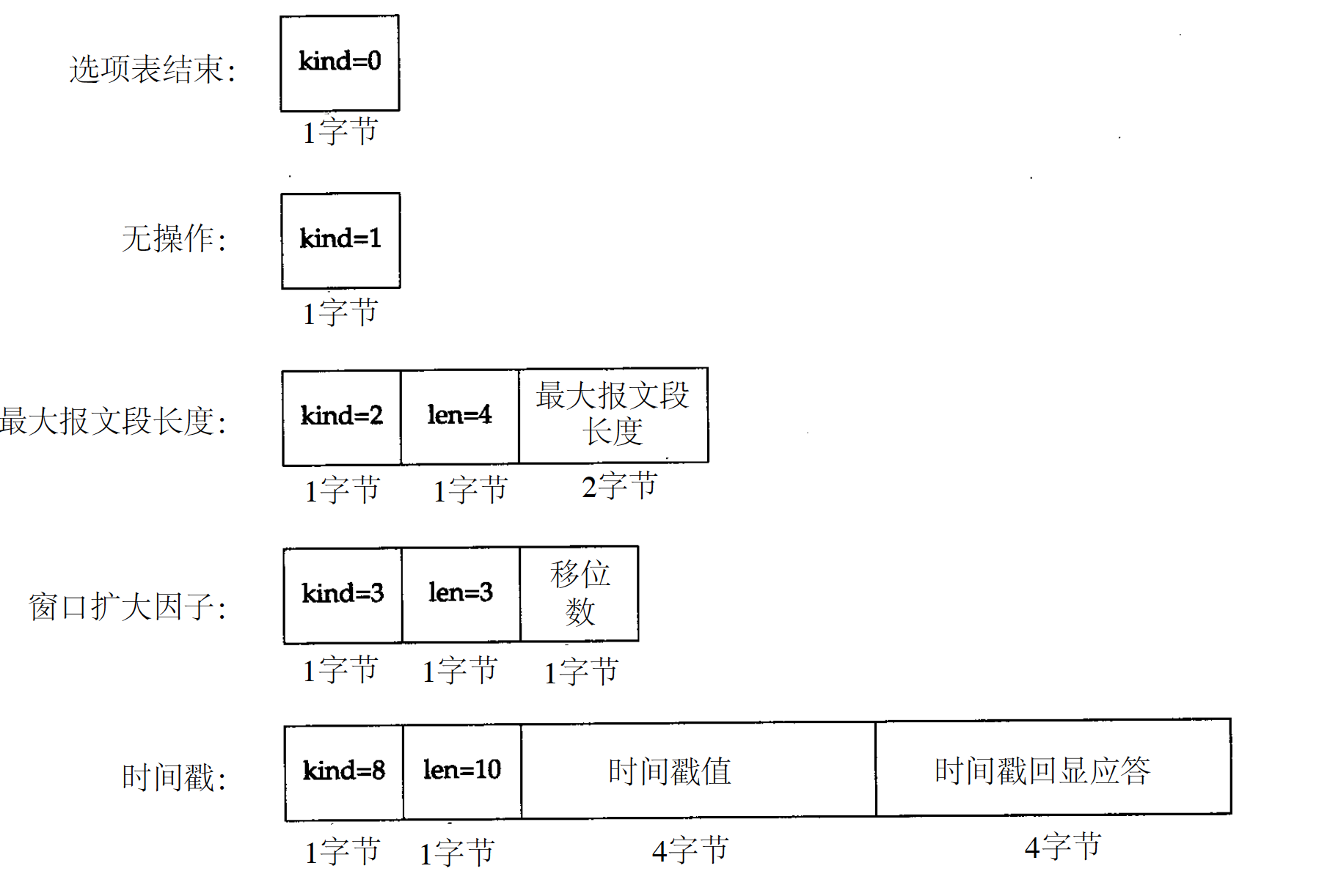
1. URG: urgent pointer
2. ACK: acknowledge serial confirmed
3. PSH: receiver should send the segment to application layer as soon as possible
4. RST: reconnect
5. SYN: invoke a connection
6. FIN: sender finish the task



For Ethernet, MSS is 1460 bytes, for IEEE802.3, MSS is 1452bytes.

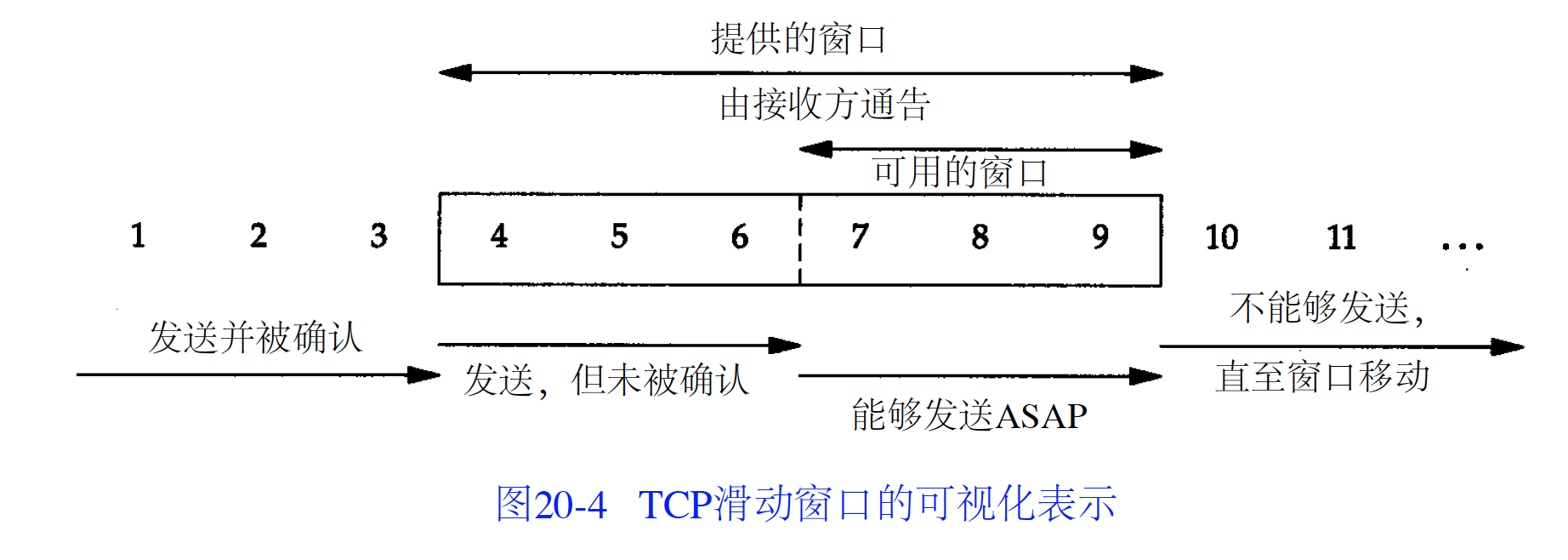




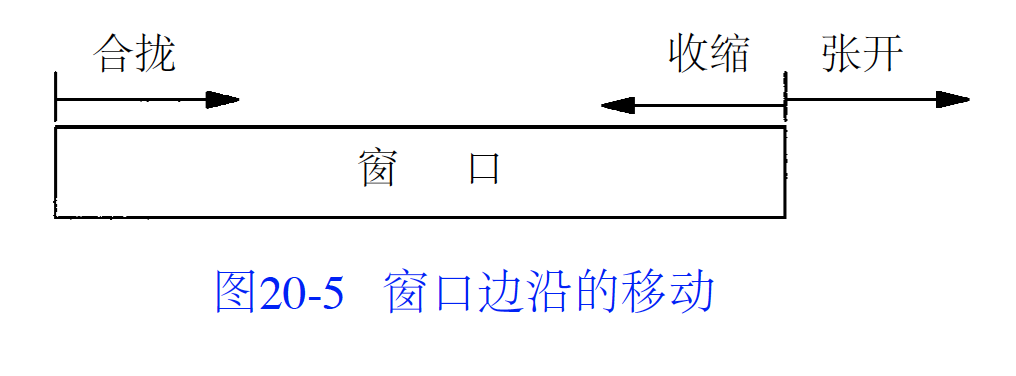


2. Explain sliding window protocol.

In this protocol, multiple packets are sent and are acknowledged using a single acknowledgment frame. Both sender and receiver maintain record of the following: a) Frames which are sent and acknowledged, are placed at left of the window b) Frames which are sent but not acknowledged, are placed in the middle of the window c) Frames which are yet to be sent, are placed at the right of the window Window announcements are sent by the receiver to the sender to acknowledge receipt of frame as well as current size of the buffer. If the buffer size is zero then sender should wait for an acknowledgement from the receiver.

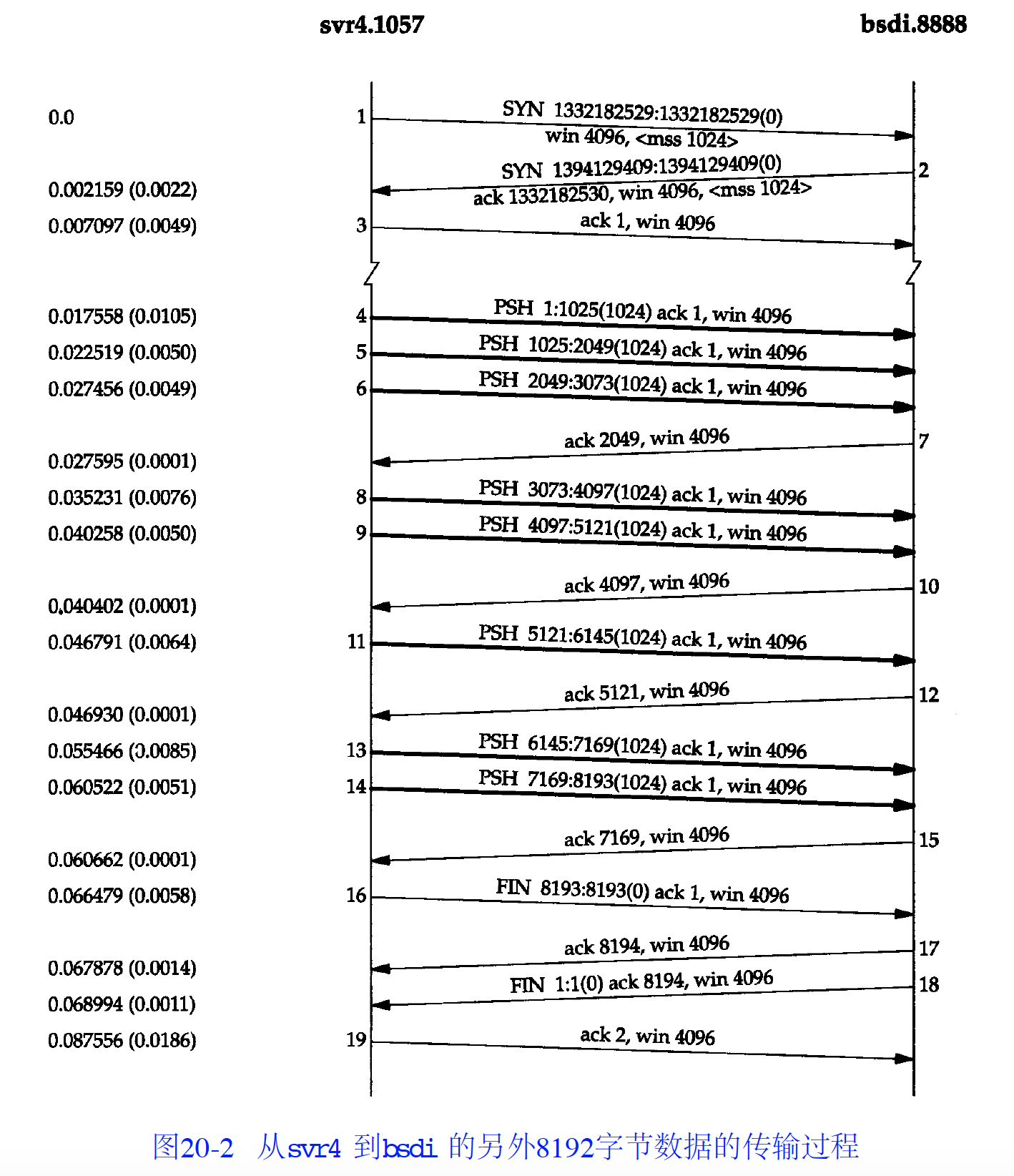


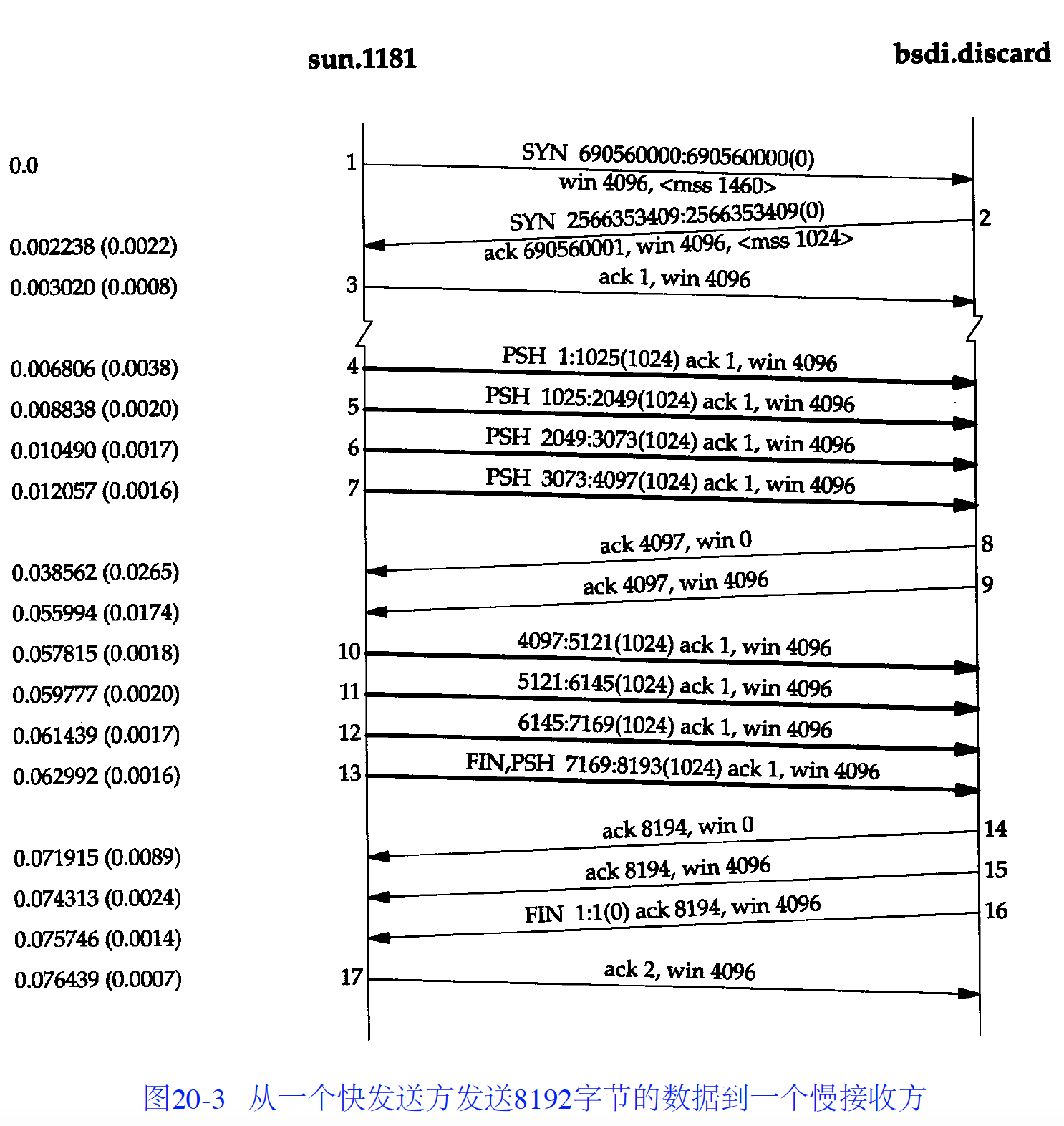
window sliding:

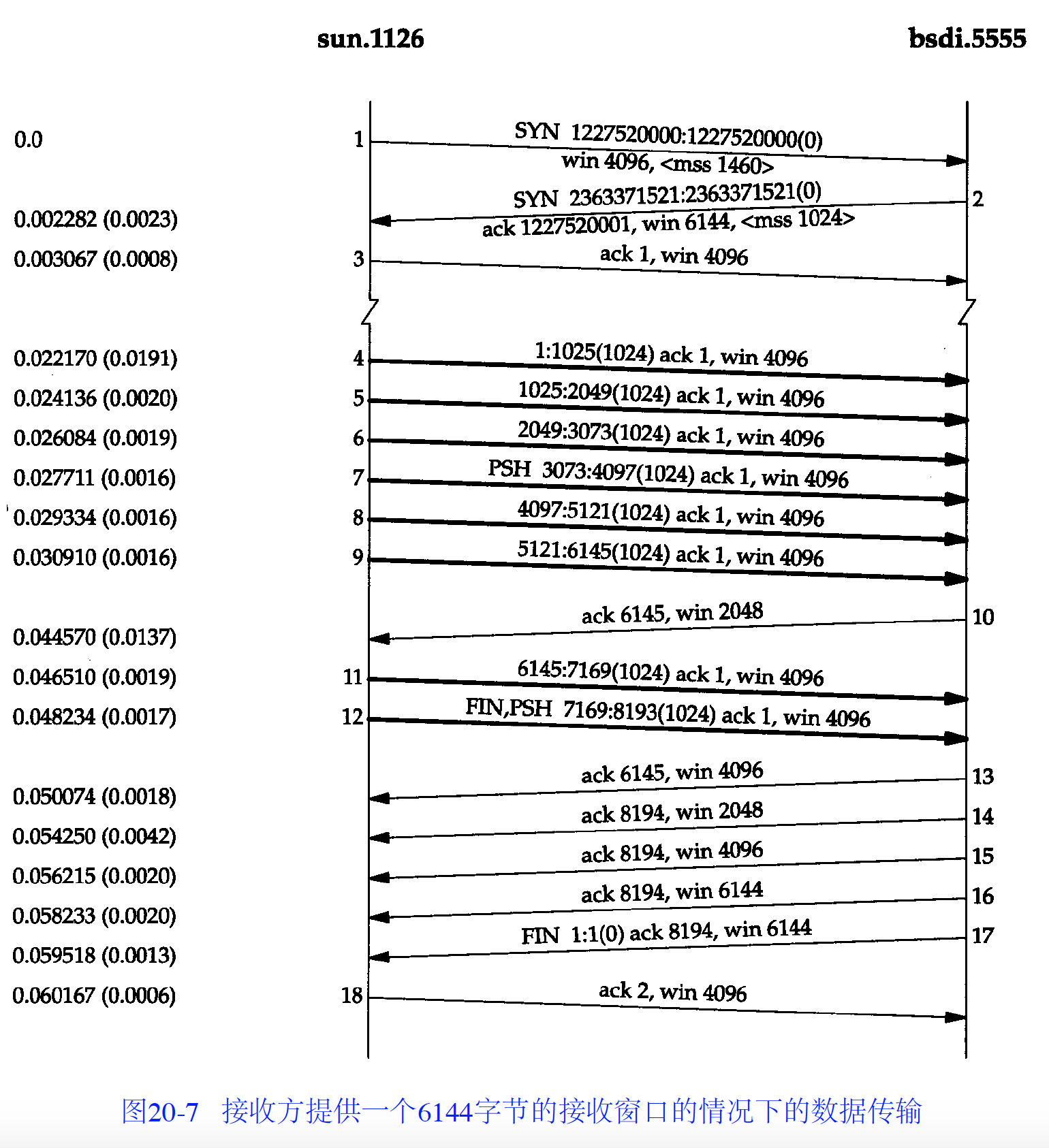


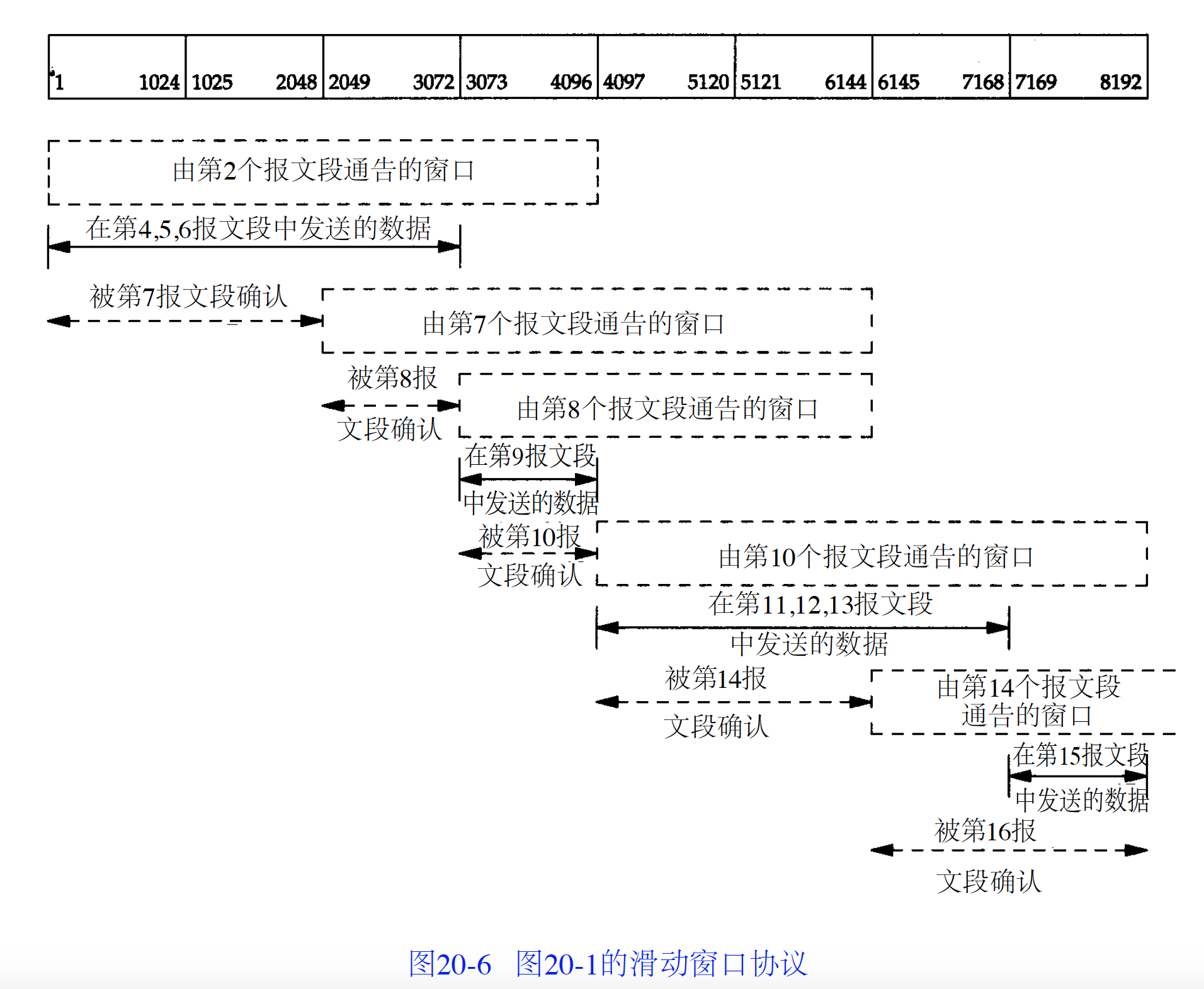
Window movement:

1. Window left side move to right side. Happens when data are sent and acknowledged.
2. Window right side move to right, allows more data to be sent. Happens when receiver process has read the data and release TCP cache memory.
3. Window right side move to left.
4. If receive a packet indicate window left side move to left, it will be thought as a repeat ACK and drop it.
5. If left side reach right side, it is a zero window, sender could not send any more data.









Conclusion:

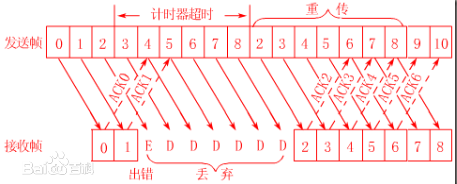
1. Sender don’t need to send a full window size data.
2. Window move to right side, window size determined by acknowledge serial.
3. Window size could reduce, but right side will not move to left.
4. Receiver dot need to send ACK until window is full.
5. Window size is provided by receiver and it could be managed by receive process.

3: Explain 1-bit sliding window protocol.

In this protocol, size of the window is 1 and it is like stop-and-wait protocol where sender should wait for the acknowledgement before sending the next frame. Therefore, there can be a maximum 1 outstanding frame present in the window at any time. This protocol is considered as inefficient because sender must wait for a round trip time before it can transmit the next frame.

4: What is go back N protocol?

In this protocol, receiver does not maintain a buffer and whenever it receives the frame, it sends an acknowledgement back to sender. If it receives a frame which is out of order then it discards it and all the following frames until it receives the missing frame.



5: Explain selective repeat protocol.

In this protocol, receiver maintains a buffer equal to the size of the window for storing out-of-order frames. Therefore, it does not discard all the frames following a missing frame but keeps them in buffer in a sequential manner and sends their acknowledgement to the sender. It does not pass these out-of-order frames to the network layer until it receives the missing frame.

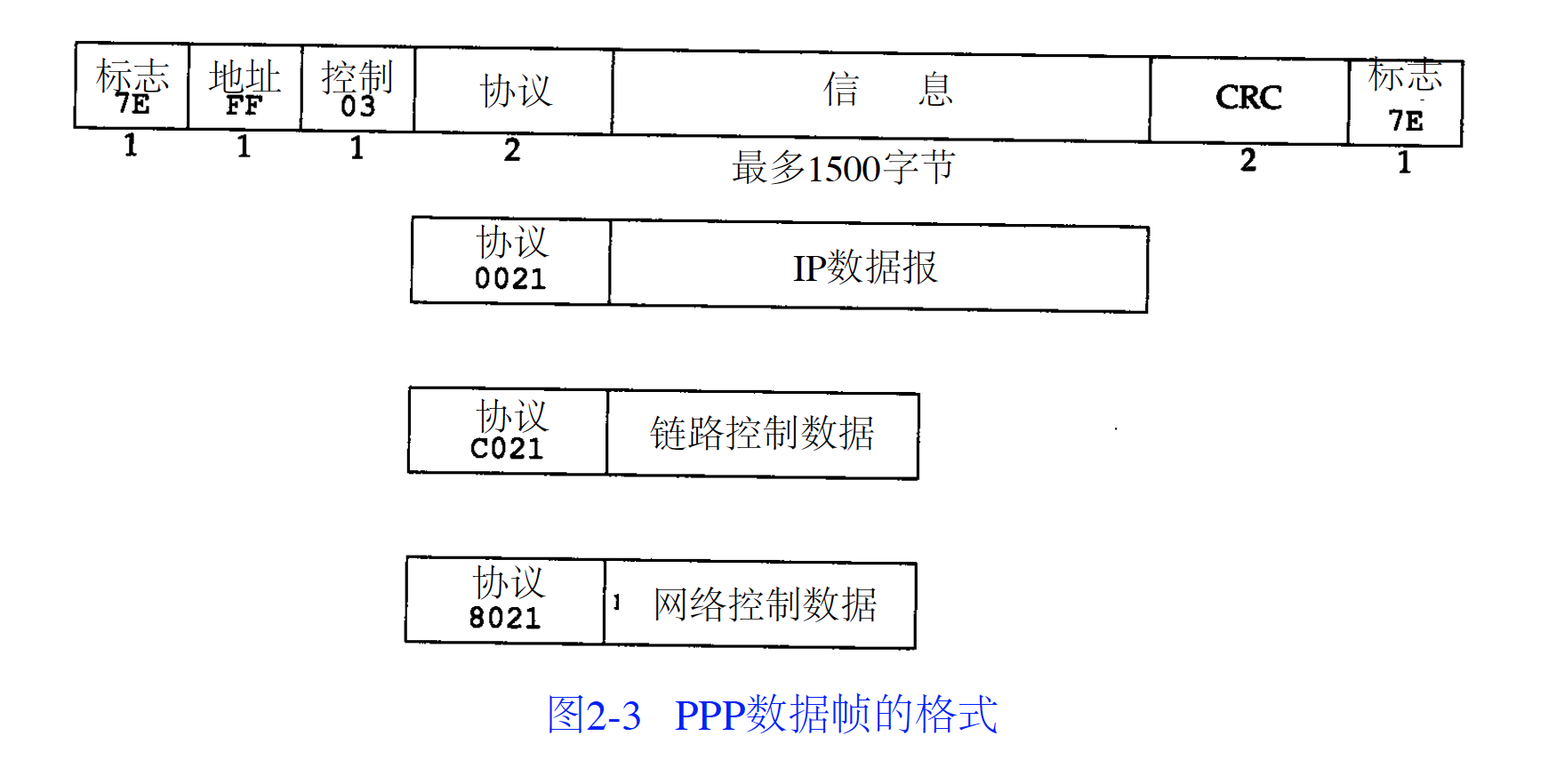
6: What is point-to-point protocol?

Point-to-point protocol is used in the internet to carry traffic among routers and between a user and Internet Service Provider (ISP). It is responsible for error-detection, negotiating IP addresses, performing authentication, supporting other protocols etc. It has the following features:

a) It uses a framing technique which flawlessly specifies end of the current frame and start of the next frame.

b) It employs a protocol known as Link Control protocol to bring a line up, test a line, negotiate options, and put a line down.

c) It uses different Network Control Protocol for different network layers supported so that options in network layer can be negotiated in an independent way.



7: What is CSMA/ CD protocol?

The CSMA/ CD (Carrier Sense Multiple Access with Collision Detection) protocol requires that a station should abort the transmission of a frame as soon as it detects a collision. In this protocol, when two machines begin transmission simultaneously, both will detect a collision and will abort the further transmission of the current frame immediately because current frames are already garbled and cannot be recovered. This technique saves time, bandwidth and is widely used on LANs.

8: What is Logical Link Control (LLC) Protocol?

This protocol is used in Logical Link Control layer which is a sub-layer on the top of MAC layer in the data link layer. It hides the differences of all 802 networks and makes them indistinguishable to the network layer by providing a common interface to the network layer. It provides three types of services to the network layer:

a) Unreliable datagram service

b) Acknowledged datagram service

c) Reliable connection-oriented service

9: What are the different types of transmission techniques?

a) Broadcasting: In broadcasting technique, all machines on the network are connected to a common communication channel. A message sent from one machine is received by all other machines. If a machine wants to send a message to a particular machine on the network, the source machine describes the address of the recipient in the address field of the message and sends the message over the communication channel. Upon receipt, all machines check the address field and if that machine is the intended recipient, it processes the message otherwise it ignores the message. Also, a machine can address all other machines on the network as intended recipient by using a special code in the address field of the message. Broadcast networks such as Local Area Networks are used in small geographic areas.

b) Point-to-point: In point-to-point technique, many connections exist between any two machines. To go from a source to a destination, a message may take one of the several possible paths. Therefore there is a need to find the best route between an individual pair of machines. Point-to-point networks such as Wide Area Networks are used in large geographic areas.

General

1: What is a client-server model?

A client-server model involves two machines called client and server which communicate with each other over the network. Initially, client sends a request over the network to the server and waits for the reply from the server. When server receives the request, it processes the request and sends the response back to the client.

2: What is peer to peer network?

In peer-to-peer system, a computer can connect and communicate with one or more other computers directly. The concept of client and server does not exist in peer-to-peer network.

3: What is the difference between LAN, MAN and WAN?

LAN (Local Area Network): A LAN is used in smaller geographic regions such as a room, a building or a campus and typically LANs operate at 10Mbps- 100Mbps.

MAN (Metropolitan Area Network): A MAN typically spans across a city.

WAN (Wide Area Network): WANs are used across large geographic areas such as a country or a continent. The speed of a WAN is between 1Mbps to 150Mbps. An example of WAN is Internet.

4: What is a network topology?

The word “topology” or “network topology” is used to refer to the shape in which various machines are connected together to form a network. There are following types of topologies possible for a Local Area Network:

1. Tree: In this topology, a machine called a “root node” (at level 1 of hierarchy) is connected to one or more other machines (at level 2 of hierarchy) which in turn are connected to one or more other machines (at level 3 of hierarchy) and so on.



1. Mesh: In this topology, all machines are directly connected to each other.



1. Star: In this topology, all machines are connected through a central common hub.



1. Bus: In this topology, all machines are connected to a single cable called a bus. e) Ring: In this topology, all machines are connected in circular manner and data flows in only one direction.



5: What is the difference between connection oriented and connectionless service?

In a connection-oriented service, when messages should be sent from a source machine to a destination machine, the source machine establishes connection with the destination machine, transmits the messages to the destination machine and when the transmission of messages is over, the connection is terminated by the source machine. Parameters such as size of the message, quality of service etc are decided by source machine, destination machine and the carrier (subnet).

In connectionless service, when a message should be sent from source machine to destination machine, a physical connection is not made; instead the source machine writes the address of the destination in the message and sends the message over the network. The message passes through multiple intermediate machines and finally reaches the destination.

6: What is the responsibility of data link layer?

The main responsibility of data link layer is to transfer error free data from source machine to destination machine. It breaks the incoming data into small units called frames and sends the frames sequentially to the destination. This layer deals with two main issues:

a) Flow control: This layer implements a flow control scheme which informs the sender about the buffer space of the receiver so that the sender can adjust the rate at which it is sending data to the receiver.

b) Error control: This layer calculates checksum i.e. number of bits present in a frame, adds the checksum to each outgoing frame and re-computes the checksum at the receiver side to ensure that transferred data is error free.

7: What is the responsibility of network layer?

Network layer determines how a packet (a unit of data) is routed from source to destination. A route can either be static or dynamic. In static routing, a table containing multiple routes is wired into the network. In dynamic routing, a route is determined at the beginning of a connection. Network layer handles issues such as network congestion, quality of service i.e. delay, transmit time etc. When packets are transmitted between two heterogeneous networks that use different address formats then the network layer is responsible for converting one address format to another address format. If the packet size of two heterogeneous networks is different then the packet may be discarded by the layer because it may be too large or short for another type of network.

8: What is the responsibility of transport layer?

Transport layer receives the data from session layer, breaks it into smaller pieces and passes it to the network layer. It ensures that the data which has been sent is received correctly at the receiver side. Transport layer provides three types of service to the session layer:

a) Connection-oriented: It delivers the packets in the same order in which they were sent.

b) Connection-less: It delivers the packets without guarantee about the order of delivery.

c) Broadcasting: It delivers the packets to multiple destinations. The type of service used is determined at the beginning of the communication between a sender and a receiver.

9: What is the responsibility of application layer?

Application layer contains following protocols for different types of applications to be used by users:

a) HTTP (Hyper Text Transfer Protocol): HTTP protocol is used by browser to send a request to server for a particular web page. When server receives the request, it returns the web page to the browser.

b) FTP (File Transfer Protocol): Through FTP protocol, users can transfer files from one machine to another machine on the network.

c) SMTP (Simple Mail Transfer Protocol): SMTP is used for sending and receiving electronic mails.

d) TELNET: TELNET allows users to log onto a different machine on which the user already has an account.

e) NNTP (Network News Transfer Protocol): NNTP is used to transfer USENET news articles over the network.

f) DNS (Domain Name System): DNS is used to map host names to network addresses.

10: What is the difference between multiplexing and demultiplexing?

Multiplexing is a process in which multiple signals are combined and are sent to the destination over a single shared communication channel. The device which performs this operation is known as multiplexer.

Demultiplexing is a reverse process in which individual signal is extracted from the combined signal and is sent to each individual receiver. The device which performs this operation is known as demultiplexer.

11: What is bandwidth?

Bandwidth: It is the difference between maximum frequency and minimum frequency in a channel. It is represented in bps.

12: How does data link layer detect error in data transmission?

The data link layer receives packets from the network layer, breaks the packets into frames, computes the checksum, adds the checksum to each frame and then transmits the frames. At the destination, checksum is re-computed. If new checksum is different from previous checksum then the frame is discarded and an error report is sent back to the sender.

13: How error is controlled by data link layer?

The data link layer ensures that a frame arrives correctly and exactly once at the destination. This is done by sending an acknowledgement back to the sender for each received frame and using sequence numbers for frames to be transmitted. The sender transmits the frame, starts a timer and waits for acknowledgement. If the frame or acknowledgement is lost then timer goes off and frame is retransmitted again. Therefore, a frame may be sent more than once. To solve this problem, sequence numbers are used by which a receiver can distinguish between two same frames.

14: What is flow control and how it is handled?

Flow control is a process of controlling the rate at which sender is transmitting frames to the destination. It is required because a slow receiver will not be able to handle packets arriving too fast from the sender. Flow control techniques are of two types:

a) Feedback based flow control: A receiver sends the information about its situation so that sender could adjust the transmission rate of the frames.

b) Rate-based flow control: A protocol is used to limit the transmission rate of the frames. Data link layer does not use rate-based flow control.

15: What are the components of a frame?

A frame has two components: header and info. The header is used for carrying control information and contains three fields:

a) kind: It is used to distinguish a control frame from a data frame

b) seq: It is used for keeping sequence number

c) ack: It is used for acknowledgement purposes The data is carried in the form of packet in info field of the frame.

16: What is the relationship between a frame and a packet?

When the network layer receives a message from the transport layer, it adds the network layer header to the message. The resulting unit is known as a packet which is passed to the data link layer.

When the data link layer receives the packet, it encapsulates the packet in “info” field of an envelope known as a frame and forwards the frame to the destination. At the receiver’s side, the data link layer extracts the packet from the frame and passes it to the network layer.

17: What is Medium Access Control layer?

The MAC layer is a sub layer of the data link layer which determines who should transmit next when there is a competition among machines for transmission on a multi-access channel. This layer has much significance in LANs because many LANs use multi-access channel for communication medium.

18: What do you mean by a collision?

It is an event which may occur when two frames are transmitted over a multi-access channel simultaneously. If two frames collide with each other it results in a garbled signal. This signal is detected by all the machines over the channel and the collided frame is retransmitted again.

19: What is the difference between multicasting and broadcasting?

When a frame is sent to a group address, it is delivered to all the machines which belong to that group. Multicasting is a technique of sending frames to all the stations in a group and it requires group management.

On the other hand, broadcasting is a technique in which a frame is sent to all the machines on the Ethernet. A broadcasting address consists of all the 1s and is a reserved address. Broadcasting does not require group management.

Only used in UDP

20: What is the difference between local and global address?

Local addresses are used by network administrators to assign them to machines on a network. Local addresses are not known outside the network in which they are assigned.

Global addresses are assigned by IEEE to uniquely identify a machine anywhere in the world and no two machines can have the same global address. A global address uses 46 bits and therefore 7 × 1013 machines can be assigned a unique global address.

21: What is a switch?

All stations on the Ethernet are connected to a central common hub called switch. The stations use twisted pair (10Base-T) cable to connect to the central hub. A switch consists of 4-32 plug-in cards where each card has up to 8 connectors and a high-speed backplane. Therefore when a station transmits a frame, it is sent to the switch where a plug-in card receives it and determines if this frame is destined for one of its connectors. If this is the case, then it forwards the frame to that connector and if not, then it is forwarded to another destination station’s card through high-speed backplane.

22: What is a bridge?

A bridge is a device which is used to connect two LANs together. A bridge works at data link layer and transports the frames based on their data link layer address. As a bridge does not examine the data in the frames, it can be used to forward different types of traffics such as IPv4, IPv6, AppleTalk, ATM and other packets.

Algorithm

1: What is shortest path routing algorithm?

Shortest path routing algorithm finds the shortest possible path among many possible paths that may exist between a source and a destination. In shortest path routing, a subnet is represented as a graph, routers are represented as nodes of the graph, and transmission lines are represented as arcs of the graph. Each node is labeled with a best-known path from the source. The metric used to represent path length can be number of hops, distance or transmission delay.

2: How does a shortest path routing algorithm work?

If a shortest path is to be found between two nodes in a graph then it follows the following steps:

a) Set the initial node to be current node.

b) Examine each neighboring nodes of current node by marking them with a tentative distance from current node. If this tentative distance is less than previously marked tentative distance then it overwrites that distance.

c) Set a neighboring node as current node which has least tentative distance from previously denoted “current node”.

d) Mark previously denoted “current node” as visited. e) Go to step b.

3: What is a distance vector routing algorithm?

In distance vector routing, each router in the subnet maintains a table for all other routers in the subnet. The table consists of two entries: distance or delay to the router and preferred line to be used to reach the router. After every short time interval, a router sends information to its neighbors about its delay to other routers. A router receives the same information from each of its neighbors. Once a router receives tables from all its neighbors, it examines the delay to every other router through each of its neighbors and uses the line which has lowest delay to another router. In this way, all routers update their routing table.

Top Brief Interview Questions

1: What are the layers of the TCP/IP reference model?

Application Layer, Transport Layer, Network Layer, Data-Link Layer



2: What is backbone network?

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles management of bandwidth and various channels.

3: What is a LAN?

LAN is short for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.

4: What is a node?

A node refers to a point or joint where a connection takes place. It can be computer or device that is part of a network. Two or more nodes are needed to form a network connection.

5: What are routers?

Routers can connect two or more network segments. These are intelligent network devices that store information in its routing table such as paths, hops and bottlenecks. With this info, they can determine the best path for data transfer. Routers operate at the OSI Network Layer.

6: What is point to point link?

It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.

7: What is anonymous FTP?

Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead log in as an anonymous guest.

8: What is subnet mask?

A subnet mask is combined with an IP address to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

9: What is VPN?

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

10: Briefly describe NAT.

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share single connection to the Internet.

11: What is RIP?

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

12: What is WAN?

WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are in different regions and countries.

13: What are proxy servers and how do they protect computer networks?

Proxy servers primarily prevent external users who identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.

14: What is a private IP address?

Private IP addresses are assigned for use on intranets. These addresses are used for internal networks and are not routable on external public networks. These ensures that no conflicts are present among internal networks while at the same time the same range of private IP addresses are reusable for multiple intranets since they do not “see” each other.

15: What is DoS?

DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the internet or any other network services. Such attacks may come in different forms and are done by a group of perpetuators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.

16: What are MAC addresses?

MAC, or Media Access Control, uniquely identifies a device on the network. It is also known as physical address or Ethernet address. A MAC address is made up of 6-byte parts.

17: What is the main purpose of OSPF?

OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

18: What are gateways?

Gateways provide connectivity between two or more network segments. It is usually a computer that runs the gateway software and provides translation services. This translation is a key in allowing different systems to communicate on the network.

19: What is SLIP?

SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

20: Give some examples of private network addresses.

10.0.0.0 with a subnet mask of 255.0.0.0  
172.16.0.0 with subnet mask of 255.240.0.0  
192.168.0.0 with subnet mask of 255.255.0.0

21: What is DHCP?

DHCP is short for Dynamic Host Configuration Protocol. Its main task is to automatically assign an IP address to devices across the network. It first checks for the next available address not yet taken by any device, then assigns this to a network device.

22: What is the main job of the ARP?

The main task of ARP or Address Resolution Protocol is to map a known IP address to a MAC layer address.

23: What is TCP/IP?

TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as heterogeneous network.

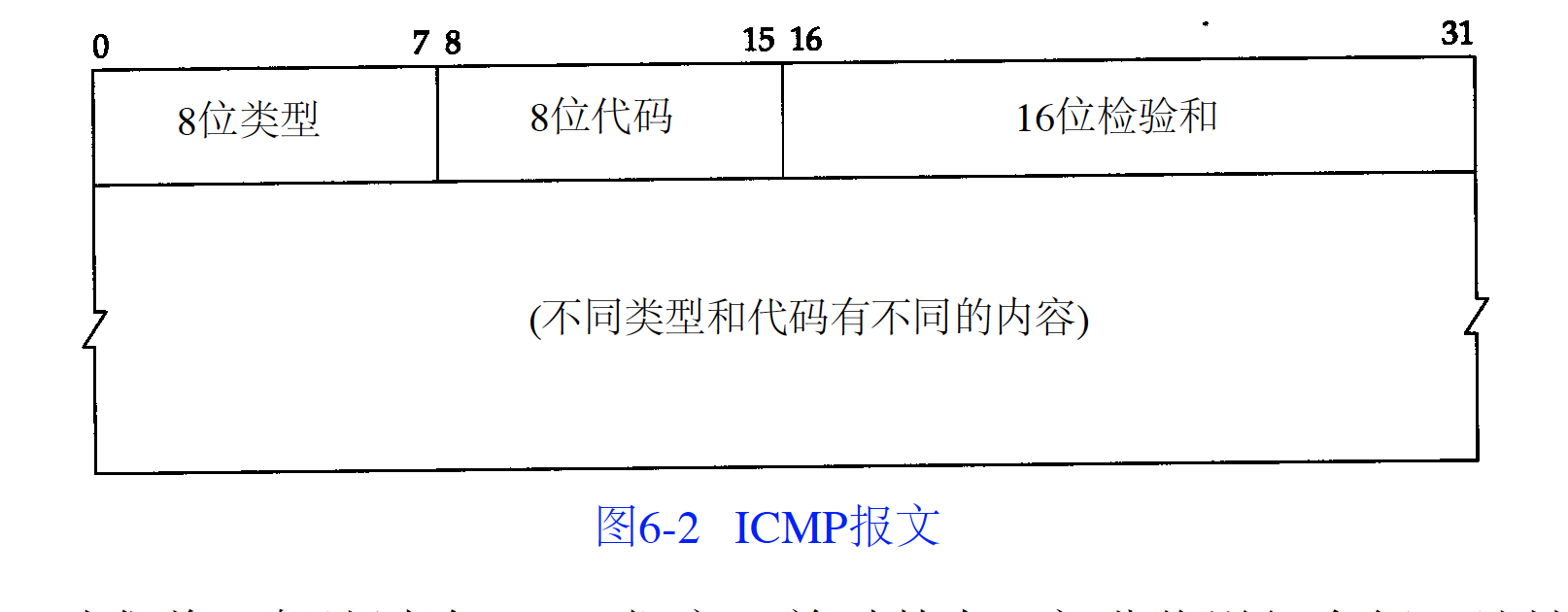
24: What is the use of a default gateway?

Default gateways provide means for the local networks to connect to the external network. The default gateway for connecting to the external network is usually the address of the external router port.

25: What is ICMP?

ICMP is Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING.

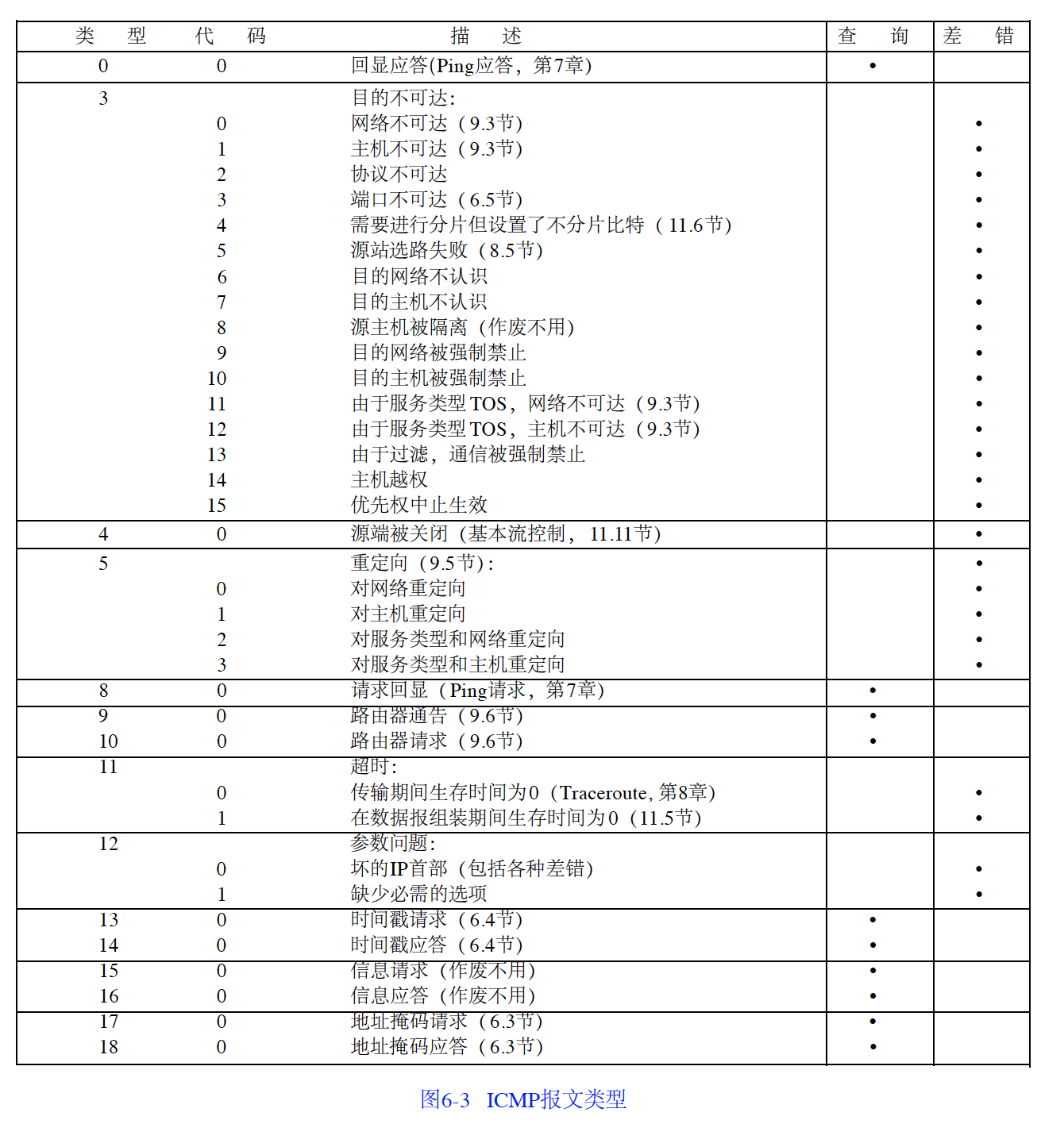


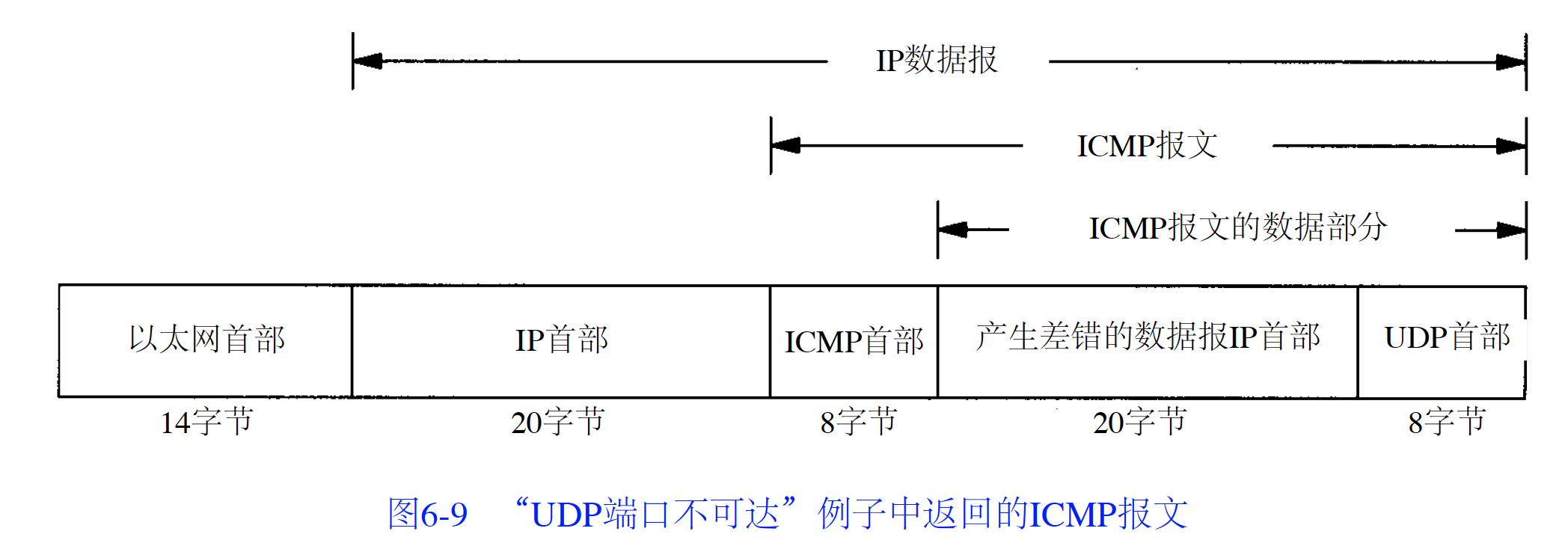


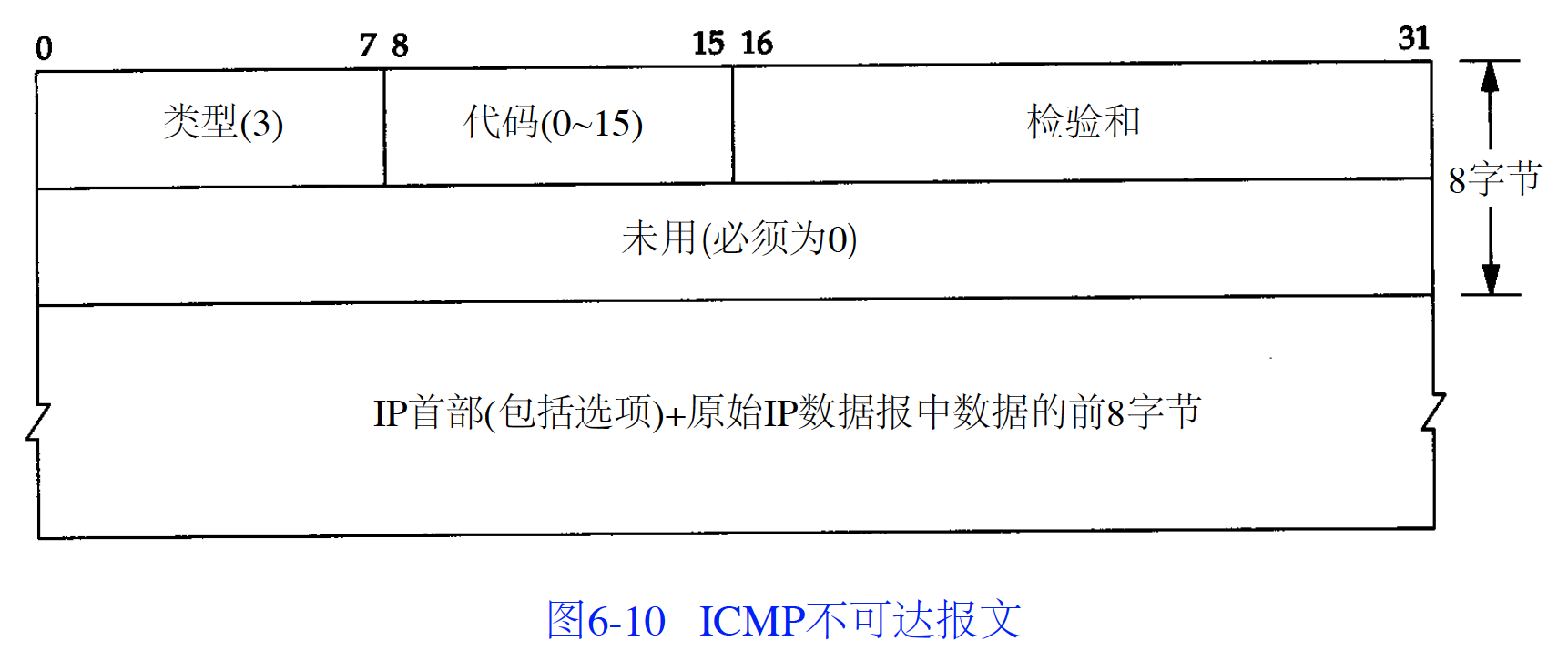
checksum include header and data, it is mandatory

flowing situations will not lead ICMP error gram:

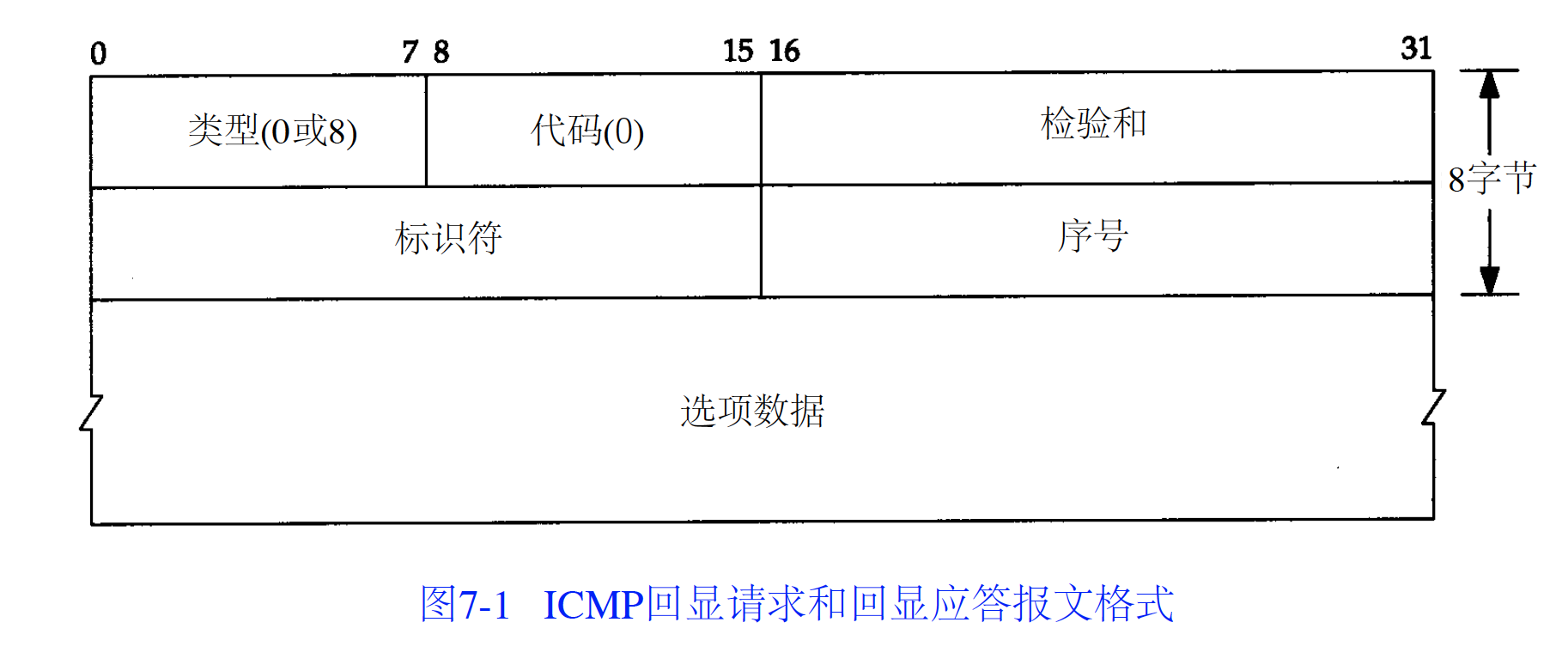
1. ICMP error gram (ICMP lookup gram maybe)
2. Destination address is multicast or broadcast address
3. Data link layer broadcast datagram
4. Source address is not zero, localback, broadcast or multicast address











26: What is Ping?

Ping is a utility program that allows you to check connectivity between network devices on the network. You can ping a device by using its IP address or device name, such as a computer name.

27: What is peer to peer?

Peer to peer are networks that does not reply on a server. All PCs on this network act as individual workstations.

28: What is DNS?

DNS is Domain Name System. The main function of this network service is to provide host names to TCP/IP address resolution.

Steps:

1. Require information in the local DNS cache, if don’t find the answer then do DNS query
2. Ask the recursive DNS servers
3. Ask the root nameservers
4. Ask the TLD nameservers
5. Ask the authoritative DNS servers where store DNS specific records
6. Recursive server retrieve the record and store in its local cache
7. Receive the answer and store in its cache

29: What is ipconfig?

Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

30: What is client/server?

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refers to workstation that access the server.

31: Describe Ethernet.

Ethernet is one of the popular networking technologies used these days. It was developed during the early 1970s and is based on specifications as stated in the IEEE. Ethernet is used in local area networks.

32: What is SMTP?

SMTP is short for Simple Mail Transfer Protocol. This protocol deals with all Internal mail, and provides the necessary mail delivery services on the TCP/IP protocol stack.

33: What is Protocol?  
A protocol is a set of rules that govern all aspects of information communication.

34: What is Piggy Backing?  
A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

35: Define cyclic redundancy check (CRC).  
C RC appends a sequence of redundant bits derived from binary division to the data unit. The divisor in the CRC generator is often represented as an algebraic polynomial.

36: What do you mean by ALOHA?  
It is the method used to solve the channel allocation problem. It is used for:  
i) ground based radio broadcasting  
ii) In a network in which uncoordinated users are competing for the use of single channel.  
It is of two types:  
1. Pure aloha  
2. Slotted aloha

37: What is mesh network?  
A network in which there are multiple network links between computers to provide multiple paths for data to travel.

38: What is the NIC?

NIC stands for Network Interface Card. NIC is the device which connects computer with network.

39: Which are the different factors that affect the security of a network?

There are mainly two security affecting factors:

1. Unauthorized Access
2. Viruses

40: What is a gateway? Is there any difference between gateway and router?

A node that is connected to two or more networks is commonly known as gateway. It is also known as router. It is used to forward messages from one network to another.

41: What is POP3?

POP3 stands for Post Office Protocol version3. POP is responsible for accessing the mail service on a client machine. POP3 works on two models such as Delete mode and Keep mode.

42: What is RAID?

RAID is a method to provide Fault Tolerance by using multiple Hard Disc Drives.

43: What is RSA Algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is mostly used for public key encryption.

Interview Test Questions

1: a no-disk work station applies IP address to server, use RARP protocol

2: RFC is IETF community’s work document

3: standard Ethernet uses 10 BASE-T

4: 3.255.255.255 is a direct broadcast address

5: limited broadcast packets don’t include itself IP address, direct broadcast address include it

6: explain ARP work principle

7: explain 10BASE-T

8: explain FDDI

9: explain token loop

10: explain CSMA/CD

11: explain OSPF

12: explain VLAN