Physical Layer

Although there are many points of knowledge involved, but I think the focus is the modem

demodulator Data Received (data) to turn the analog signal into a digital signal.

Because the phone line transmits analog signals, the modulator converts digital signals to analog signals for the data that will be sent.

As for analog and digital signals, my understanding is that the signals transmitted on the link are really analog signals, but this analog signal simulates a digital signal, which means that the analog signal is processed as a digital signal.

There are several ways to reuse channels. respectively, time division multiplexing, statistical time Division multiplexing, Code Division multiplexing, frequency division multiplexing. Time Division multiplexing is a bit like RR.

Hub: The main function of the hub is to regenerate and reshape the received signal to enlarge the transmission distance of the network, and to focus all nodes on the node that is centered on it. It works on the physical layer. That means he can't choose the path, he just amplifies the signal. function is very simple. The job is simple. Hubs can only connect machines with the same rate. These are either 10M or 100M .

Expand：

Digital signal in the physical layer transmission, is essentially a digital signal or analog signal, why?

[https://www.zhihu.com/question/29244850/answer/107289428](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.zhihu.com%2Fquestion%2F29244850%2Fanswer%2F107289428)

Data Link Layer

The unit of data sent by this layer is called frame, and frame is actually the data link layer that adds a piece of data to the end of the data from the network layer. is the frame header ( left , SOH) and frame tail ( right , EOT) .

One of the roles is to differentiate the start and end of frames

The link layer protocol provides:

data portion of frame ( data from the previous layer ) Maximum length of (MTU) .

Transparent transmission: Character Filling method

Reliable transfer: Error detection ( redundancy check CRC) actually the data part is added a redundant code, so there is a problem written above, not on the upper end of the data to add directly to the end, but first divided into groups ( group first because there are limits for maximum length ) , and then add at the end of the data N bit redundancy code, and then add the end and end, this is called the frame.

But I do not understand the specific method of honor detection. After that there is a need to learn.

Flow control:

Bandwidth difference, if send fast receive slow data will be lost. So consignee control the speed of the hair side.

the acknowledgement and retransmission mechanism. After the receiver receives the correct (redundant validation) frame, there is a feedback signal (ACK), and the sender then sends the next frame. If you receive a malformed frame that returns a Nak , the sender receives The data in the cache after the NAK.

If the receiver does not have a feedback signal for a certain period of time, the data is lost and automatically retransmission.

Return signal loss also retransmission, because the sender can not tell whether the return signal is lost or the data did not send the past. Anyway, the timeout timer is retransmission when the signal is confiscated.

To solve the problem of repeating frame , add ordinal number ( is estimated to be added to the frame header ) , ordinal only 0 and 1 represents ( means only 1 bit)

protocol: PPP ( Point-to-Point Protocol ) apply between any two physical devices

The above frame encapsulation, redundancy check, confirm retransmission and so on in this agreement has the detailed stipulation. For example, the placeholder for a redundant checksum, in the PPP Protocol, provides a detailed account of what escape characters are used as placeholders. It also specifies what the start and end symbols are. It also has the maximum length of the frame, and it checks the link in a few minutes . ( Data Link protocol LCP-- to establish, configure, test link methods, Control the node on the link ( switch?) ), which is physical and is physically connected by holding the link. ).

system Mark an address that identifies the Internet device.

Data compression

protocol: Peer-to-peer ( peer calculation ) include LCP and NCP

NCP the is a network control protocol. Logically control node ( router ).

PPP the frame of the, PPP is byte-oriented ( Minimum bytes ) , so all frames are integer bytes



F : Flag field, equivalent to SOH .

A : Address field, the network layer is now idle.

C : Control Fields

protocol: Because PPP the can be compatible with any protocol up, so what you write here depends on the top.

FCS : Test sequence, or redundancy code. It appears that the redundancy code is not written in the IP datagram.

F : Flag Fields

PPP to differentiate between frame and end and IP Datagram ( transparency ) , come up with two methods. is the character padding method and the 0 bit padding respectively.

PPP character Fill

completed by hardware, 0x7E Go 0x7d and 0x5e . 0x7d to 0x7d and 0x5d. The control character is preceded by a 0x7d and the encoding of the control character is changed.

PPP 0 bit padding

The sender found a 5 contiguous 1 Replace with 0. when the receiver finds five consecutive 1 then the 1 Delete.

Key: 802.3 The standard divides the data link layer into two tiers, logical link control, respectively (LLC) and media access control (MAC) .

but the device manufacturer does not care LLC layer, but incorporating logical controls into the MAC layer.

Nic called Communication adapter

1 Serial parallel conversion is the transport layer of the IP The datagram is encapsulated in frames.

2 Caching Data ( traffic control, reliable transfer)

3 in Windows The driver is installed inside, which is actually to Windows The provides a control interface.

4 Implementing an Ethernet protocol is actually implementing PPP protocol.

Ethernet：

Station the concept of.

Data link layer in the case of Ethernet, there is no retransmission, there is no need for frame numbering.

detect data to the previous level to manage ( network layer? Transport floor? Application layer? )tosend a signal to the sender if the previous layer needs to be charged. In this retransmission mechanism, in fact, the data link layer is a fool, it only do data sending and receiving, even if the data resend it does not know, because it does not detect data.

Multi-point access: Multiple computers connected to a bus.

Carrier monitoring: Before sending data with electronic technology to detect if there are other computers in the bus to send signals. Do not send, avoid collisions .

collision: The signal on the bus is distorted when the collision occurs. Unable to recover valid information from the signal. The maximum retransmission is repeated after the collision times ( binary exponential type avoidance algorithm)

Enhanced collision: After a collision, send interference signals, so that all computers on the bus know that a collision occurred.

Ethernet Regulations typically less than byte data is an invalid frame terminated unexpectedly because of a collision

Using hubs to extend Ethernet

the channel utilization calculation (the longer the frame, the lower the delay bandwidth product, a the smaller the value of the. The channel utilization is also higher at this time)

mac Address The ( name management of the physical device during transmission. ) The address mentioned here is actually a first name or identifier. the Standard stipulates that the MAC address is 48bit. For convenience, use the to represent the mac address. The first three systems are manufacturer identifiers. The latter three are expanded. The last 6 is used to determine the specific machine's ?( before 6 bits are used to mark specific vendors, after 6 The bit is used to mark specific products. "Someone on Baidu said that)

Route has two mac address, other device is a mac address. A network adapter corresponds to a mac address with two network adapters routed.

Network card: Received mac after the frame, first see if it is sent to the station. If not, discard. If you are sending a to this site ( , for example, to a different host attached to your network or to another route, ) , accept it. And then do other processing.

There are three kinds of frames sent to this site:

Tan: One-to-one (I think the application SDN becomes Tan)

Broadcast frame: A pair of all

Multicast frames: One-to-many

mac Frames and PPP Frame Differences

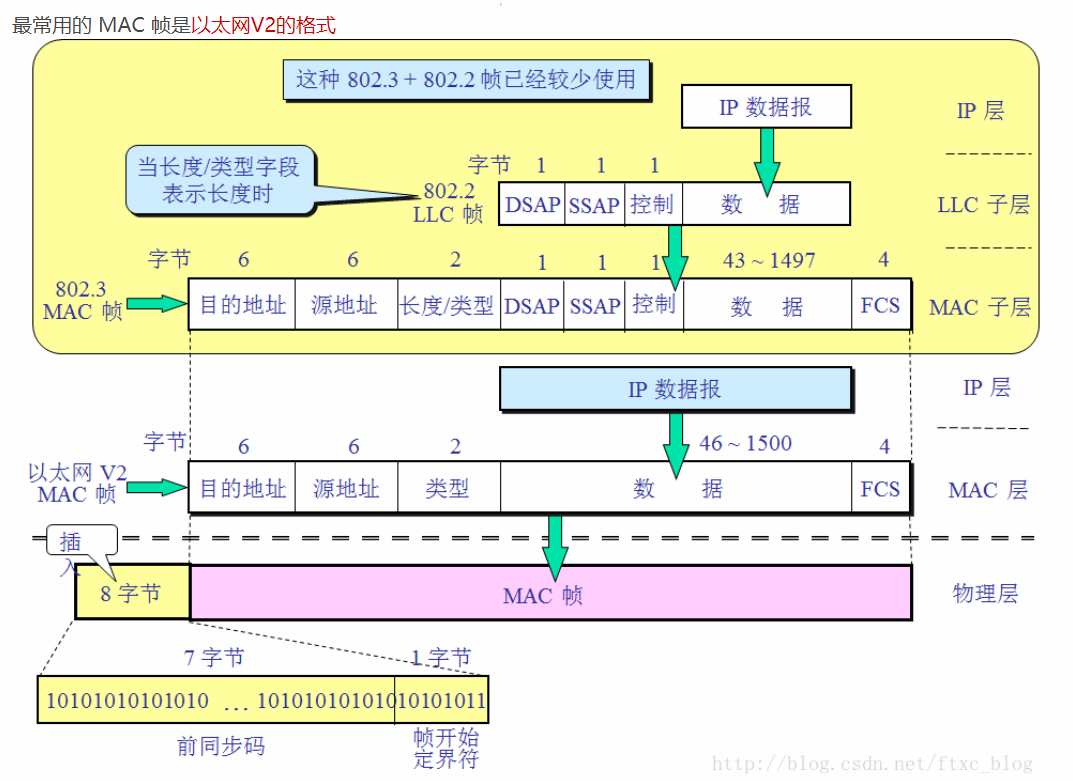
here mac frames exist on Ethernet, and PPP the frame is a wide area network. A wide area network is a IP address-addressed (IP address is the addressing mechanism of the network layer ), but the local area network has its own addressing mechanism , the MAC address is used internally on the LAN for addressing ( link layer ) .

PPP is in the area of Wan, MAC is a LAN category, depending on the actual situation and the environment to choose a different protocol, PPP the supported network structures can only be point-to-point, mac the supports multiple point-to-point.

In Ethernet mac , remote words are used PPP (such as ADSL dialing is based on PPP ).

Ethernet Encapsulation and PPP encapsulation is all about IP Encapsulation of Layers

here mac frames are actually in PPP Frames are added to the beginning and end of the frame to make up the mac frame.



Type field (2 bytes):

The is used to flag what protocol is used on the previous layer so that the received MAC The data on the frame is given to the previous layer of this The protocol. In fact, for upward compatibility. ( But I guess it only works by letting the next machine that receives this frame to determine which protocol frame I'm following. Because the format is different for the data interpretation rules is not the same. (It's like coding, but it's like coding?) ))

data fields (46-1500):

official name is MAC Customer data field Minimum length bytes -18 header and tail of bytes = data Field Minimum length. The minimum length is the byte, because the minimum byte required for transmission is the?, with the end added , so the minimum data field is . The valid length is 64~1518. More than that.

FCS Fields (4 bytes):

when the length of the data field is less than byte, you should add the integer byte fill field after the data field to ( guaranteed Ethernet MAC frame length not less than bytes ( The video says this is a redundant check sequence, I think this is more reliable, because you can not populate only 4 bytes Ah, + plus 4 is not equal to ,.)

inserted before the frame 8 the first field in the byte is a total 7 bytes, a front sync code, used to quickly implement MAC the bit synchronization of the frame. The second field is the frame start delimiter, which means that the following information is the MAC frame. It is important to note that the8 byte does not belong to the mac frame.

if mac frame is not valid ( is not an integer number section, frame length does not meet the requirements,FCS detect ) , the frame is discarded directly. the Ethernet does not require the receiving side to send confirmation frames. is not confirmation. ( does the Ethernet have no flow control?) Or is it that the retransmission is already a flow control?)

the minimum interval between frames is 9.6us , which is the time of the contention period. It is also the time to send 96bit data, on the one hand, to verify that the other party is receiving the data correctly ( does not return frames, so how do you implement the flow control?) Does it have to be transmitted correctly as long as there is no collision? Obviously not, so if the frame is invalid, how do you know if the sender should not retransmit it? )and, on the other hand, a time to process frames on the receiving end.

Hub: Half-duplex ( crash abort send)

Physical Layer mac frame. When more than one hub builds a network, the collision domain becomes larger, one station sends the message, and all The stations on the hub are broadcast. multiple hubs are actually a single bus.

Network Bridge: Half-duplex ( crash abort send)

Data Link Layer mac frame, get mac after the frame is not broadcast, the destination address is resolved first, and then the destination mac address one-to-one send mac frame.

Maintain a table

|  |  |
| --- | --- |
| Station Address ( all mac addresses of machines connected to the bus) | Port ( Network Bridge is a total of two ports, so the port number is not 1 is 2) |
|  |  |

The network Bridge replaces the hub. A hub is the equivalent of a bus, but the line that the network Bridge pulls out is the bus.

Switch: Full-duplex ( No collisions, one bus per station)

VLAN ( virtual LAN ) because each PC exclusive of a single bus, so logically built VLAN .

in detail, in the mac insert another between the original address and the type of the frame 4 a fragment of the byte. Called the vlan tag (tag), the switch uses this tag to know which station this piece of information belongs to. It is worth noting that, even if you insert the 4 byte fragments, not the original 46~1500 conflict. The minimum number of bytes or 46~1500.

Carrier Extension ( only half duplex 1000M Network is used, expand mac frame, min ? bytes ( original )

Group Bursts ( extends only the first frame, followed by 0.96us , even if the data is together. There is no need for a separate carrier extension)

Network layer

Virtual Circuit Service: X.25 Protocol

Flow Control is responsible for the network ( routers are responsible? )

virtual circuit number exists X.25 Grouping Header

Datagram Services: IP Protocol (TCP/IP One of the protocol systems)

Flow Control the is responsible for both the sender and the receiver. the ( , which was previously learned to confirm the retransmission mechanism, does this not by routing but by the PC ( network card ).? )

IP Protocol There are three protocols in use, respectively

Address Resolution Protocol (ARP) , reverse Address Resolution Protocol (RARP) : For backward compatibility

Internet Control Message Protocol (ICMP) , Internet Group Management Protocol (IGMP) : for up compatibility

Address Resolution Protocol is based on IP Address get to mac address.

Leverage over the network layer IP address addressing, under the data link layer mac address addressing.

IP Pre -Datagram The byte is a fixed part.

**version** :

IP The version of the protocol, current IP protocol version number is 4 , Next Generation IP protocol version number is 6 .

**Header Length:**

IP the length of the header. the sum of the length of the fixed part ( byte) and the variable part. A total of 4 bits. The maximum is 1111, that is, ten on , representing IP the maximum length of the header can be 32bits ( 4 bytes), and also The is the maximum 15\*4=60 byte, excluding the length of the fixed part bytes, The maximum length of the variable part is the ? byte.

**Service Type** :

Type of Service .

**total length** :

IP The total length of the message. The sum of the length of the header and the length of the data part.

**Identity** :

The uniquely identifies each datagram sent by the host. Usually every message is sent, its value plus one. When the IP message length exceeds the MTU(maximum transmission Unit) of the transport network , the value of this identity field is copied to the the identifies fields for all data fragments so that the fragments can be made back to the original data in accordance with the inside of the identity field when they reach their final destination .

**Flag** :

Total 3 bit. R,DF,MF three bits. Currently only two digits are valid,DF bit: to 1 to indicate no fragmentation, to 0 to Express fragmentation. MF: "more slices" for 1, and for 0 to indicate that this is the last piece.

**Slice offset** :

The offset shift in the original data message relative to the first. (it needs to be multiplied by the 8).

The relative position of a piece in the original group after fragmentation. In other words, relative to the **user data field** , start the? point where the slice starts. Slice offsets are offset units in 8 bytes. That is, the length of each fragment must be a number of times The is an integer of 8 bytes (? ).

calculation: The first byte of each datagram is the original datagram ( Transport Layer ) the first byte of the. If this is the 0 Byte, then the slice offset is 0/8=0. If 1400/8=175.

**Lifetime** :

IP The maximum number of routers that the message is allowed to pass through. For each router,TTL minus 1, when 0 , road The datagram is discarded by the device. the TTL field is initially set by the sender with a 8 bit field . recommended initial values by points The assign number RFC Specifies that the current value is ?. when you send a ICMP Echo reply, you often set the TTL to the maximum 255.

**Protocol** :

indicates IP The message carries data using that protocol so that the destination host's IP The layer knows to put the datagram on which process to hand (different protocols have specialized process processing). Similar to the port number, where the protocol number is used, the protocol number of TCP is 6, andUDP is . The protocol number for ICMP is 1, andIGMP has the protocol # 2.

**Header Checksum** :

Calculation IP checksum of the head, checking IP the integrity of the header.

**source IP Address** :

Identity IP the source-side device of the datagram.

**Purpose IP Address** :

Identity IP the destination address of the datagram.

ICMP : is a connectionless protocol, Network Layer Protocol

[http://blog.csdn.net/tigerjibo/article/details/7356936](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Ftigerjibo%2Farticle%2Fdetails%2F7356936)( must see)

ICMP Yes ( Internet Control Message Kyoto ) Internet Control [message](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E6%258A%25A5%25E6%2596%2587) protocol. This is a child protocol for the [TCP/IP protocol family](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FTCP%2FIP%25E5%258D%258F%25E8%25AE%25AE%25E6%2597%258F) , for the IP [host](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E4%25B8%25BB%25E6%259C%25BA) , [Routing](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%25AF%25E7%2594%25B1) To pass control messages between the controllers. Control message means [network access](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25BD%2591%25E7%25BB%259C%25E9%2580%259A) No, [host](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E4%25B8%25BB%25E6%259C%25BA) Whether the [Route](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%25AF%25E7%2594%25B1) is available, and so on, is the message for the network itself. Although these control messages do not transmit user data, they play an important role in the transfer of user data.

When you encounter IP data cannot access targets, IP [Router](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%25AF%25E7%2594%25B1%25E5%2599%25A8) cannot forward at current transfer rate [packets](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E6%2595%25B0%25E6%258D%25AE%25E5%258C%2585) , and so on, automatically sends ICMP message. ICMP message in IP Frame Structure Header **Protocol** **( can be found in the above diagram, altogether 8bit)** Type field (Kyoto 8bit) The value of =1.

as shown in the following illustration, ICMP package has a 8 the header of a long byte, where the previous 4 bytes are fixed formats that contain 8 bit Type field, 8 bit code fields and bit checksums; 4 byte based on ICMP The type of the package and takes a different value.

we often use them on the network ICMP protocols, such as those we use frequently to check for network access [Ping](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FPing) Command ( Linux and Windows ), this Ping the procedure is actually ICMP the process of protocol work. There are other [network commands](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25BD%2591%25E7%25BB%259C%25E5%2591%25BD%25E4%25BB%25A4) ( [tracking Route](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%259F%25E8%25B8%25AA%25E8%25B7%25AF%25E7%2594%25B1) ) The Tracert command is also based on the ICMP protocol.

ICMP when a transmission error is used as a normal IP the data is transmitted. Only the Protocol field is 1, and the receiving side sees this 1 and knows that this message is an error message for ICMP , instead of user data. But whether the error message or user data, they are in the transmission process is no difference. Only after receiving this message, there is a difference in the parsing process of the message.

type is divided into two types : Error message, inquiry message

error message: Terminal unreachable, Source station suppression, time exceeded, parameter problems, changing routing ( redirect ) .

Internal Gateway Protocol (IGP): RIP , OSPF , is , IGRP , EIGRP .

External Gateway Protocol (EGP): only BGP-4

Routing Algorithm :

[http://blog.csdn.net/lpjishu/article/details/52413919](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Flpjishu%2Farticle%2Fdetails%2F52413919)

[http://blog.csdn.net/qq\_33936481/article/details/54379818](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fqq_33936481%2Farticle%2Fdetails%2F54379818)

RIP Protocol (UDP message transfer ) :

[http://blog.csdn.net/lycb\_gz/article/details/1612254](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Flycb_gz%2Farticle%2Fdetails%2F1612254)

with **Transport Layer** make **routing Table** Transport OF, **RIP message Format** The format is as follows.

[Http://blog.sina.com.cn/s/blog\_c079d59e0102wgn9.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.sina.com.cn%2Fs%2Fblog_c079d59e0102wgn9.html)

RIP maximum message length is bytes. RIP message headers occupy 4 bytes , and each route entry takes up a eight-bit group byte. So , the maximum RIP message is 4+ (25\*20) =504 bytes , Plus 8 bytes UDP header , so RIP datagram size ( without IP Package Header ) Up to a maximum of bytes.

The routing token is the number of the autonomous system, which is designed to filter out routing information outside the autonomous system. (Routing information for other autonomous systems may also be transmitted.) ）

OSPF Protocol (IP Datagram Transport ) :

[http://blog.csdn.net/qq\_16811963/article/details/52144299](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fqq_16811963%2Farticle%2Fdetails%2F52144299)

[http://blog.csdn.net/ztguang/article/details/70949781](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fztguang%2Farticle%2Fdetails%2F70949781)

Use IP The datagram transmission.

OSPF Datagram format:

Version number:

This field indicates OSPF the current version number of the. The most recent version is 2. Version 1 and version 2 are not compatible.

Type:

This field indicates that the column appended to the group header is OSPF Grouping 5 which of the types.

Group length:

This field contains the entire OSPF The length of the group, which includes the OSPF header.

Routers ID:

This field contains 4 bytes IP address. The router ID is used to uniquely identify the router in the autonomous system. for a Cisco router, this field contains the largest of this router (highest ) IP address. If you set the loopback address (loopback) with, the largest loopback address becomes the router ID . after the router ID is selected by, it will not change until the router restarts and is selected as the router ID The interface for is closed,, or the IP address on this interface has been deleted or superseded.

Area ID:

The This field specifies the area number to which the grouping belongs. This is also a 4 byte number. In order to form a neighbor relationship, its value must be the same on both sides. There are two ways to write this field: Zone 1 or area 0.0.0.1. There is no difference between the two kinds of books write.

Checksum:

This field contains an entire other than the authentication section that is corrupted by the data OSPF the checksum for grouping.

Autype:

This field contains a certified type code: 0 The indicates no authentication ( NULL authentication ). 1 indicates that the authentication class is of normal text. 2 indicates that the authentication type is MD5.

Certification:

if normal text is authenticated, this The Bit field contains the authentication key. If the message digest is authenticated, the authentication field for the this ? bit is redefined as some other parameter. See Appendix D,RFC2328, understanding close on MD5 More details of the certification scheme.

BGP Protocol (TCP message ) :

[Http://www.360doc.com/content/10/1230/16/2614615\_82680038.shtml](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fwww.360doc.com%2Fcontent%2F10%2F1230%2F16%2F2614615_82680038.shtml)

Support CIDR , so BGP The routing table should have a network prefix and a next hop route, and a destination route The sequence of autonomous systems to pass

IP Multicast (IPV6) : Using Internet Group management protocols IGMP , multicast routing protocol.

[Https://baike.baidu.com/item/%E5%A4%9A%E6%92%AD/6867723?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E5%25A4%259A%25E6%2592%25AD%2F6867723%3Ffr%3Daladdin)

Multicast is IPv6 Packet 's 3 One of the basic destination address types, multicast is a bit of communication to multiple points, IPv6 not adopted IPv4 the multicast terminology in, but rather as a special example of multicast.

**IP** Multicast **(also Multicomputer or** [**multicast**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25BB%2584%25E6%2592%25AD) **) technology, which allows one or more hosts (multicast sources) to send a single** [**packet**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E6%2595%25B0%25E6%258D%25AE%25E5%258C%2585) **of to multiple hosts (one at a time) tcp/** [**IP Network technology**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FIP%25E7%25BD%2591%25E7%25BB%259C%25E6%258A%2580%25E6%259C%25AF) **. Multicast, as a point-to-point communication, is** one of the most effective ways to save [**network bandwidth**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25BD%2591%25E7%25BB%259C%25E5%25B8%25A6%25E5%25AE%25BD) . **In the network audio / Video Broadcast application, when you need to set a** [**node**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%258A%2582%25E7%2582%25B9) **when the signal from is delivered to multiple nodes, it is a serious waste of network bandwidth, whether by means of repetitive point-to-point communication or by broadcast, and only multicast is the best option. Multicast enables one or more multicast sources to packets data only to specific multicast groups, and only hosts joining the multicast group receive packets. Currently,IP Multicast technology is widely used in network audio / Video Broadcast,** [**AOD**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FAOD) **/vod ,** [**Network video conferencing**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25BD%2591%25E7%25BB%259C%25E8%25A7%2586%25E9%25A2%2591%25E4%25BC%259A%25E8%25AE%25AE) **, multimedia remote education, Push technology, such as stock quotes, and** [**virtual reality**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%2599%259A%25E6%258B%259F%25E7%258E%25B0%25E5%25AE%259E) **Games.**

to implement IP Multicast traffic, requiring a between the multicast source and the receiver [Router](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%25AF%25E7%2594%25B1%25E5%2599%25A8) , [hub](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E9%259B%2586%25E7%25BA%25BF%25E5%2599%25A8) , [switch](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E4%25BA%25A4%25E6%258D%25A2%25E6%259C%25BA) and host support required IP multicast. Currently,IP Multicast technology has been widely supported by hardware and software vendors.

Multicast **traffic requires** a multicast source [**node**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%258A%2582%25E7%2582%25B9) **all routers between the and the destination node must provide a pair** of **Internet Group Management Protocol ( IGMP ),** multicast [**Routing protocol**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%25B7%25AF%25E7%2594%25B1%25E5%258D%258F%25E8%25AE%25AE) **, such as PIM , DVMRP , and so on.**

Actually see so much also do not know how to achieve, the world so many computers, is not to share the list of multicast groups around the world? If so, the multicast is not much practical.

Tunneling Technology:

Some routes do not support multicasting, so a multicast datagram is preceded by a unicast datagram, pretending to be a unicast datagram transmitted through this route.

Virtual Address: These address routers do not forward.

VPN: when you want to communicate with hosts on the Internet (require encryption)

[https://baike.baidu.com/item/%e8%99%9a%e6%8b%9f%e4%b8%93%e7%94%a8%e7%bd%91%e7%bb%9c/8747869?fromtitle=vpn& Fromid=382304&fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E8%2599%259A%25E6%258B%259F%25E4%25B8%2593%25E7%2594%25A8%25E7%25BD%2591%25E7%25BB%259C%2F8747869%3Ffromtitle%3DVPN%26fromid%3D382304%26fr%3Daladdin)

NAT: when you want to communicate with hosts on the Internet (no encryption is required)

[Https://www.cnblogs.com/bo083/articles/2170189.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fbo083%2Farticles%2F2170189.html)

**Transport Layer**

**TCP ( Connection-oriented, reliable, ) :**

TCP is the Transport layer protocol in the Internet, using [Three handshake protocol](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E4%25B8%2589%25E6%25AC%25A1%25E6%258F%25A1%25E6%2589%258B%25E5%258D%258F%25E8%25AE%25AE) The establishes a connection.

The connection that is referred to here is a logical connection, and the **router does not know** that the connection was created.

TCP A connection does not mean that an actual or virtual link exists at both ends of the data exchange. It means that both sides of the connection maintain some resources (such as input and output buffers, multiple timers) and link state information, and modify the allocation of these resources through the mutual management of control messages, and provide interface to the user.

[Https://baike.baidu.com/item/TCP/33012?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FTCP%2F33012%3Ffr%3Daladdin) ( TCP Basics on Baidu)

[http://network.51cto.com/art/201411/456783.htm](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fnetwork.51cto.com%2Fart%2F201411%2F456783.htm)( about three handshake and four breakup)

[https://www.jianshu.com/p/ef892323e68f](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.jianshu.com%2Fp%2Fef892323e68f)( about some other details)

[https://www.cnblogs.com/yueminghai/p/6646043.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fyueminghai%2Fp%2F6646043.html)( flow control )( Transport Layer 2, 1 when to around)

[Https://baike.baidu.com/item/Nagle%E7%AE%97%E6%B3%95/5645172?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FNagle%25E7%25AE%2597%25E6%25B3%2595%2F5645172%3Ffr%3Daladdin)( Baidu Nagle)

[http://blog.csdn.net/yuan1125/article/details/51536490](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fyuan1125%2Farticle%2Fdetails%2F51536490)(Nagle algorithm details , combined with actual code)

[https://baike.baidu.com/item/%E7%B3%8A%E6%B6%82%E7%AA%97%E5%8F%A3%E7%BB%BC%E5%90%88%E5%BE%81/6167377 ? Fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E7%25B3%258A%25E6%25B6%2582%25E7%25AA%2597%25E5%258F%25A3%25E7%25BB%25BC%25E5%2590%2588%25E5%25BE%2581%2F6167377%3Ffr%3Daladdin)( confusing window syndrome interpretation and workaround)

[https://www.cnblogs.com/zhaoyl/archive/2012/09/20/2695799.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fzhaoyl%2Farchive%2F2012%2F09%2F20%2F2695799.html)( confused window and Nagle Reference 1)

[http://blog.csdn.net/wdscq1234/article/details/52463952](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fwdscq1234%2Farticle%2Fdetails%2F52463952)( muddled window and Nagle Reference 2)

[http://blog.csdn.net/wdscq1234/article/details/52432095](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fwdscq1234%2Farticle%2Fdetails%2F52432095)( muddled window and Nagle Reference 3)

[https://www.cnblogs.com/yueminghai/p/6646043.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fyueminghai%2Fp%2F6646043.html)(TCP Knowledge Completion)

The data it transmits is called TCP Message Segment

No broadcast and multicast available

Face byte throttling

 After each packet is sent, wait for the other person's confirmation, and then send the next group after receiving the confirmation message. (a bit like a flow control)

There are also timeout retransmissions.

header has bytes.

when applying layers to TCP the layer is sent for transmission across the network using 8 bit-byte representation [Data flow](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E6%2595%25B0%25E6%258D%25AE%25E6%25B5%2581) , TCP The divides the data stream into the appropriate length of the message segment, the maximum transmission segment size ( [MSS](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FMSS%2F3567770) ) The maximum transfer unit of the data link layer of the network that is typically connected to the computer ( [MTU](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FMTU) ). TCP then passes the packet to the IP layer, which is used by the network to pass packets to the receiving entity's TCP layer.

TCP to ensure message transmission is reliable [1] , a sequence number is given for each package, and the sequence number also guarantees the sequential receipt of packets that are delivered to the receiving entity. The receiving entity then sends a corresponding acknowledgment (ACK) to the bytes that have been successfully received, and If the sending end entity does not receive a confirmation within the reasonable round-trip time delay (RTT) , The corresponding data (if lost) will be retransmission.



in data correctness and legality, TCP use a checksum function to verify that the data has errors, to compute checksums when sending and receiving, and to use the MD5 the authentication encrypts data.





In the guarantee of reliability, the mechanism of timeout retransmission and incidentally confirmation is adopted.





Slide window on flow control [1] The Protocol, which provides for retransmission of unacknowledged groupings within a window. https://baike.baidu.com/item/ARQ/7402812



For congestion control, use a popular TCP Congestion Control algorithm (also known as AIMD algorithm). The algorithm mainly consists of three main parts:1) Castian, multiplicative minus,2) slow start, and3to respond to timeout events.

[http://blog.csdn.net/mary19920410/article/details/58030147](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fmary19920410%2Farticle%2Fdetails%2F58030147)

[Https://www.jianshu.com/p/e2dd554279d7](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.jianshu.com%2Fp%2Fe2dd554279d7)

           bit source is a slogan, The is used for the destination port number to find the application process for both the sender and receiver side, plus IP The source end of the header IP and Terminal IP , only one confirmation TCP connection.

           bit ordinal: Identifies the stream of data bytes sent, identifying the first byte of data in the message segment, 2^3-1 Back from 0 start. the ISN (Initial Sequence number)that contains the connection selected by this host, the first data byte ordinal to be sent is isn+1.

           bit Confirmation serial number: ACK to 1 is valid, last successfully received data byte ordinal number +1 (if received as 1024--2048 , returns 2049 ).

           4 bit Header Length: header 32bits number of words, TCP Maximum A The length of the byte, excluding any selected fields, normal bytes.

           6bits : URG emergency pointer; ACK Confirm that the ordinal number is valid; PSH the receiving party should hand over this message segment to the application tier as soon as possible; RST rebuild the connection; SYN a synchronization sequence number to initiate a new connection; FIN The originator completes the send task.

           bit window size: TCP flow control, number of bytes, starting at the value indicated by the confirmation sequence number, the byte expected to be received by the receiving end, maximum is 65535.

           bit checking and: including calculations TCP the header and data synthesis binary inverse code and test and.

           bit emergency pointer: URG to 1 The is valid, the positive offset, plus the Ordinal field value represents the ordinal of the last byte.

           Optional fields: Example: MSS.

**Timeout retransmission time selection ( Transport layer 2,60:00 around)**

[Https://www.cnblogs.com/yueminghai/p/6646043.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fyueminghai%2Fp%2F6646043.html)

**Concrete implementation:**

TCP send a message segment every , set a timer for this segment . as long as the timer is set to the retransmission time but no confirmation has been received , the will retransmit this message segment

**Weighted average round-trip time:**

**Practices:**

TCP the retains RTT a weighted average round trip time for RTTS(This is also known as smooth round trip time), first measurements to RTT Samples , RTTS value is taken as measured RTT Sample Values . after each measurement to a new RTT Sample , Recalculate once RTTS :

**Formula:**

**New RTTS = (1 TNF) x ( old RTTS) + Alpha ( new RTT Samples )**

**Description:**

in-style , 0≤α 1. if Alpha very close to 0 , means RTT value updated slower if you select Alpha is close to 1, to indicate that the RTT value is updated more quickly RFC 2988 The recommended Alpha value is clutch,, 0.125

**UDP ( no connection, unreliable ) :**

**UDP does not have congestion control.**

[**Https://baike.baidu.com/item/UDP/571511?fr=aladdin**](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FUDP%2F571511%3Ffr%3Daladdin)

Use UDP The protocol includes: [TFTP](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FTFTP) , [SNMP](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FSNMP) , NFS , DNS , BOOTP

The data it transmits is called UDP message or User datagram.

Support 1:1 1:n n:n communication.

Only alternate Half-duplex communication is supported

Header only 8 bytes

UDP The has the disadvantage of not providing packet grouping, assembling, and sorting packets, that is, when a message is sent, it is not possible to know whether it arrived safely or completely.

It does not provide message arrival confirmation, sequencing, and flow control functions.

UDP Yes [OSI](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2FOSI) a connectionless Transport layer protocol in the reference Model, which is used primarily for transfers that do not require packet order arrivals, and the inspection and sequencing of packet transmission sequences is done by the application layer [2] ,

UDP the message has no reliability assurance, order guarantee and flow control field, and the reliability is poor. However, because of the less control options for the UDP protocol, the latency is small during data transfer, the data transfer efficiency is high, it is suitable for applications with low reliability requirements, or applications that can guarantee reliability, such as DNS ,TFTP,SNMP , and so on.

the maximum length of the datagram varies according to the operating environment. Theoretically, the maximum length of a datagram including a header is the 65535 byte. However, some practical applications tend to limit the size of datagrams, sometimes to 8192 bytes.

in fact, UDP The chaos of the protocol is rarely present, and is usually only possible when the network is very congested.

1. **Source ports:** Source port number. When you need a reply, use the full when you don't need it.0.   
**2. Destination port:** The destination port number. This must be used when delivering the message at the endpoint.    
**3. Length:** UDP the length of the user datagram, and the minimum value is 8 (header only).    
**4. validation and:** Detect UDP the user datagram is in error in transit. Throw away the wrong.

Pseudo Header:

Port number: 16bit

range of port numbers from 0 to 65535

most TCP/IP implement assign to temporary port number 1024---5000 the port number between. the port number that is greater than 5000 is reserved for other servers.

Socket (Socket, exists only in TCP):

IP Address: Port number

Network Programming API interface abbreviation is also Soket .

TCP Congestion Control : slow start, congestion avoidance, fast retransmission, quick recovery

[http://blog.csdn.net/sinat\_21112393/article/details/50810053](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fsinat_21112393%2Farticle%2Fdetails%2F50810053)( Reference 1)

[https://www.zhihu.com/question/23055347/answer/197672107](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.zhihu.com%2Fquestion%2F23055347%2Fanswer%2F197672107)( Some popular science with reality , Most of the content is trustworthy. )

when Cwnd<ssthresh , the slow start algorithm is used.

when Cwnd>ssthresh , use the congestion avoidance algorithm instead.

when Cwnd=ssthresh , slow start and congestion avoidance algorithms are arbitrary.

Congestion avoidance:

The congestion window grows slowly. That is, each round trip time RTT will send the sender's congestion window CWnd plus 1, instead of doubling. This congestion window grows slowly according to the linear rule.

Slow start:

The congestion window grows slowly. The congestion window doubles after a transmission round. This is the multiplication growth, and the addition of the congestion avoidance algorithm behind the growth comparison.

1. Initial value is maximum segment MSS ( This is the video version of the statement , and online saying differently)

Fast retransmission ( receiver ) :

the requires the receiving party to issue a duplicate acknowledgement immediately after receiving a segment of a disorder. the ( takes precedence over the reverse timeout for the time-out period, which means that the sender can know the data by three duplicate acknowledgement messages before the time-out timer ends. report lost)

Quick Restore ( Sender)

① performs a "multiplication reduction" algorithm when the sender receives three consecutive acknowledgements, and the Ssthresh The threshold is halved. ( video says threshold +3mss) But the slow start algorithm is not followed.

② considers that if there is congestion on the network, it will not receive several duplicate confirmations, so the sender now thinks the network may not be congested. Instead of performing a slow start algorithm at this point, the CWnd is set to the size of the Ssthresh , and then the congestion avoidance algorithm is executed.

Multiplication reduction:

either in the **slow start phase** or in **congestion avoidance phase** , as long as the sender determines that the network is congested (based on the did not receive confirmation, although no packets were received confirming that they might be missing for other reasons, but because it was not possible to determine, the was treated as congestion. Set the slow start threshold to half the size of the sending window when congestion occurs. However , after, set the congestion window to 1, execute the slow start algorithm

**Application Layer**

Domain。

[Https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D/86062?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2F%25E5%259F%259F%25E5%2590%258D%2F86062%3Ffr%3Daladdin)

File Transfer Protocol FTP ( use TCP)

Install FTP Software ( default to Port)

TFTP Protocol ( use UDP)

[Https://baike.baidu.com/item/tftp/455170?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2Ftftp%2F455170%3Ffr%3Daladdin)

[http://blog.csdn.net/zlj\_fly/article/details/40227623](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fzlj_fly%2Farticle%2Fdetails%2F40227623)

Remote Terminal Protocol TELNET Protocol ( In fact, Remote Assistance protocol , using TCP protocol)

NVT format

WWW Protocol

1. HTTP Protocol

[https://www.cnblogs.com/ranyonsue/p/5984001.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Franyonsue%2Fp%2F5984001.html)( detailed , the is well written, I think it is more comprehensive, but there is still a place to fill. )

[https://www.cnblogs.com/li0803/archive/2008/11/03/1324746.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2Fli0803%2Farchive%2F2008%2F11%2F03%2F1324746.html)( The header parameter is explained in more detail)

[https://www.cnblogs.com/TankXiao/archive/2012/02/13/2342672.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fwww.cnblogs.com%2FTankXiao%2Farchive%2F2012%2F02%2F13%2F2342672.html)( detailed 2)

[http://blog.sina.com.cn/s/blog\_4b9b714a01017lwr.html](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.sina.com.cn%2Fs%2Fblog_4b9b714a01017lwr.html)( expand:SQL to inject)

[http://blog.csdn.net/myfuturein/article/details/8046899](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fmyfuturein%2Farticle%2Fdetails%2F8046899)( Expand: Cross-site request forgery)

CGI :

[http://www.jdon.com/idea/cgi.htm#I3](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fwww.jdon.com%2Fidea%2Fcgi.htm%23I3) ( There are some basic explanations)

in fact, for requests made by clients, I do different feedback based on the request type and parameters, and for any request my processing is performed within the server script and does not say write a script for a single function and then use the server script to invoke it. Anyway, I don't quite understand the CGI thing because it's not used.

But there is also a saying on the internet is " Common Gateway Interface , short name CGI . is a physical program that runs on a server and provides an interface to the client HTML page. So in fact , the HTML server script I wrote earlier is a CGI, which is more broadly understood. The first paragraph of the understanding is narrow.

static pages, dynamic pages, active World Wide Web documents

In fact, static pages, dynamic pages and active World Wide Web documents these three kinds of distinctions are not obvious. Now a page it is dynamic and active.

Web Information Retrieval

is a popular reptile, the principle is very simple, so dozens of lines of code can write a simple crawler. But good crawler algorithms are complex, like the bottom of Google.

SMTP Protocol ( to send mail,TCP Protocol)

[http://blog.csdn.net/kerry0071/article/details/28604267](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=http%3A%2F%2Fblog.csdn.net%2Fkerry0071%2Farticle%2Fdetails%2F28604267)

SMTP Use TCP Port

Cannot send . EXE

message content can only be ASCII Code

Limit Message Length ( include attachments)

MIME Protocol ( supplemental SMTP Protocol)

POP Protocol ( to receive mail,TCP Protocol)

[Https://baike.baidu.com/item/pop%E5%8D%8F%E8%AE%AE/734244?fr=aladdin](https://www.microsofttranslator.com/bv.aspx?from=zh-CHS&to=en&a=https%3A%2F%2Fbaike.baidu.com%2Fitem%2Fpop%25E5%258D%258F%25E8%25AE%25AE%2F734244%3Ffr%3Daladdin)

SMTP Use TCP Port A

IMAP Protocol

DHCP Protocol ( Dynamic Host Configuration Protocol,UDP)