Network Reference Model



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |
|  |  |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



Contents

[1 Network Reference Model 1](#_Toc59714037)

[1.1 Foreword 1](#_Toc59714038)

[1.2 Objectives 1](#_Toc59714039)

[1.3 Applications and Data 1](#_Toc59714040)

[1.3.1 Origin of the Story – Applications 1](#_Toc59714041)

[1.3.2 Application Implementation – Data 2](#_Toc59714042)

[1.4 Network Reference Model and Standard Protocols 2](#_Toc59714043)

[1.4.1 OSI Reference Model 2](#_Toc59714044)

[1.4.2 TCP/IP Reference Model 3](#_Toc59714045)

[1.4.3 Common TCP/IP Protocols 4](#_Toc59714046)

[1.4.4 Common Protocol Standardization Organizations 5](#_Toc59714047)

[1.4.5 Application Layer 5](#_Toc59714048)

[1.4.6 Transport Layer 7](#_Toc59714049)

[1.4.7 TCP and UDP 7](#_Toc59714050)

[1.4.8 TCP Connection Setup - Three-Way Handshake 9](#_Toc59714051)

[1.4.9 TCP Sequence Number and Acknowledgment Number 10](#_Toc59714052)

[1.4.10 TCP Window Sliding Mechanism 10](#_Toc59714053)

[1.4.11 TCP Shutdown - Four-Way Handshake 11](#_Toc59714054)

[1.4.12 Network Layer 12](#_Toc59714055)

[1.4.13 Working Process of a Network Layer Protocol 13](#_Toc59714056)

[1.4.14 Data Link Layer 14](#_Toc59714057)

[1.4.15 Ethernet and Source MAC Addresses 14](#_Toc59714058)

[1.4.16 ARP 15](#_Toc59714059)

[1.4.17 Physical Layer 19](#_Toc59714060)

[1.4.18 Common Transmission Media 19](#_Toc59714061)

[1.5 Data Communication Process 21](#_Toc59714062)

[1.5.1 Data Encapsulation on the Sender 21](#_Toc59714063)

[1.5.2 Data Transmission on the Intermediate Network 22](#_Toc59714064)

[1.5.3 Data Decapsulation on the Receiver 23](#_Toc59714065)

[1.6 Summary 24](#_Toc59714066)

[1.7 Quiz 23](#_Toc59714067)

# 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

On completion of this course, you will be able to:

Understand the data definition and transmission process.

Understand the concepts and advantages of the network reference model.

Understand common standard protocols.

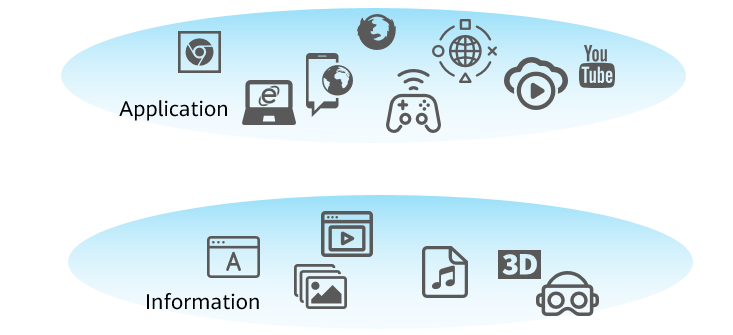
Understand the data encapsulation and decapsulation processes.

## Applications and Data

### 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.

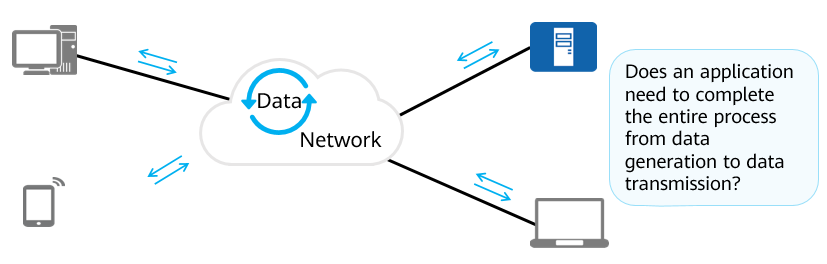


Application and Information

### 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.



Data generation and transmission

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.

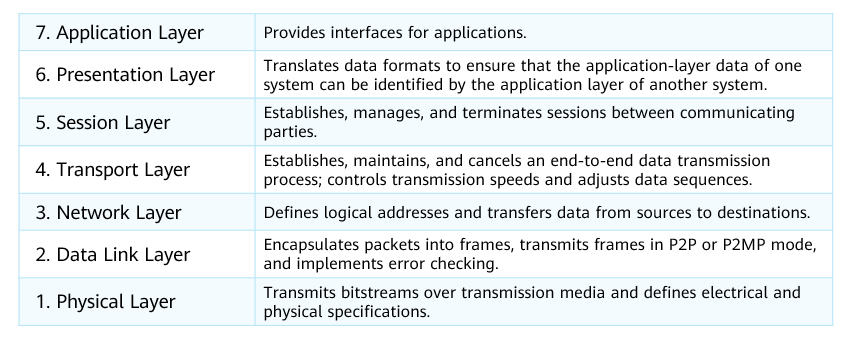
## Network Reference Model and Standard Protocols

### OSI Reference Model

The Open Systems Interconnection Model (OSI) was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.

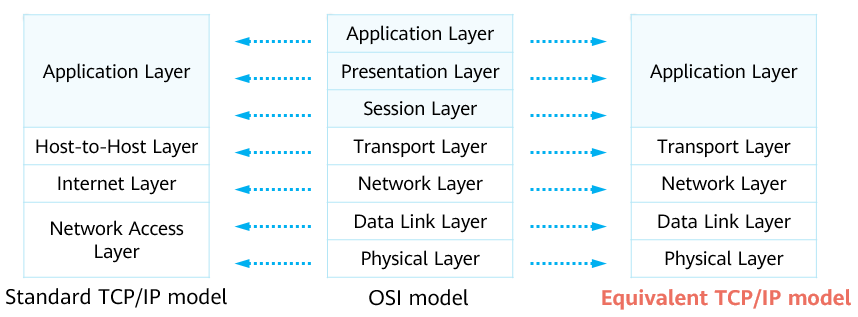
The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:

* 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.



OSI Reference Model

### TCP/IP Reference Model



TCP/IP Reference Model

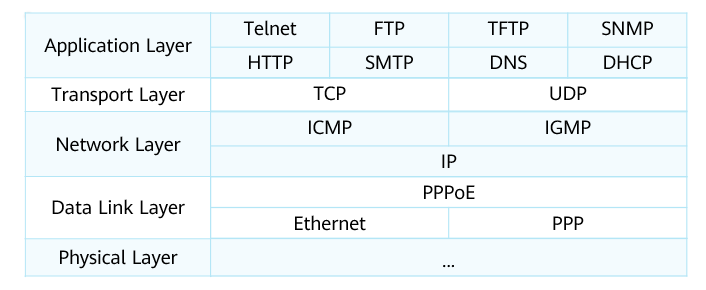
The TCP/IP model is similar to the OSI model in structure and adopts a hierarchical architecture. Adjacent TCP/IP layers are closely related.

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.

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.

### Common TCP/IP Protocols

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



Common TCP/IP Protocols

* 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.

* Data link layer

Point-to-Point Protocol (PPP): is a data link layer protocol that works in point-to-point mode. PPP is mainly used on wide area networks (WANs).

Ethernet: is a multi-access and broadcast protocol at the data link layer, which is the most widely used local area network (LAN) technology.

Point-to-Point Protocol over Ethernet (PPPoE): connects multiple hosts on a network to a remote access concentrator through a simple bridge device (access device). Common applications include home broadband dialup access.

### Common Protocol Standardization Organizations

* Internet Engineering Task Force (IETF)

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.

* Institute of Electrical and Electronics Engineers (IEEE)

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).

* International Organization for Standardization (ISO)

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.

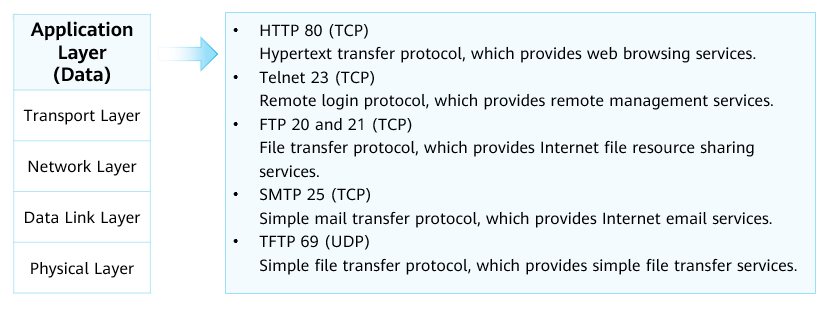
### Application Layer

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.

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.

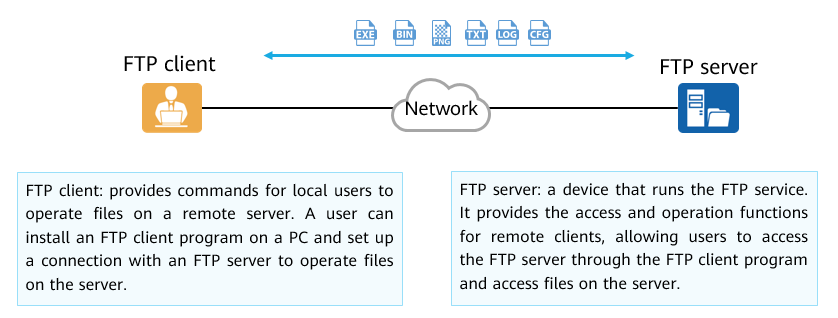
PDUs transmitted at the application layer are called data.



Application Layer

1. Common Application Layer Protocols – FTP

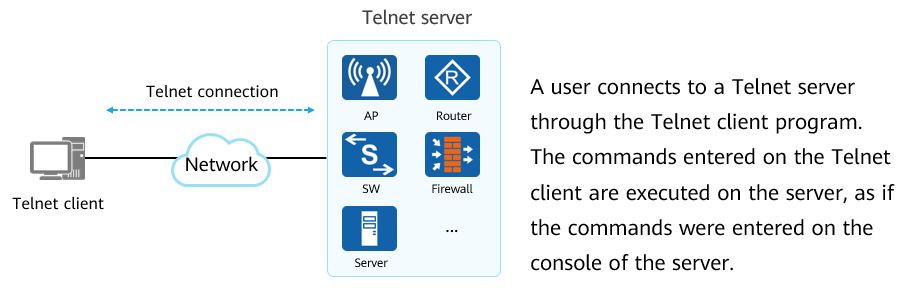
The File Transfer Protocol (FTP) transfers files from one host to another to implement file download and upload. This protocol adopts the client/server (C/S) structure.



FTP

1. Common Application Layer Protocols - Telnet

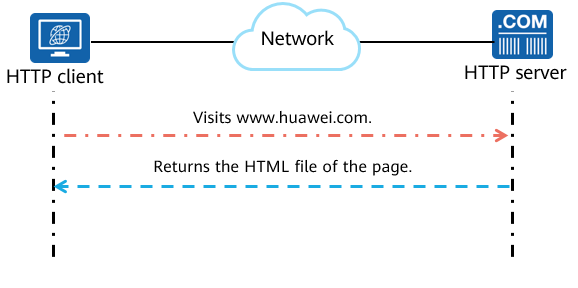
Telnet is a standard protocol that provides remote login services on a network. It provides users with the ability to operate remote devices through local PCs.



Telnet

1. Common Application Layer Protocols – 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.

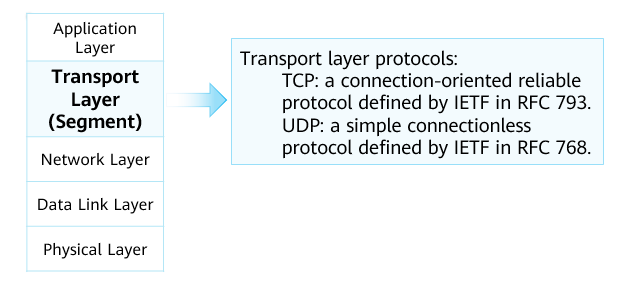


HTTP

### 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.

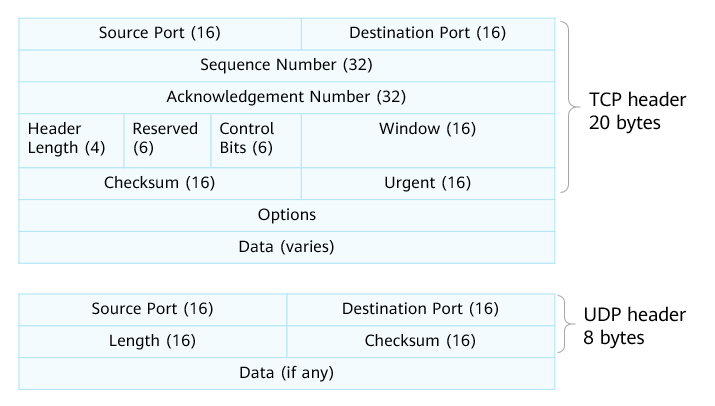
PDUs transmitted at the transport layer are called segments.



Transport Layer

### TCP and UDP

1. Header Formats



Header Formats

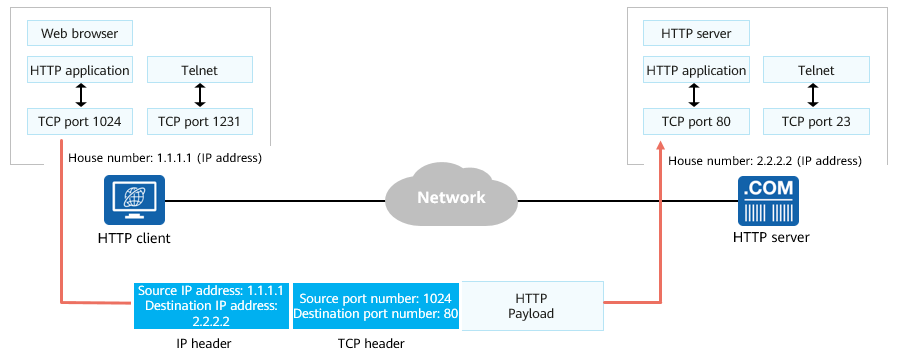
TCP header:

* 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.
* Urgent: indicates the urgent pointer. The urgent pointer is valid only when the URG flag is set. The Urgent field indicates that the sender transmits data in emergency mode. The urgent pointer indicates the number of urgent data bytes in a segment (urgent data is placed at the beginning of the segment). This field is 16 bits long.
* Options: This field is optional. This field is 0 to 40 bytes long.

UDP 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.
* Length: specifies the total length of the UDP header and data. The possible minimum length is 8 bytes because the UDP header already occupies 8 bytes. Due to the existence of this field, the total length of a UDP segment does not exceed 65535 bytes (including an 8-byte header and 65527-byte data).
* Checksum: checksum of the UDP header and UDP data. This field is 16 bits long.

1. Port Numbers



Port Numbers

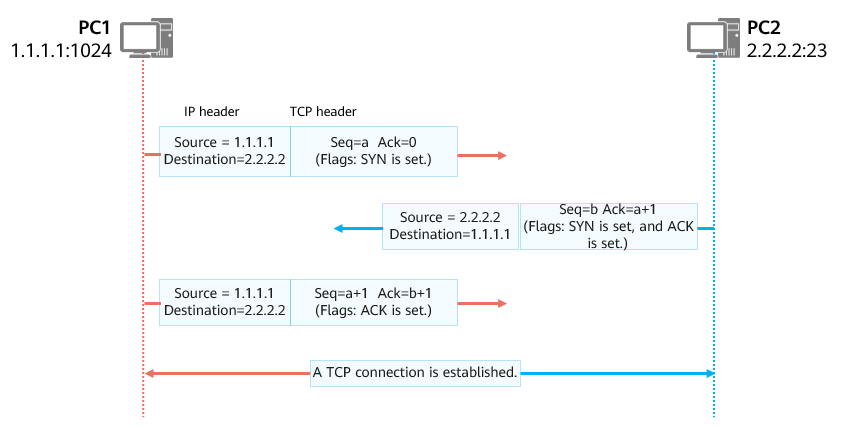
Generally, the source port used by a client is randomly allocated, and the destination port is specified by the application of a server.

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.



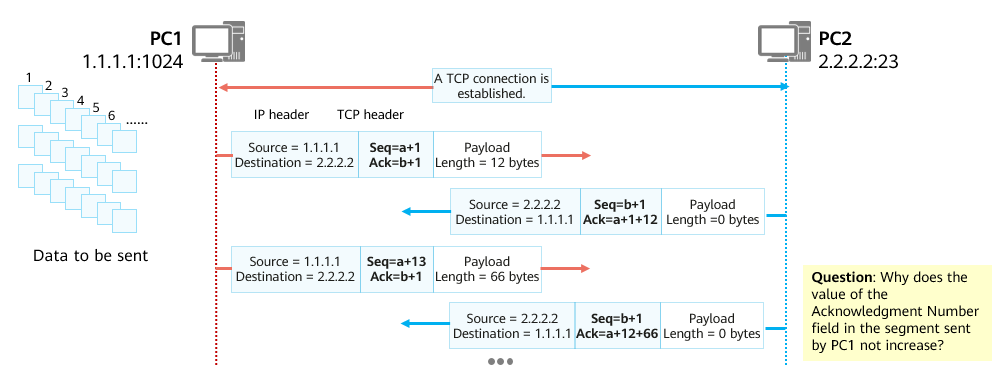
TCP Connection Setup - Three-Way Handshake

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.



TCP Sequence Number and Acknowledgment Number

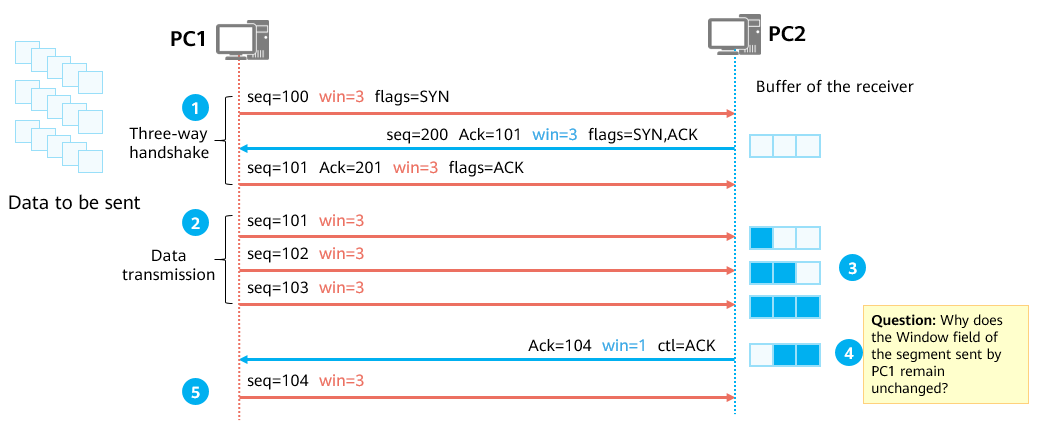
Assume that PC1 needs to send segments of data to PC2. The transmission process is as follows:

* 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.
* PC1 uses the number of the first byte of each segment of data as the sequence number and sends out the TCP segment.
* 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)
* 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.



TCP Window Sliding Mechanism

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.

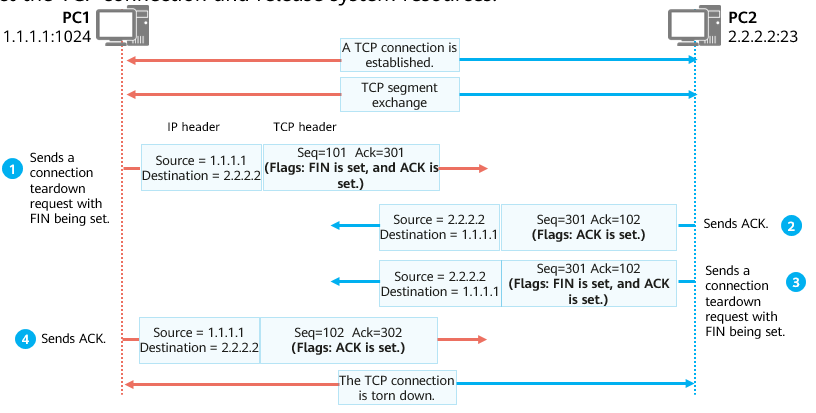
3: After receiving the data, the receiver stores the data in the buffer and waits for the upper-layer application to obtain the buffered data. After the data is obtained by the upper-layer application, the corresponding buffer space is released.

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 Shutdown - Four-Way Handshake

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.

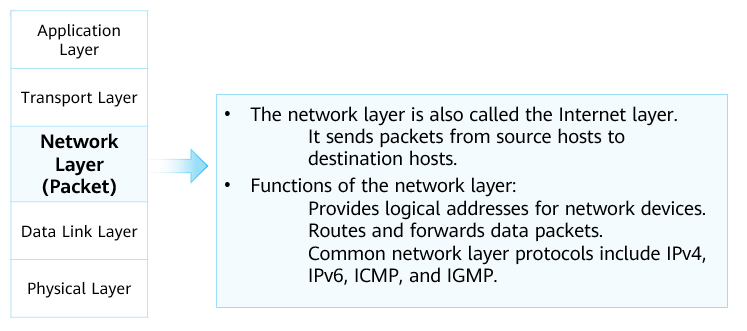
3: PC2 checks whether data needs to be sent. If so, PC2 sends the data, and then a TCP segment with FIN being set to close the connection. Otherwise, PC2 directly sends a TCP segment with FIN being set.

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.

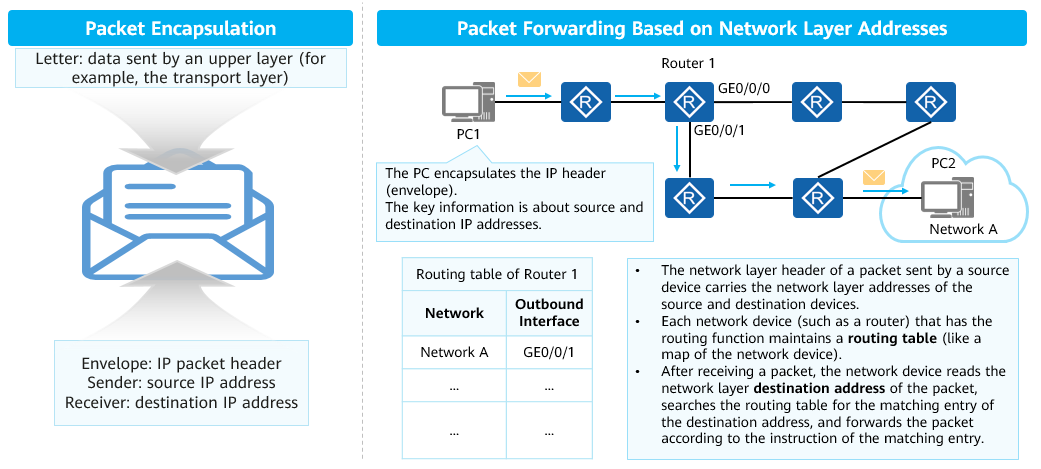
PDUs transmitted at the network layer are called packets.



Network Layer

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

### Working Process of a Network Layer Protocol



Working Process of a 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.

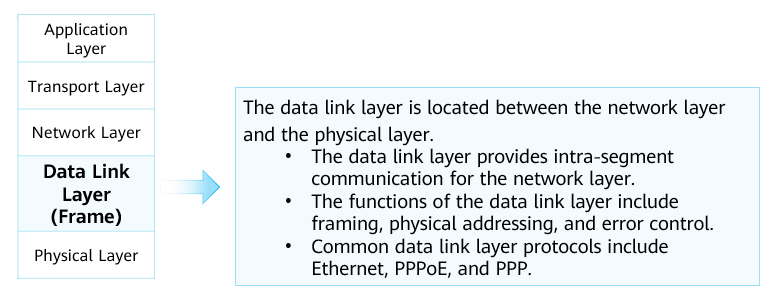
When the IP packet reaches the destination host, the destination host determines whether to accept the packet based on the destination IP address and then processes the packet accordingly.

* 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

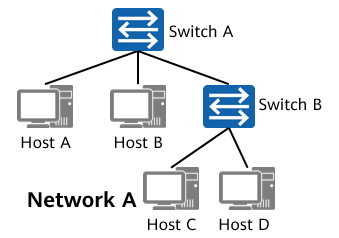
The data link layer is located between the network layer and the physical layer and provides services for protocols such as IP and IPv6 at the network layer. PDUs transmitted at the data link layer are called frames.

Ethernet is the most common data link layer protocol.



Data Link Layer

### Ethernet and Source MAC Addresses

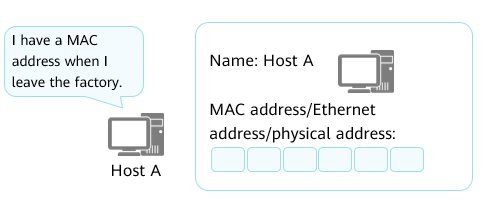


Ethernet Definition

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.

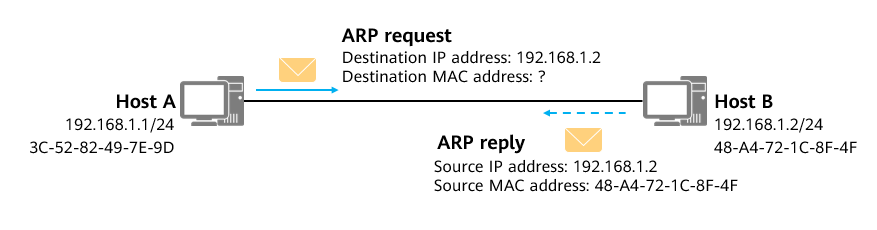
A device that works at the data link layer, such as an Ethernet switch, maintains a MAC address table to guide data frame forwarding.

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.



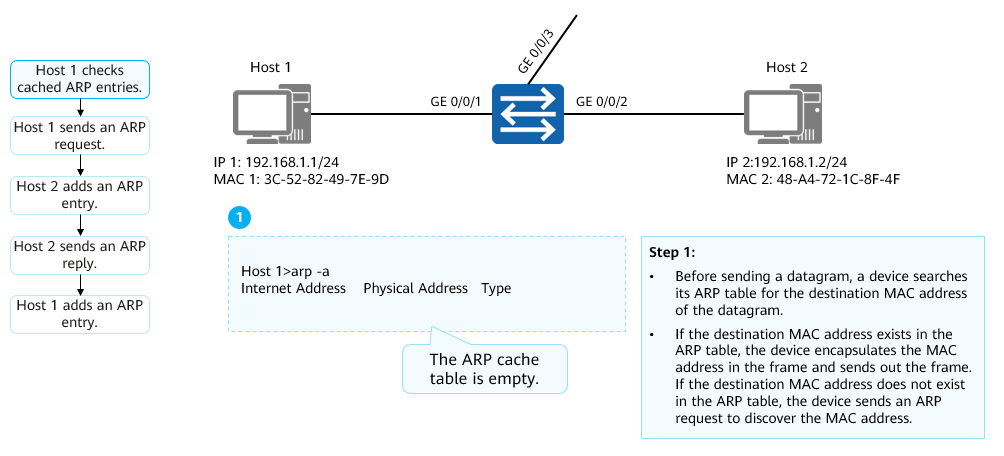
ARP

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)



ARP Implementation Principles (1)

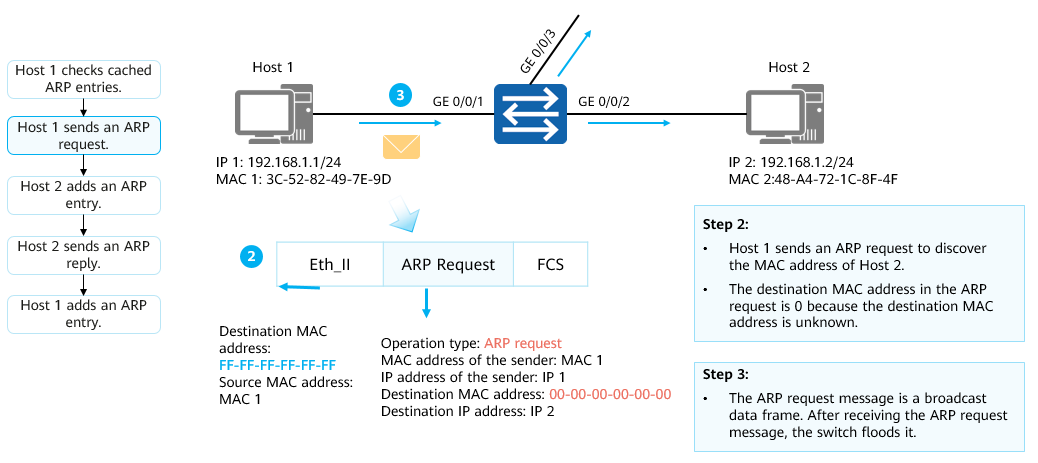
Generally, a network device has an ARP cache. The ARP cache stores the mapping between IP addresses and MAC addresses.

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.

ARP Implementation Principles (2)



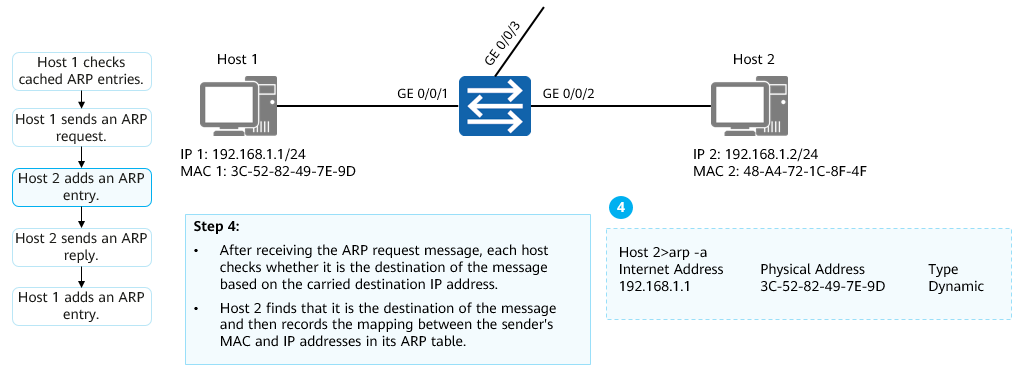
ARP Implementation Principles (2)

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.

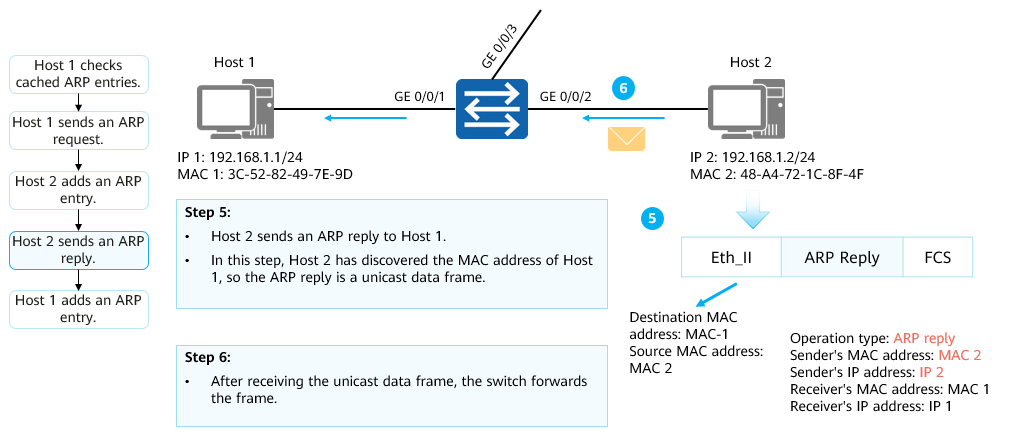
ARP Implementation Principles (3)



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)



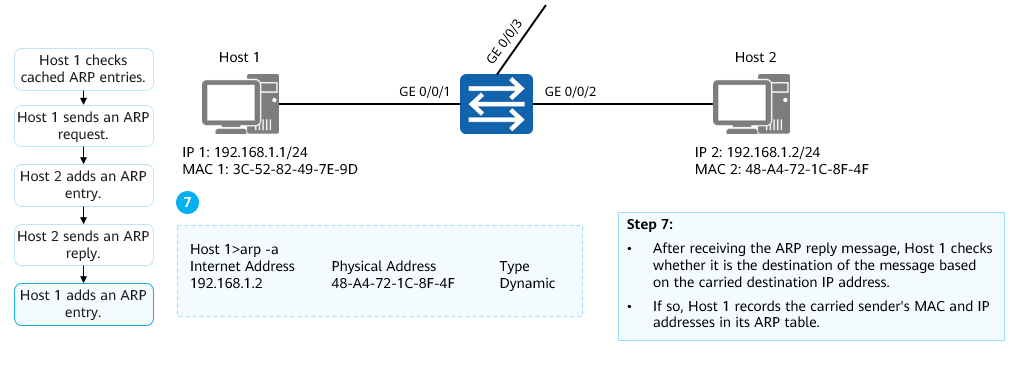
ARP Implementation Principles (4)

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)



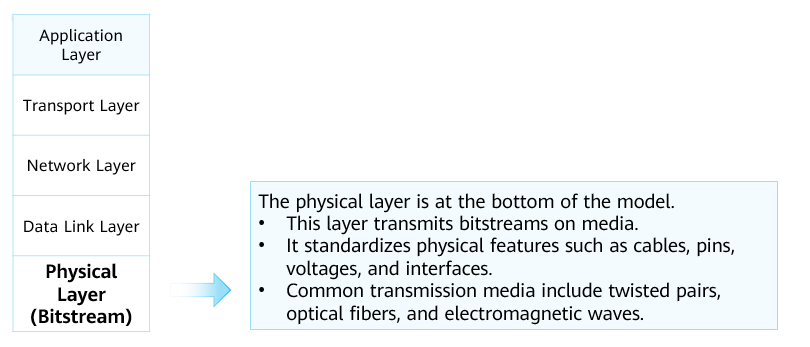
ARP Implementation Principles (5)

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.

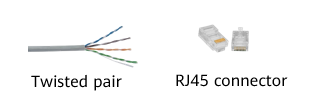
PDUs transmitted at the physical layer are called bitstreams.



Physical Layer

### Common Transmission Media

Data transmission through twisted pairs:



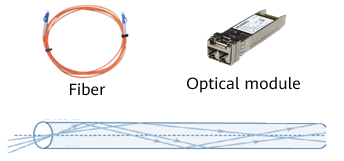
Data transmission through twisted pairs

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

Data transmission through optical fibers:



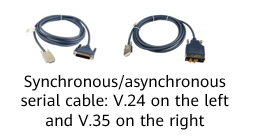
Data transmission through optical fibers

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.

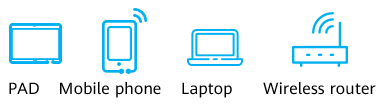
Data transmission through serial cables:



Data transmission through serial cables

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.

Data transmission between terminal and wireless routers through wireless signals:

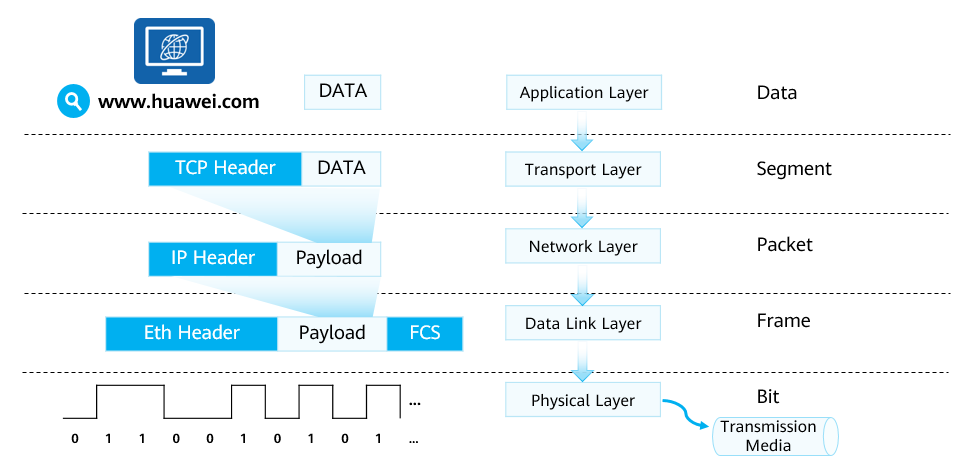


Data transmission between terminal and wireless routers through wireless signals

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.

## Data Communication Process

### Data Encapsulation on the Sender



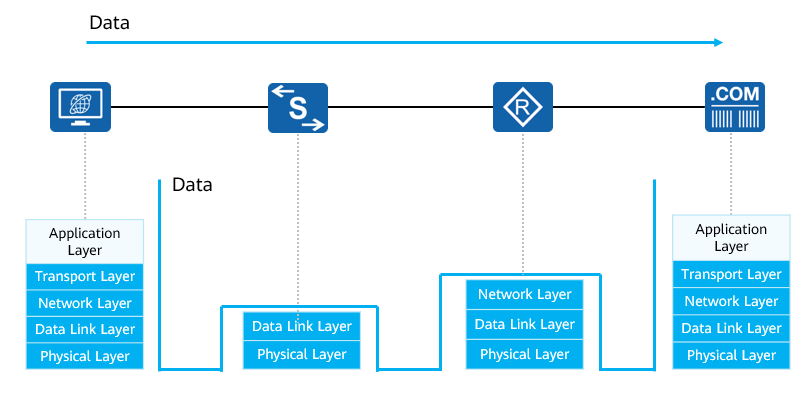
Data Encapsulation on the Sender

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.
6. Ethernet is used as the data link layer protocol. Therefore, after the IPv4 module completes encapsulation, it sends the packet to the Ethernet module (such as the Ethernet NIC) at the data link layer for processing.
7. After receiving the packet from the IPv4 module, the Ethernet module adds the corresponding Ethernet header and FCS frame trailer to the packet. At this layer, the PDU is called a frame.
8. After the Ethernet module completes encapsulation, it sends the data to the physical layer.
9. Based on the physical media, the physical layer converts digital signals into electrical signals, optical signals, or electromagnetic (wireless) signals.
10. The converted signals start to be transmitted on the network.

### Data Transmission on the Intermediate Network

Encapsulated data is transmitted on the network.

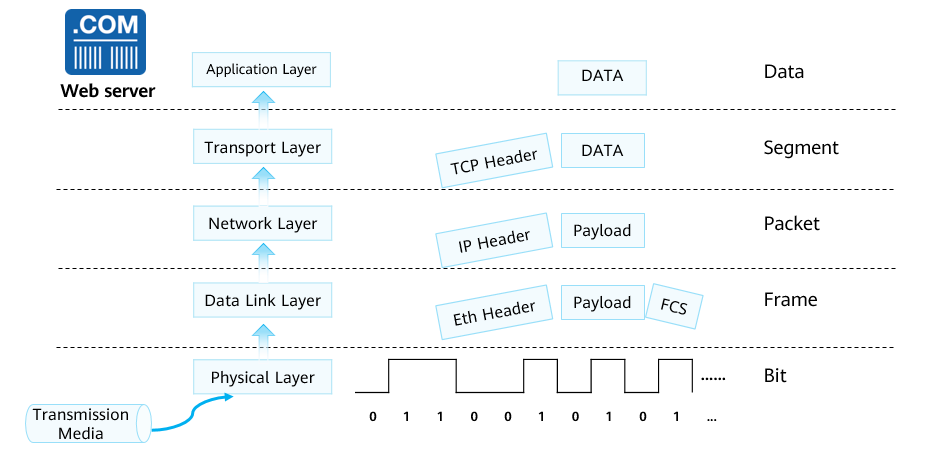


Data Transmission on the Intermediate Network

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



Data Decapsulation on the Receiver

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.

## Quiz

1. (Single) Which of the following organizations is not a common protocol standardization organization? ( )
2. IETF(Internet Engineering Task Force)
3. IEEE(Institute of Electrical and Electronics Engineers)
4. ISO(International Organization for Standardization)
5. IEC(International Electrotechnical Commission)
6. (Single) Which of the following transport-layer protocols is HTTP based on? ( )
7. TCP 80
8. TCP 23
9. TCP 25
10. UDP 69
11. (Multiple) Which of the following protocols are transport-layer protocols? ( )
12. TCP
13. FTP
14. UDP
15. HTTP
16. (True or false) IP and MAC addresses must be encapsulated for communication on a network. ( )
17. True
18. False
19. (True or false) ARP Reply packets are broadcast. ( )
20. True
21. False
22. What are the benefits of the layered model?
23. What are the common protocols at the application layer, transport layer, network layer, and data link layer?

## 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.