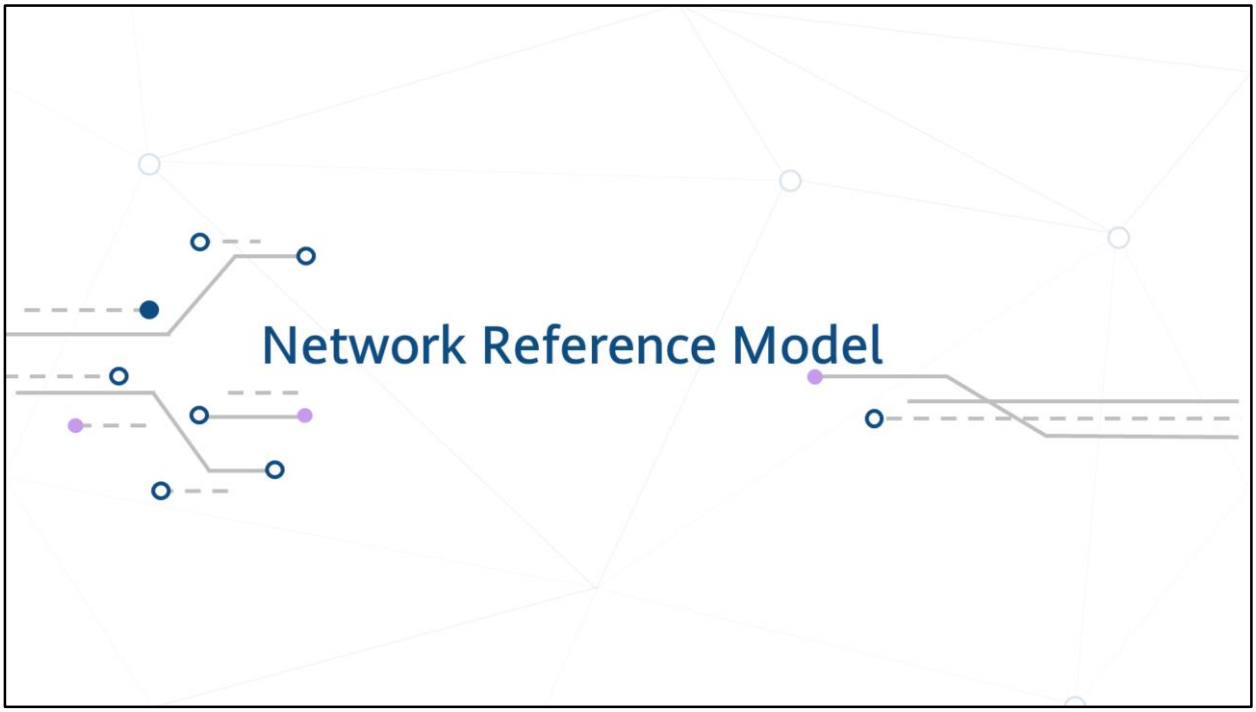

Network Reference Model

Foreword

- In the digital era, various information is presented as data in our life. What is data? How is data transmitted?
- In this course, we will use the network reference model to understand the "life" of data.

Objectives

- Understand the data definition and transmission process.
- Understand the concepts and advantages of the network reference model.
- Understand common standard protocols.
- Understand the data encapsulation and decapsulation processes.

Contents

Origin of the Story - Applications

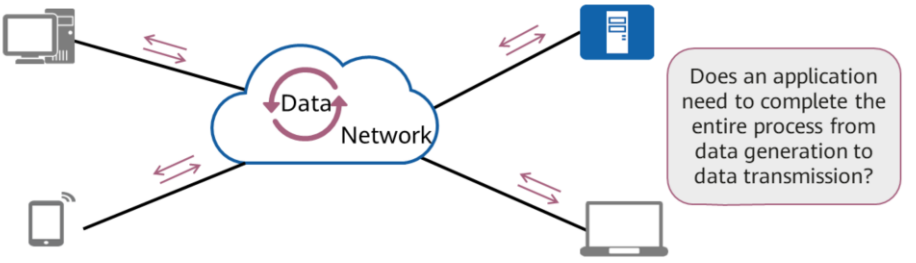
Applications are used to meet various requirements of people, such as web page access, online gaming, and online video playback.

Information is generated along with applications. Texts, pictures, and videos are all information presentation modes.

Application Implementation - Data

Data generation In the computer field, data is the carrier of all kinds of information.

Data transmission Data generated by most applications needs to be transmitted between devices.



HUAWEI

- A computer can identify only digital data consisting of 0s and 1s. It is incapable of reading other types of information, so the information needs to be translated into data by certain rules.
- However, people do not have the capability of reading electronic data. Therefore, data needs to be converted into information that can be understood by people.
- A network engineer needs to pay more attention to the end-to-end data transmission process.

Contents

HUAWEI

OSI Reference Model

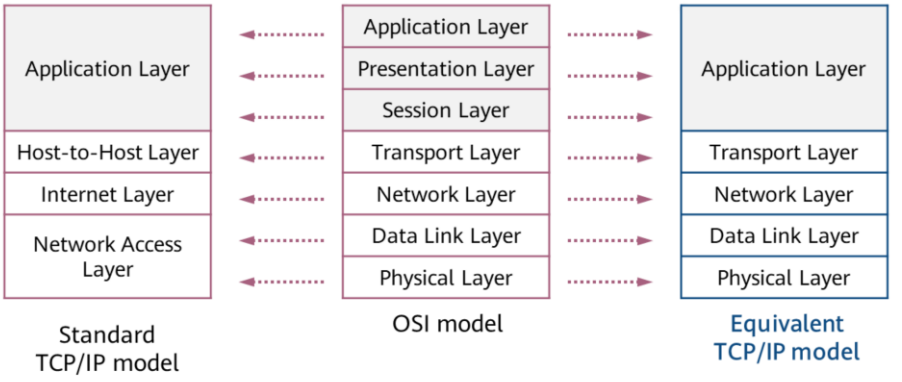
7. Application Layer	Provides interfaces for applications.
6. Presentation Layer	Translates data formats to ensure that the application-layer data of one system can be identified by the application layer of another system.
5. Session Layer	Establishes, manages, and terminates sessions between communicating parties.
4. Transport Layer	Establishes, maintains, and cancels an end-to-end data transmission process; controls transmission speeds and adjusts data sequences.
3. Network Layer	Defines logical addresses and transfers data from sources to destinations.
2. Data Link Layer	Encapsulates packets into frames, transmits frames in P2P or P2MP mode, and implements error checking.
1. Physical Layer	Transmits bitstreams over transmission media and defines electrical and physical specifications.

- The Open Systems Interconnection Model (OSI) was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.
- The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:
  - Physical layer: transmits bit flows between devices and defines physical specifications such as electrical levels, speeds, and cable pins.
  - Data link layer: encapsulates bits into octets and octets into frames, uses MAC addresses to access media, and implements error checking.
  - Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
  - Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error checking before retransmission.
  - Session layer: establishes, manages, and terminates sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between applications on different devices.
  - Presentation layer: provides data encoding and conversion so that data sent by the application layer of one system can be identified by the application layer of another system.
  - Application layer: provides network services for applications and the OSI layer

closest to end users.

TCP/IP Reference Model

The OSI protocol stack is complex, and the TCP and IP protocols are widely used in the industry. Therefore, the TCP/IP reference model becomes the mainstream reference model of the Internet.



- The TCP/IP model is similar to the OSI model in structure and adopts a hierarchical architecture. Adjacent TCP/IP layers are closely related.
- The standard TCP/IP model combines the data link layer and physical layer in the OSI model into the network access layer. This division mode is contrary to the actual protocol formulation. Therefore, the equivalent TCP/IP model that integrates the TCP/IP standard model and the OSI model is proposed. Contents in the following slides are based on the equivalent TCP/IP model.

Common TCP/IP Protocols

The TCP/IP protocol stack defines a series of standard protocols.

<table>
<tr><td rowspan="2">Application Layer</td><td>Telnet</td><td>FTP</td><td>TFTP</td><td>SNMP</td></tr>
<tr><td>HTTP</td><td>SMTP</td><td>DNS</td><td>DHCP</td></tr>
<tr><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td rowspan="2">Network Layer</td><td colspan="2">ICMP</td><td colspan="2">IGMP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td rowspan="2">Data Link Layer</td><td colspan="4">PPPoE</td></tr>
<tr><td colspan="2">Ethernet</td><td colspan="2">PPP</td></tr>
<tr><td>Physical Layer</td><td colspan="4">``````</td></tr>
</table>

- Application Layer
  - Hypertext Transfer Protocol (HTTP): is used to access various pages on web servers.
  - File Transfer Protocol (FTP): provides a method for transferring files. It allows data to be transferred from one host to another.
  - Domain name service (DNS): translates from host domain names to IP addresses.
- Transport layer
  - Transmission Control Protocol (TCP): provides reliable connection-oriented communication services for applications. Currently, TCP is used by many popular applications.
  - User Datagram Protocol (UDP): provides connectionless communication and does not guarantee the reliability of packet transmission. The reliability can be ensured by the application layer.
- Network layer
  - Internet Protocol (IP): encapsulates transport-layer data into data packets and forwards packets from source sites to destination sites. IP provides a connectionless and unreliable service.
  - Internet Group Management Protocol (IGMP): manages multicast group memberships. Specifically, IGMP sets up and maintains memberships between IP hosts and their directly connected multicast routers.
  - Internet Control Message Protocol (ICMP): sends control messages based on the IP protocol and provides information about various problems that may exist in the communication environment. Such information helps administrators diagnose problems and take proper measures to resolve the problems.

Common Protocol Standardization Organizations

IETF Internet Engineering Task Force

IETF is a voluntary organization responsible for developing and promoting Internet protocols (especially protocols that constitute the TCP/IP protocol suite), and releasing new or replacing old protocol standards through RFCs.

IEEE Institute of Electrical and Electronics Engineers

IEEE has formulated about 30% of standards in the electronics, electrical, and computer science fields worldwide. Those standards include well-known IEEE802.3 (Ethernet) and IEEE802.11 (Wi-Fi).

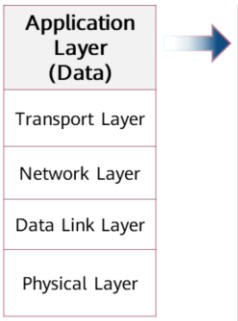
ISO International Organization for Standardization

ISO is an international organization that plays an important role in the formulation of computer network standards, such as the OSI model defined in ISO/IEC 7498-1.

Application Layer

The application layer provides interfaces for application software so that applications can use network services. The application layer protocol designates transport layer protocols and ports.

PDUs transmitted at the network layer are called data.



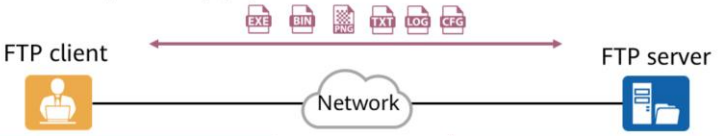
- HTTP 80 (TCP)
  Hypertext transfer protocol, which provides web browsing services.
- Telnet 23 (TCP)
  Remote login protocol, which provides remote management services.
- FTP 20 and 21 (TCP)
  File transfer protocol, which provides Internet file resource sharing services.
- SMTP 25 (TCP)
  Simple mail transfer protocol, which provides Internet email services.
- TFTP 69 (UDP)
  Simple file transfer protocol, which provides simple file transfer services.

- The TCP/IP suite enables data to be transmitted over a network. The layers use packet data units (PDUs) to exchange data, implementing communication between network devices.
- PDUs transmitted at different layers contain different information. Therefore, PDUs have different names at different layers.

Common Application Layer Protocols - FTP

FTP File Transfer Protocol

FTP transfers files from one host to another to implement file download and upload. This protocol adopts the client/server (C/S) structure.



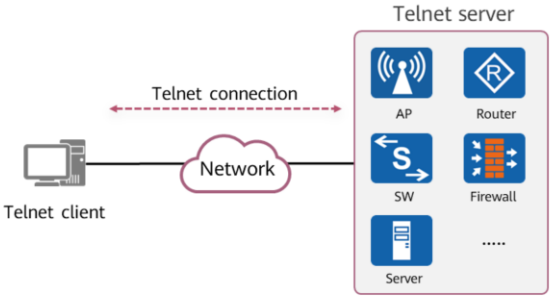
FTP client: provides commands for local users to operate files on a remote server. A user can install an FTP client program on a PC and set up a connection with an FTP server to operate files on the server.

FTP server: a device that runs the FTP service. It provides the access and operation functions for remote clients, allowing users to access the FTP server through the FTP client program and access files on the server.

Common Application Layer Protocols - Telnet

Telnet A standard protocol that provides remote login services on a network.

It provides users with the ability to operate remote devices through local PCs.

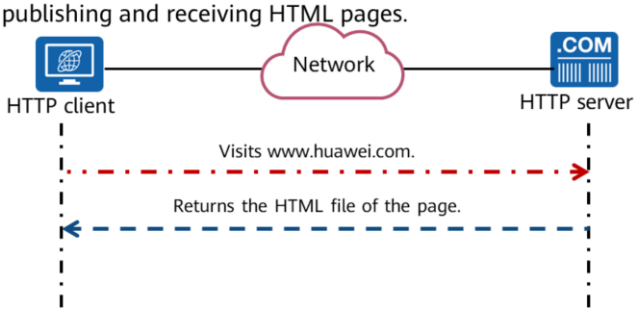


A user connects to a Telnet server through the Telnet client program. The commands entered on the Telnet client are executed on the server, as if the commands were entered on the console of the server.

Common Application Layer Protocols - HTTP

HTTP HyperText Transfer Protocol

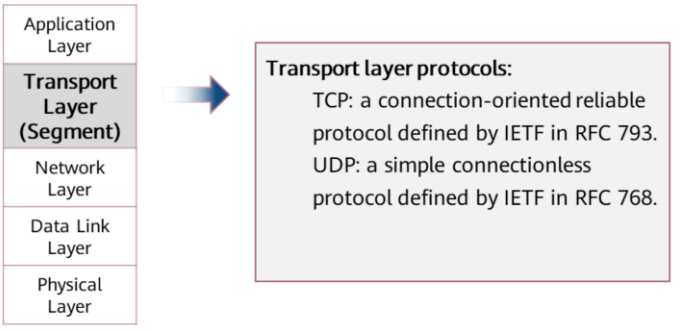
HTTP is one of the most widely used network protocols on the Internet. HTTP was originally designed to provide a method for publishing and receiving HTML pages.



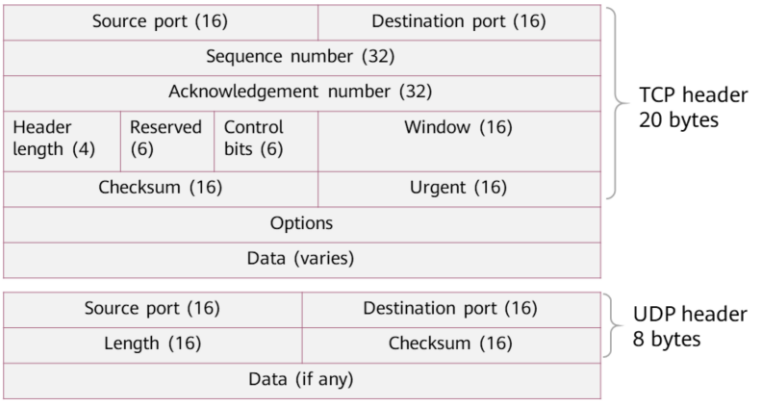
Transport Layer

A transport layer protocol receives data from an application layer protocol, encapsulates the data with the corresponding transport layer protocol header, and helps establish an end-to-end (port-to-port) connection.

PDUs transmitted at the transport layer are called segments.

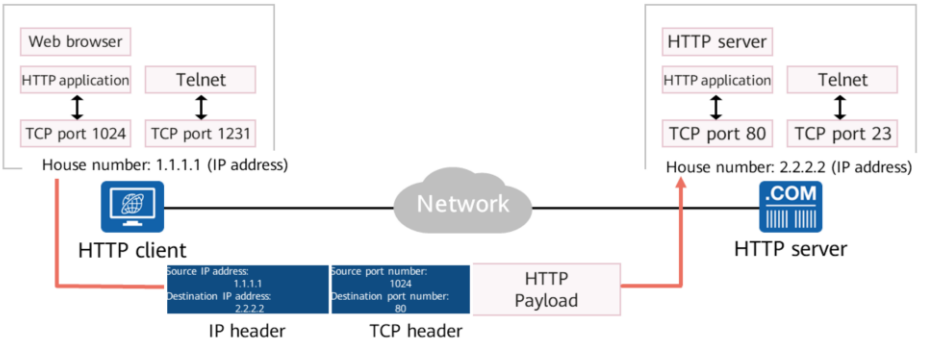


TCP and UDP - Header Formats



- TCP header:
  - Source Port: identifies the application that sends the segment. This field is 16 bits long.
  - Destination Port: identifies the application that receives the segment. This field is 16 bits long.
  - Sequence Number: Every byte of data sent over a TCP connection has a sequence number. The value of the Sequence Number field equals the sequence number of the first byte in a sent segment. This field is 32 bits long.
  - Acknowledgment Number: indicates the sequence number of the next segment's first byte that the receiver is expecting to receive. The value of this field is 1 plus the sequence number of the last byte in the previous segment that is successfully received. This field is valid only when the ACK flag is set. This field is 32 bits long.
  - Header Length: indicates the length of the TCP header. The unit is 32 bits (4 bytes). If there is no option content, the value of this field is 5, indicating that the header contains 20 bytes.
  - Reserved: This field is reserved and must be set to 0. This field is 6 bits long.
  - Control Bits: control bits, includes FIN, ACK, and SYN flags, indicating TCP data segments in different states.
  - Window: used for TCP flow control. The value is the maximum number of bytes that are allowed by the receiver. The maximum window size is 65535 bytes. This field is 16 bits long.
  - Checksum: a mandatory field. It is calculated and stored by the sender and verified by the receiver. During checksum computation, the TCP header and TCP data are included, and a 12-byte pseudo header is added before the TCP segment. This field is 16 bits long.

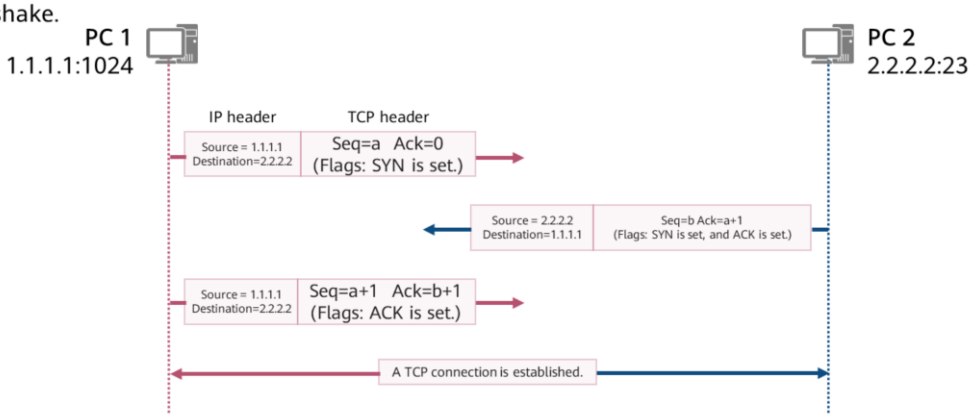
TCP and UDP - Port Numbers



Generally, the source port used by a client is randomly allocated, and the destination port is specified by the application of a server. The system generally selects a source port number that is greater than 1023 and is not being used.
The destination port number is the listening port of the application (service) enabled on the server. For example, the default port number for HTTP is 80.

TCP Connection Setup - Three-Way Handshake

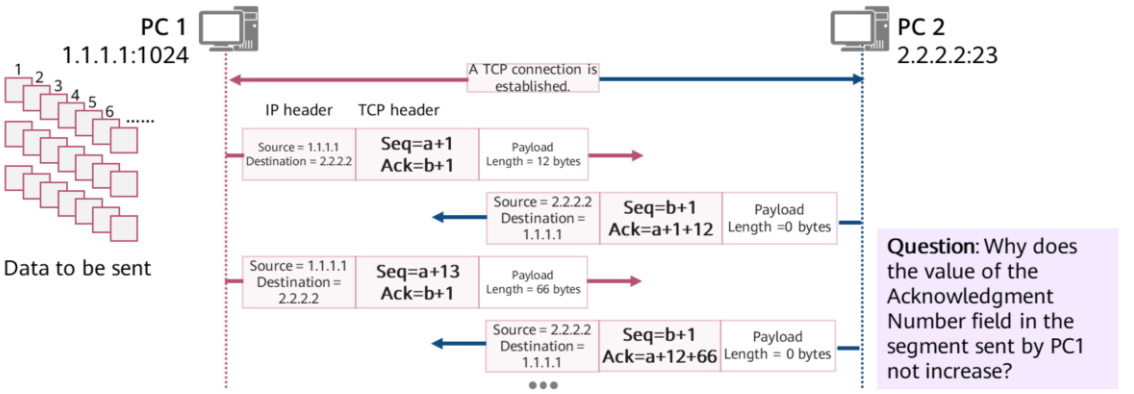
Before sending data, a TCP-based application needs to establish a connection through three-way handshake.



- The TCP connection setup process is as follows:
  - The TCP connection initiator (PC1 in the figure) sends the first TCP segment with SYN being set. The initial sequence number a is a randomly generated number. The acknowledgment number is 0 because no segment has ever been received from PC2.
  - After receiving a valid TCP segment with the SYN flag being set, the receiver (PC2) replies with a TCP segment with SYN and ACK being set. The initial sequence number b is a randomly generated number. Because the segment is a response one to PC1, the acknowledgment number is a+1.
  - After receiving the TCP segment in which SYN and ACK are set, PC1 replies with a segment in which ACK is set, the sequence number is a+1, and the acknowledgment number is b+1. After PC2 receives the segment, a TCP connection is established.

TCP Sequence Number and Acknowledgment Number

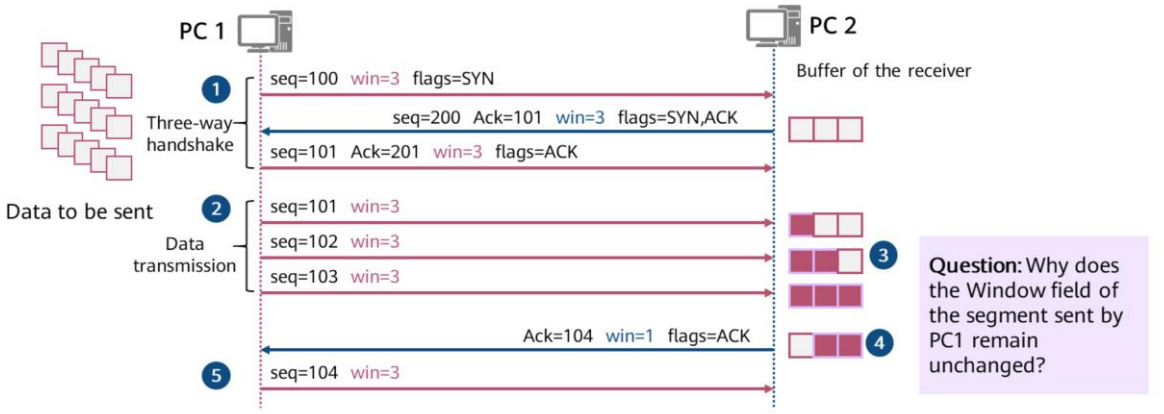
TCP uses the Sequence Number and Acknowledgment Number fields to implement reliable and ordered data transmission.



- Assume that PC1 needs to send segments of data to PC2. The transmission process is as follows:
    1. PC1 numbers each byte to be sent by TCP. Assume that the number of the first byte is a+1. Then, the number of the second byte is a+2, the number of the third byte is a+3, and so on.
    2. PC1 uses the number of the first byte of each segment of data as the sequence number and sends out the TCP segment.
    3. After receiving the TCP segment from PC1, PC2 needs to acknowledge the segment and request the next segment of data. How is the next segment of data determined? Sequence number (a+1) + Payload length = Sequence number of the first byte of the next segment (a+1+12)
    4. After receiving the TCP segment sent by PC2, PC1 finds that the acknowledgment number is a+1+12, indicating that the segments from a+1 to a+12 have been received and the sequence number of the upcoming segment to be sent should be a+1+12.
- To improve the sending efficiency, multiple segments of data can be sent at a time by the sender and then acknowledged at a time by the receiver.

TCP Window Sliding Mechanism

TCP uses the sliding window mechanism to control the data transmission rate.

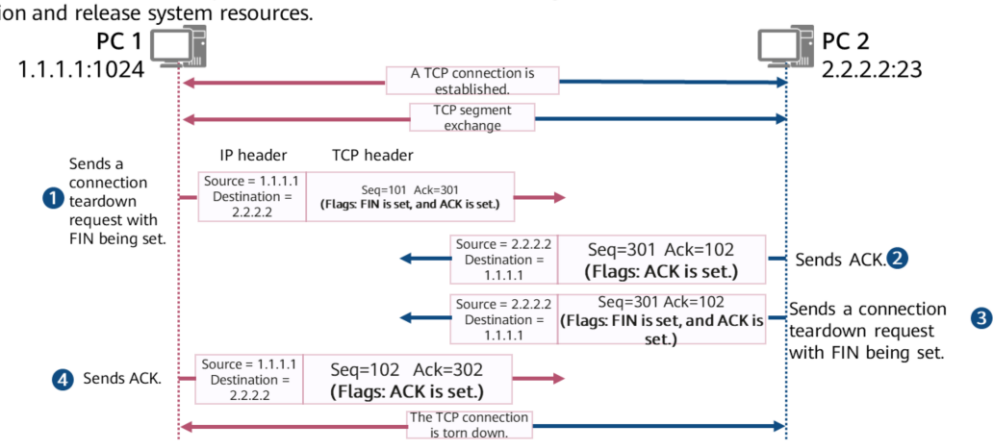


HUAWEI

1. During the TCP three-way handshake, both ends notify each other of the maximum number of bytes (buffer size) that can be received by the local end through the Window field.
2. After the TCP connection is set up, the sender sends data of the specified number of bytes based on the window size declared by the receiver.
3. After receiving the data, the receiver stores the data in the buffer and waits for the upper-layer application to obtain the buffered data. After the data is obtained by the upper-layer application, the corresponding buffer space is released.
4. The receiver notifies the current acceptable data size (window) according to its buffer size.
5. The sender sends a certain amount of data based on the current window size of the receiver.

TCP Shutdown - Four-Way Handshake

After data transmission is complete, TCP needs to use the four-way handshake mechanism to disconnect the TCP connection and release system resources.

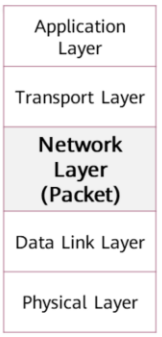


- TCP supports data transmission in full-duplex mode, which means that data can be transmitted in both directions at the same time. Before data is transmitted, TCP sets up a connection in both directions through three-way handshake. Therefore, after data transmission is complete, the connection must be closed in both directions. This is shown in the figure.
    1. PC1 sends a TCP segment with FIN being set. The segment does not carry data.
    2. After receiving the TCP segment from PC1, PC2 replies with a TCP segment with ACK being set.
    3. PC2 checks whether data needs to be sent. If so, PC2 sends the data, and then a TCP segment with FIN being set to close the connection. Otherwise, PC2 directly sends a TCP segment with FIN being set.
    4. After receiving the TCP segment with FIN being set, PC1 replies with an ACK segment. The TCP connection is then torn down in both directions.

Network Layer

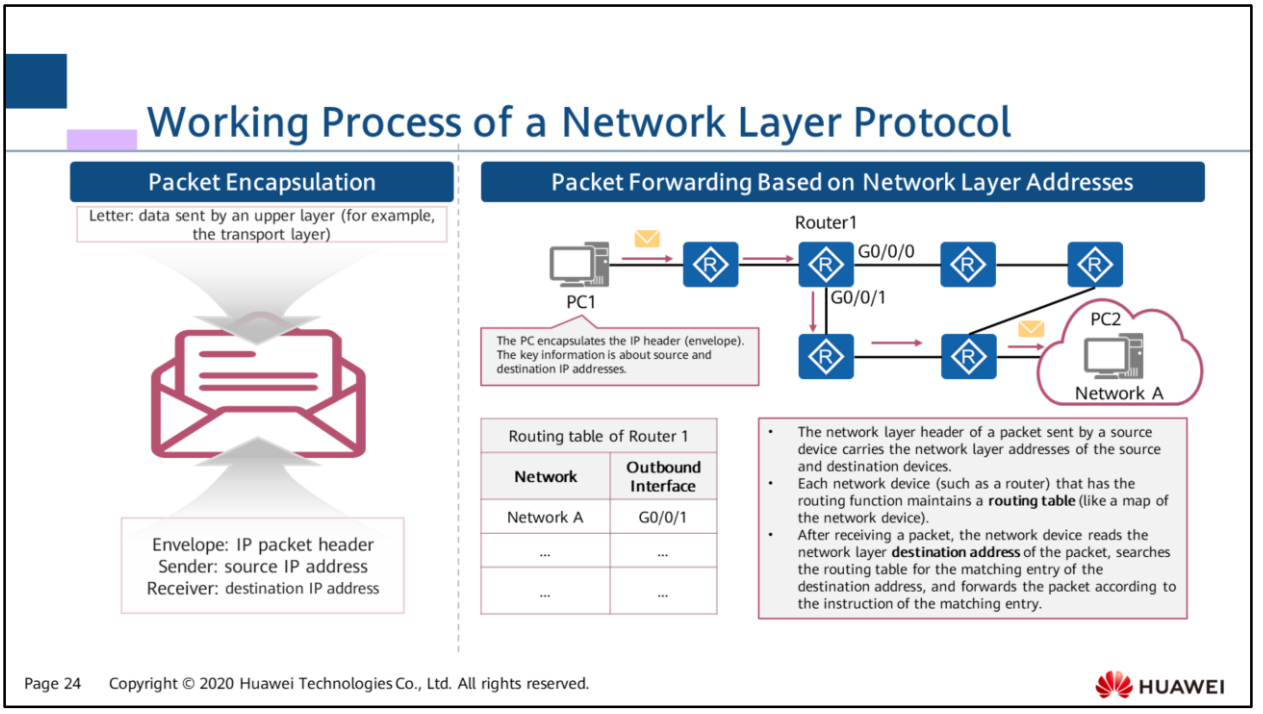
The transport layer is responsible for establishing connections between processes on hosts, and the network layer is responsible for transmitting data from one host to another.

PDUs transmitted at the network layer are called packets.



- The network layer is also called the Internet layer.
  - It sends packets from source hosts to destination hosts.
- Functions of the network layer:
  - Provides logical addresses for network devices.
  - Routes and forwards data packets.
  - Common network layer protocols include IPv4, IPv6, ICMP, and IGMP.

- Internet Protocol Version 4 (IPv4) is the most widely used network layer protocol.

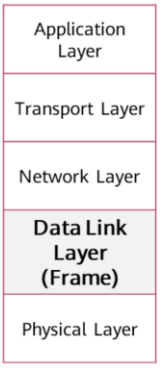


- When IP is used as the network layer protocol, both communication parties are assigned a unique IP address to identify themselves. An IP address can be written as a 32-bit binary integer. To facilitate reading and analysis, an IP address is usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, such as, 192.168.1.1.
- Encapsulation and forwarding of IP data packets:
    - When receiving data from an upper layer (such as the transport layer), the network layer encapsulates an IP packet header and adds the source and destination IP addresses to the header.
    - Each intermediate network device (such as a router) maintains a routing table that guides IP packet forwarding like a map. After receiving a packet, the intermediate network device reads the destination address of the packet, searches the local routing table for a matching entry, and forwards the IP packet according to the instruction of the matching entry.
    - When the IP packet reaches the destination host, the destination host determines whether to accept the packet based on the destination IP address and then processes the packet accordingly.
- When the IP protocol is running, routing protocols such as OSPF, IS-IS, and BGP are required to help routers build routing tables, and ICMP is required to help control networks and diagnose network status.

Data Link Layer

The data link layer is located between the network layer and the physical layer and provides services for protocols such as IP and IPv6 at the network layer. PDUs transmitted at the data link layer are called frames.

Ethernet is the most common data link layer protocol.

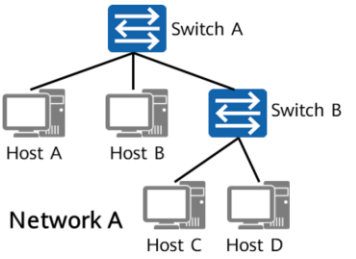


The data link layer is located between the network layer and the physical layer.

- The data link layer provides intra-segment communication for the network layer.
- The functions of the data link layer include framing, physical addressing, and error control.
- Common data link layer protocols include Ethernet, PPPoE, and PPP.

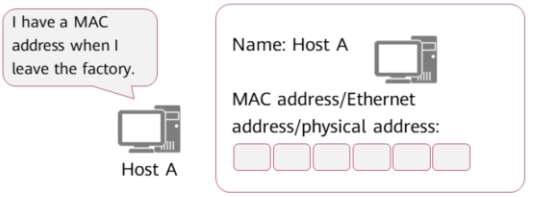
Ethernet and Source MAC Addresses

Ethernet Definition



- Ethernet is a broadcast multiple access protocol that works at the data link layer protocol.
- The network interfaces of PCs comply with the Ethernet standard.
- Generally, a broadcast domain corresponds to an IP network segment.

Ethernet Source MAC Addresses



- A media access control (MAC) address uniquely identifies a NIC on a network. Each NIC requires and has a unique MAC address.
- MAC addresses are used to locate specific physical devices in an IP network segment.
- A device that works at the data link layer, such as an Ethernet switch, maintains a MAC address table to guide data frame forwarding.

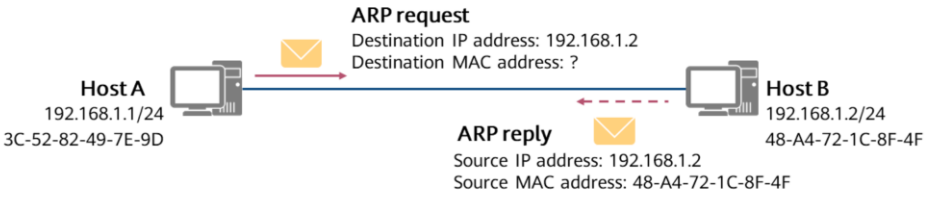
HUAWEI

- A MAC address is recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator. Example: 48-A4-72-1C-8F-4F

ARP

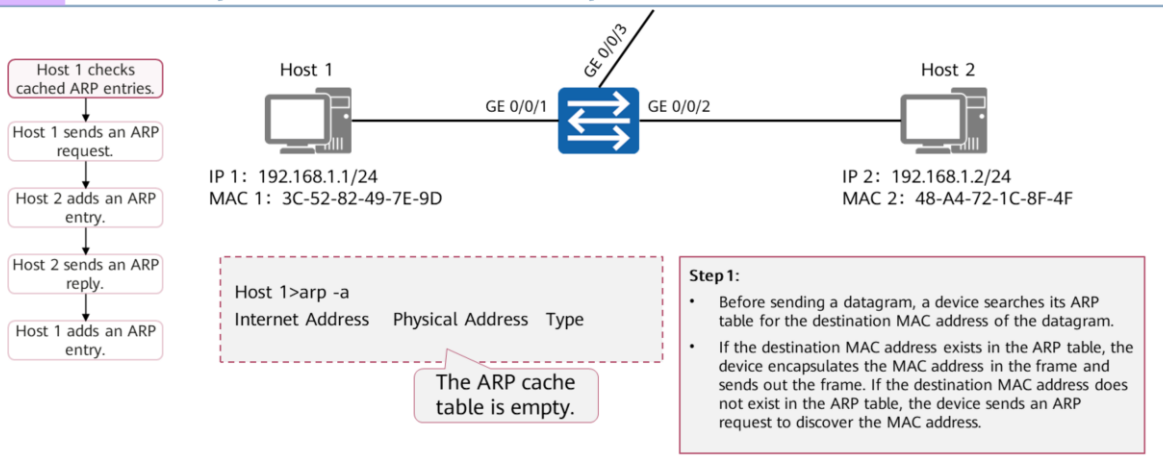
ARP Address Resolution Protocol

Discovers the MAC address associated with a given IP address.



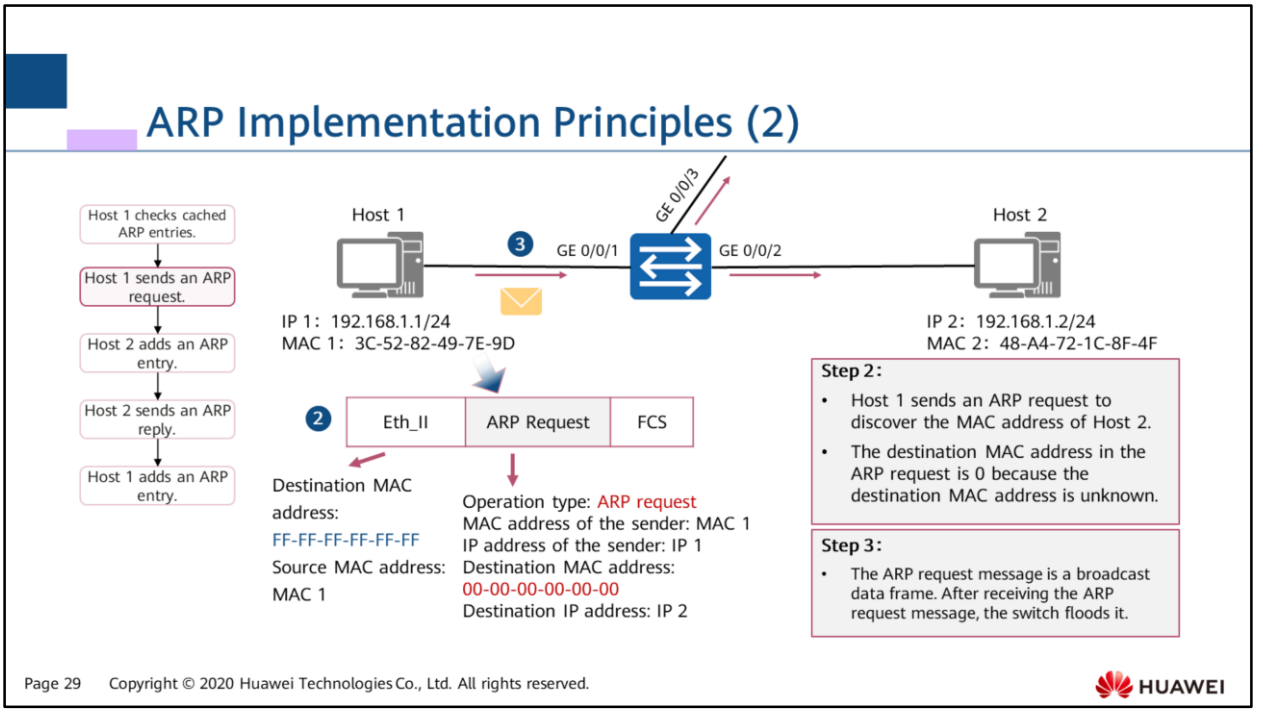
- The Address Resolution Protocol (ARP) is a TCP/IP protocol that discovers the data link layer address associated with a given IP address.
- ARP is an indispensable protocol in IPv4. It provides the following functions:
  - Discovers the MAC address associated with a given IP address.
  - Maintains and caches the mapping between IP addresses and MAC addresses through ARP entries.
  - Detects duplicate IP addresses on a network segment.

ARP Implementation Principles (1)



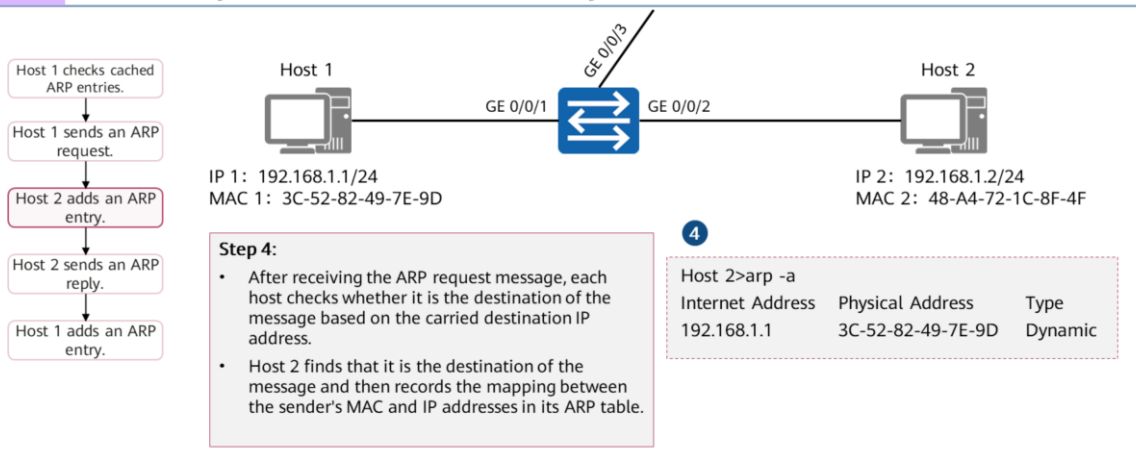
HUAWEI

- Generally, a network device has an ARP cache. The ARP cache stores the mapping between IP addresses and MAC addresses.
- Before sending a datagram, a device searches its ARP table. If a matching ARP entry is found, the device encapsulates the corresponding MAC address in the frame and sends out the frame. If a matching ARP entry is not found, the device sends an ARP request to discover the MAC address.
- The learned mapping between the IP address and MAC address is stored in the ARP table for a period. Within the validity period (180s by default), the device can directly search this table for the destination MAC address for data encapsulation, without performing ARP-based query. After the validity period expires, the ARP entry is automatically deleted.
- If the destination device is located on another network, the source device searches the ARP table for the gateway MAC address of the destination address and sends the datagram to the gateway. Then, the gateway forwards the datagram to the destination device.



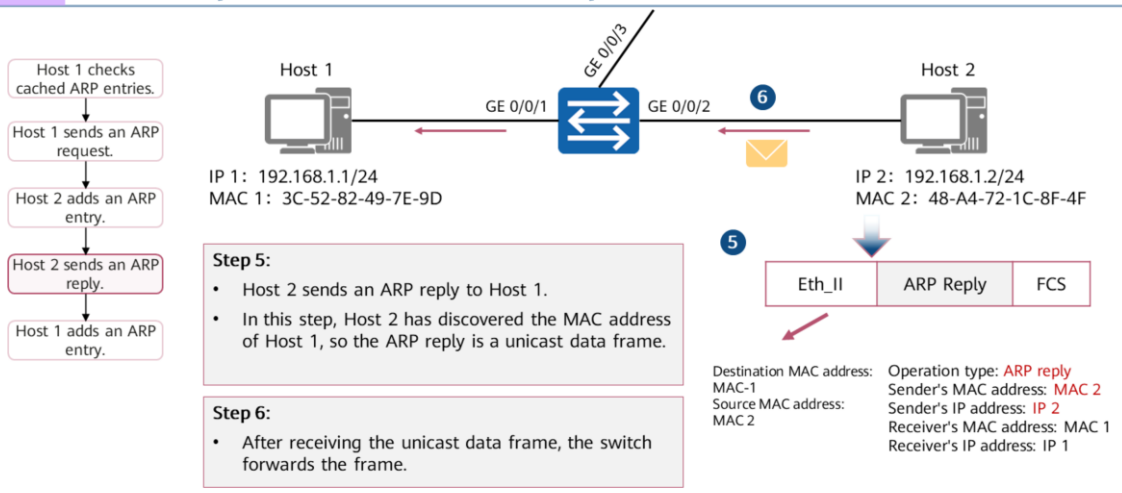
- In this example, the ARP table of Host 1 does not contain the MAC address of Host 2. Therefore, Host 1 sends an ARP request message to discover the destination MAC address.
- The ARP request message is encapsulated in an Ethernet frame. The source MAC address in the frame header is the MAC address of Host 1 at the transmit end. Because Host 1 does not know the MAC address of Host 2, the destination MAC address is the broadcast address FF-FF-FF-FF-FF-FF.
- The ARP request message contains the source MAC address, source IP address, destination MAC address, and destination IP address. The destination MAC address is all 0s. The ARP request message is broadcast to all hosts on the network, including gateways.

ARP Implementation Principles (3)



- After receiving the ARP request message, each host checks whether it is the destination of the message based on the carried destination IP address. If not, the host does not respond to the ARP request message. If so, the host adds the sender's MAC and IP addresses carried in the ARP request message to the ARP table, and then replies with an ARP reply message.

ARP Implementation Principles (4)



Step 5:

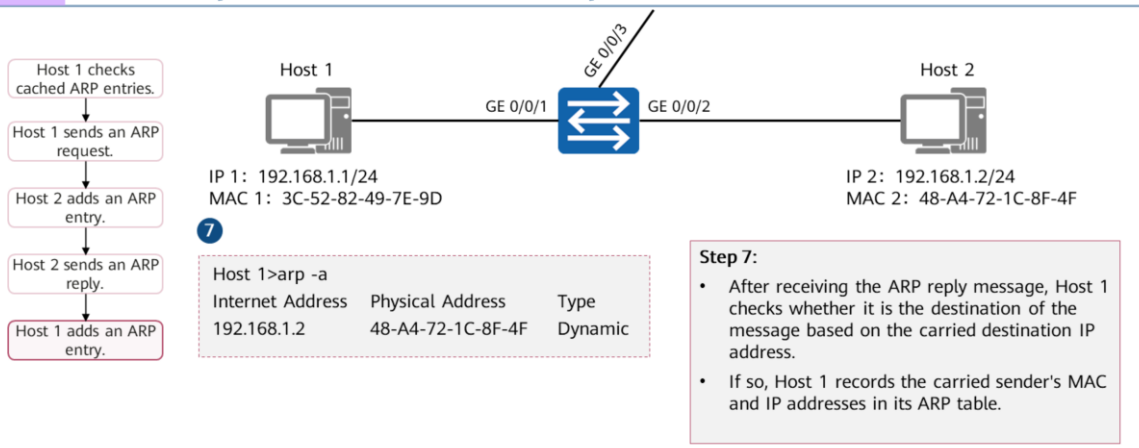
- Host 2 sends an ARP reply to Host 1.
- In this step, Host 2 has discovered the MAC address of Host 1, so the ARP reply is a unicast data frame.

Step 6:

- After receiving the unicast data frame, the switch forwards the frame.

- Host 2 sends an ARP reply message to Host 1.
- In the ARP reply message, the sender's IP address is the IP address of Host 2 and the receiver's IP address is the IP address of Host 1. The receiver's MAC address is the MAC address of Host 1 and the sender's MAC address is the MAC address of Host 2. The operation type is set to reply.
- ARP reply messages are transmitted in unicast mode.

ARP Implementation Principles (5)

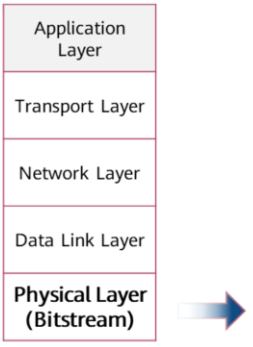


- After receiving the ARP reply message, Host 1 checks whether it is the destination of the message based on the carried destination IP address. If so, Host 1 records the carried sender's MAC and IP addresses in its ARP table.

Physical Layer

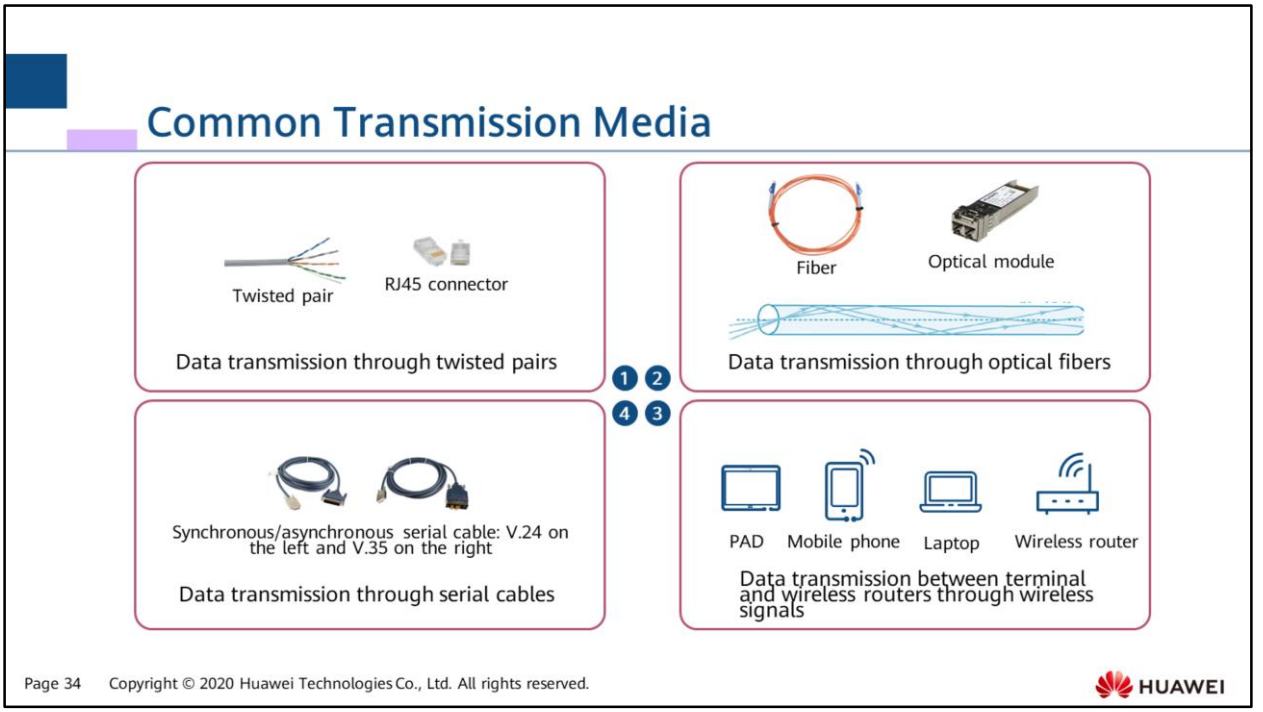
After data arrives at the physical layer, the physical layer converts a digital signal into an optical signal, an electrical signal, or an electromagnetic wave signal based on the physical media.

PDUs transmitted at the physical layer are called bitstreams.



The physical layer is at the bottom of the model.

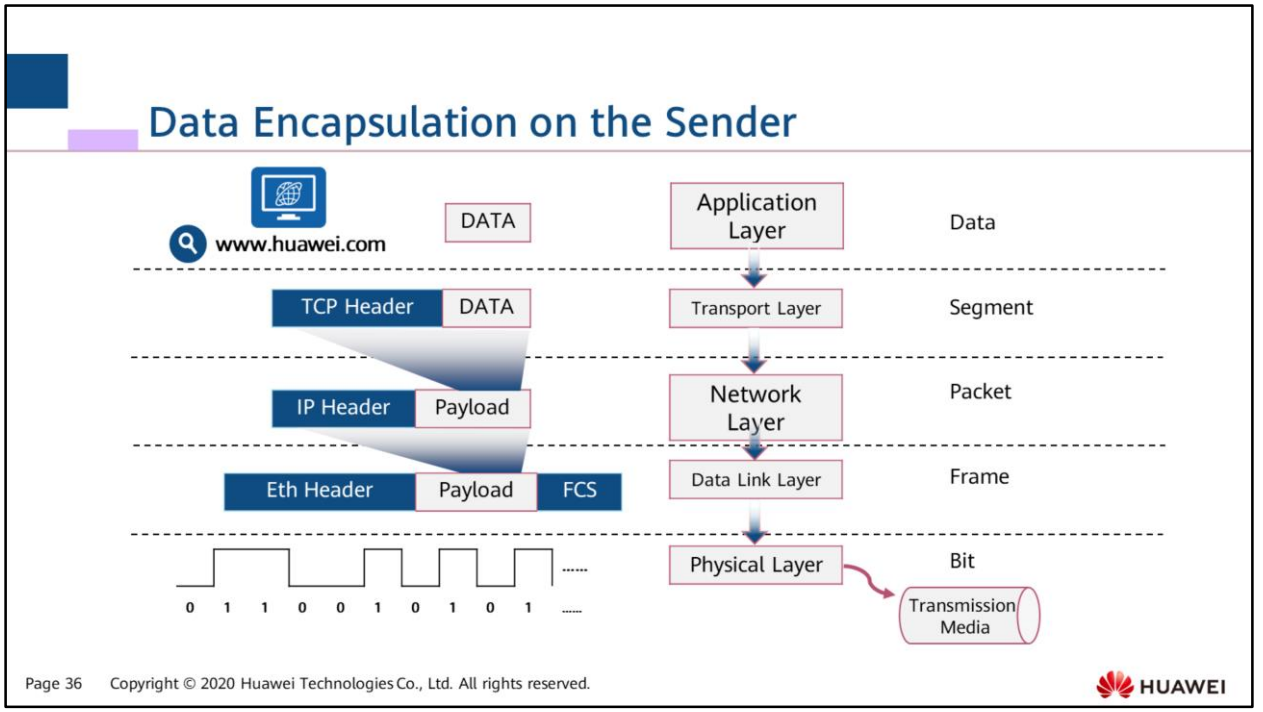
- This layer transmits bitstreams on media.
- It standardizes physical features such as cables, pins, voltages, and interfaces.
- Common transmission media include twisted pairs, optical fibers, and electromagnetic waves.



- Twisted pairs: most common transmission media used on Ethernet networks. Twisted pairs can be classified into the following types based on their anti-electromagnetic interference capabilities:
  - STP: shielded twisted pairs
  - UTP: unshielded twisted pairs
- Optical fiber transmission can be classified into the following types based on functional components:
  - Fibers: optical transmission media, which are glass fibers, used to restrict optical transmission channels.
  - Optical modules: convert electrical signals into optical signals to generate optical signals.
- Serial cables are widely used on wide area networks (WANs). The types of interfaces connected to serial cables vary according to WAN line types. The interfaces include synchronous/synchronous serial interfaces, ATM interfaces, POS interfaces, and CE1/PRI interfaces.
- Wireless signals may be transmitted by using electromagnetic waves. For example, a wireless router modulates data and sends the data by using electromagnetic waves, and a wireless network interface card of a mobile terminal demodulates the electromagnetic waves to obtain data. Data transmission from the wireless router to the mobile terminal is then complete.

Contents

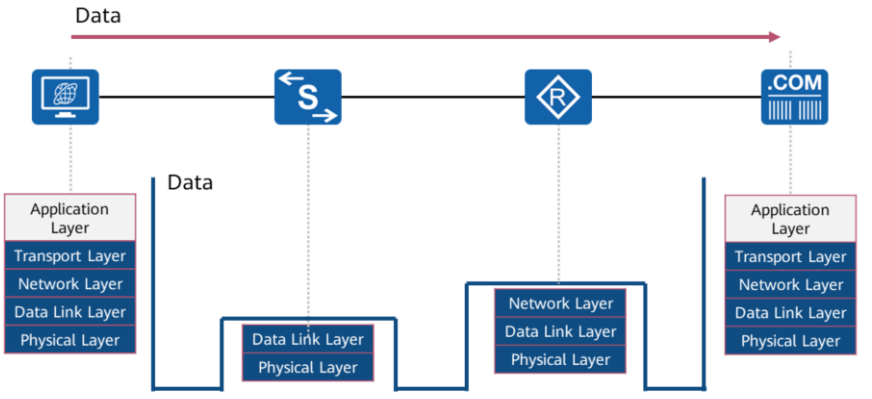
HUAWEI



- Assume that you are using a web browser to access Huawei's official website. After you enter the website address and press Enter, the following events occur on your computer:
    1. The browser (application program) invokes HTTP (application layer protocol) to encapsulate the application layer data. (The DATA in the figure should also include the HTTP header, which is not shown here.)
    2. HTTP uses TCP to ensure reliable data transmission and transmits encapsulated data to the TCP module.
    3. The TCP module adds the corresponding TCP header information (such as the source and destination port numbers) to the data transmitted from the application layer. At the transport layer, the PDU is called a segment.
    4. On an IPv4 network, the TCP module sends the encapsulated segment to the IPv4 module at the network layer. (On an IPv6 network, the segment is sent to the IPv6 module for processing.)
    5. After receiving the segment from the TCP module, the IPv4 module encapsulates the IPv4 header. At this layer, the PDU is called a packet.

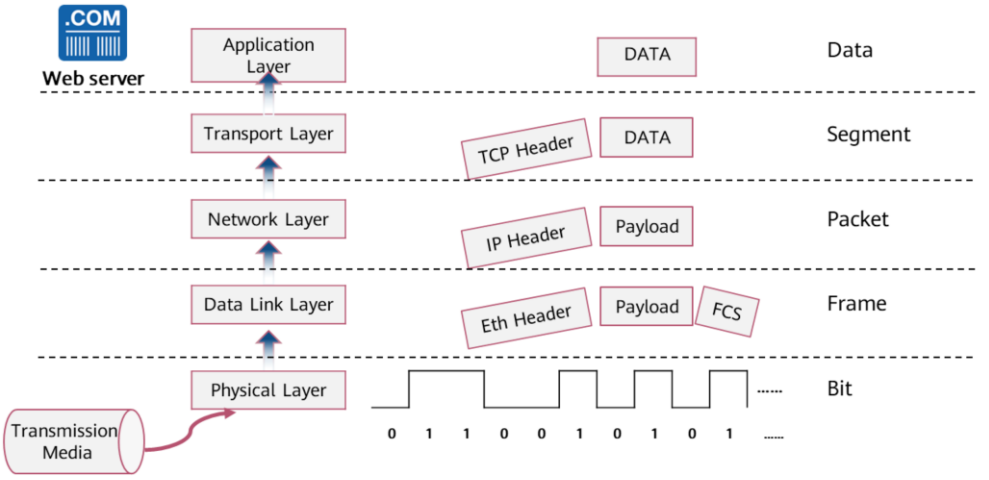
Data Transmission on the Intermediate Network

Encapsulated data is transmitted on the network.



- In most cases:
  - A Layer 2 device (such as an Ethernet switch) only decapsulates the Layer 2 header of the data and performs the corresponding switching operation according to the information in the Layer 2 header.
  - A Layer 3 device (such as a router) decapsulates the Layer 3 header and performs routing operations based on the Layer 3 header information.
  - Note: The details and principles of switching and routing will be described in subsequent courses.

Data Decapsulation on the Receiver



HUAWEI

- After being transmitted over the intermediate network, the data finally reaches the destination server. Based on the information in different protocol headers, the data is decapsulated layer by layer, processed, transmitted, and finally sent to the application on the web server for processing.

Summary

- Both the OSI reference model and the TCP/IP reference model adopt the layered design concept.
  - Clear division of functions and boundaries between layers facilitates the development, design, and troubleshooting of each component.
  - The functions of each layer can be defined to impel industry standardization.
  - Interfaces can be provided to enable communication between hardware and software on various networks, improving compatibility.
- Data generation and transmission require collaboration between modules. Meanwhile, each module must fulfill its own responsibilities.

Quiz

What are the benefits of the layered model?

- Clear division of functions and boundaries between layers facilitates the development, design, and troubleshooting of each component.
- The functions of each layer can be defined to impel industry standardization.
- Interfaces can be provided to enable communication between hardware and software on various networks, improving compatibility.

1. Answer:
   - Clear division of functions and boundaries between layers facilitates the development, design, and troubleshooting of each component.
   - The functions of each layer can be defined to impel industry standardization.
   - Interfaces can be provided to enable communication between hardware and software on various networks, improving compatibility.
2. Answer:
   - Application layer: HTTP, FTP, Telnet, and so on
   - Transport layer: UDP and TCP
   - Network layer: IP, ICMP, and so on
   - Data link layer: Ethernet, PPP, PPPoE, and so on

Quiz

What are the common protocols at the application layer, transport layer, network layer, and data link layer?

- Application layer: HTTP, FTP, Telnet, and so on
- Transport layer: UDP and TCP
- Network layer: IP, ICMP, and so on
- Data link layer: Ethernet, PPP, PPPoE, and so on