R1. What is the difference between a host and an end system? List several different types of end systems. Is a Web server an end system?

R2. The word protocol is often used to describe diplomatic relations. How does Wikipedia describe diplomatic protocol?

R3. Why are standards important for protocols?

R1

1. Different references

"Terminal" generally refers to the personal computer operated by the user on the network. It is a term generated from the original computer network. Strictly speaking, it does not include relay equipment such as LAN switches and routers. In a system where many people use a mainframe computer in the middle, the device of the mainframe computer used by each user is called a terminal. At present, personal computers are usually called terminals.

"Host computer" refers to the mainframe computer used by the terminal, which comes from the original meaning of the English word "host", namely "service provider". However, in the Internet world, whether large or small, all the computers that make up the network are called hosts. At present, all computers with IP addresses are generally referred to as hosts.

2. Different classification

Host: divided into computer host, Internet host and mini computer host.

Terminal: at present, common client devices are divided into two categories: one is fat client and the other is thin client. Then, the more powerful devices based on open industrial standard architecture represented by PC are called "fat client", and others are classified as "thin client". The space and scale of thin client industry are also large, which is no less than the current scale of PC.

In the top - down, the host is equivalent to the end system, and the two are unified in concept

Computers, smart phones and game consoles connected to the Internet all belong to end systems

The web server also belongs to the end system

R2

The term "agreement" has two meanings. In the legal sense, it is defined as an international agreement to supplement or modify a treaty. In the diplomatic sense, the term refers to a set of rules, procedures, conventions and rituals related to relations between states. Generally speaking, etiquette represents a recognized and generally accepted international etiquette system.

R3

The standard protocol can take effect, and the end system can communicate based on the standard established by the protocol

P6

Obtain the HTTP/1.1 specification (RFC 2616). Answer the following questions:

a. Explain the mechanism used for signaling between the client and server to indicate that a persistent connection is being closed. Can the client, the server, or both signal the close of a connection?

b. What encryption services are provided by HTTP?

c. Can a client open three or more simultaneous connections with a given server?

d. Either a server or a client may close a transport connection between them if either one detects the connection has been idle for some time. Is it possible that one side starts closing a connection while the other side is transmitting data via this connection?

Explain.

a. Unless the connect header of the request contains a "close" tag, the HTTP / 1.1 server can always assume that the HTTP / 1.1 client wants to maintain a persistent connection. If the server wants to close the connection immediately after sending the response, it should send a header field containing "close".

This may include the HTTP connection header field and whether you want the server to keep the connection header field open / 1. If the client does not want to maintain the connection for more requests, it should send a header field with a value of "close".

If the client with the "close" request is the last one sent by the server.

Therefore, either the client or the server can signal that the connection is closed.

b. The HTTP protocol itself is not encrypted and uses TCP port 80.

HTTPS protocol uses SSL encryption algorithm and TCP 443 port.

The communication content of HTTP is encrypted through the combination with SSL (secure socket layer) or TLS (Transport Layer Security)

HTTPS adopts mixed encryption (public key + shared encryption). When the key can be exchanged reliably, shared encryption is used.

Encryption and decryption use a key, which is passed to the pair. The key is in danger of leakage, but the speed is faster than the public key.

c. No, two at most.

d. One end is closed and the other end cannot transmit data through the connection.

Therefore, the client software is required to reopen the transport layer connection and retransmit the abandoned request sequence without user interaction.

P12

Write a simple TCP program for a server that accepts lines of input from a client and prints the lines onto the server’s standard output. (You can do this by modifying the TCPServer.py program in the text.) Compile and execute your program. On any other machine that contains a Web browser, set the proxy server in the browser to the host that is running your server program; also configure the port number appropriately. Your browser should now send its GET request messages to your server, and your server should display the messages on its standard output. Use this platform to determine whether your browser generates conditional GET messages for objects that are locally cached.

from socket import \*

serverPort = 12000

serverSocket = socket(AF\_INET, SOCK\_STREAM)

serverSocket.bind(("", serverPort))

serverSocket.listen(1)

print("The server is ready to receive")

while 1:

connectSocket, addr = serverSocket.accept()

sentence = connectSocket.recv(1024)

print(sentence.decode())

connectSocket.close()