11-7BCN-xx

SC 6 Nxxxxx

Title: Future Network: Problem Statement and Requirements - Part X: Network Model - TCP/IP/M

Source: China National Body

Project: TBD

Project Editors: TBD

Status: 1nd WD.

This document is a technology report written by experts of china national body.
The contents of this report will be introduced and discussed at the SC 6/WG 7 February 2012 plenary meeting in Guangzhou, there are certain expectations that can be great attention by SC6/WG7 meeting and can become the sub project of TR29181.

ISO/TC /SC6 Nxxxxx

Date: 2012-12-31

ISO-IEC TR29181-X (1rd WD)

ISO/JTC1/SC6/WG7

Secretariat: KATS

Future Network: Problem Statement and Requirements – Part 2:

Network Model – TCP/IP/M

Élément introductif — Élément principal — Partie n: Titre de la partie

Document type:
Document subtype:
Document stage:
Document language:

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard (“state of the art”, for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR.FNPSR was prepared by Technical Committee ISO/IEC JTC1/SC6, TELECOMMUNICATION AND INFORMATION EXCHANGE BETWEEN SYSTEMS, Working Group 7.

ISO/IEC TR 29181 consists of 7 parts including

- TR 29181-1 - Part 1: General Aspects
- TR 29181-2 - Part 2: Naming and Addressing
- TR 29181-3 - Part 3: Switching and Routing
- TR 29181-4 - Part 4: Mobility
- TR 29181-5 - Part 5: Security
- TR 29181-6 - Part 6: Media Distribution, and
- TR 29181-7 - Part 7: Service Composition

Introduction

This technical report is Part X of the Technical report on Future Network – Problem Statement and Requirements developed by ISO/IEC JTC1 SC6 WG7; it described three/four mixed structure of the network model for future network. The objective of TCP/IP/M is to solve the real-time media communication problems of high quality from the network structure, the problem caused by triple play is solved to provide a network environment that is smooth and green environmental protection. The purpose of the present report is to discuss how to develop a clean design of the new network model (TCP/IP/M) that help FN project achieve its lofty ambitions.

Network model is the root of the communication network, all the hardware and the software of network communication depends on it. The design of the network model can change the network structure fundamentally; it can solve the shortage of the old network system and meet new requirements of future network.

Considering evolutionary approaches which seek to engage gradual improvement with available technologies while protecting the integrity of overall structure of old networks, a new scheme will produce a totally new naming and addressing scheme. A clean slate design needs thorough analysis, full understanding of the demand, careful planning and collective work. In order to achieve the maximum benefits and find the best solution, a strategic planning document is needed before specific schemes are standardized.

This report may serve as a strategic planning document for the design of FN-NM. It explains the missions of FN-NM and discusses how it should be developed.

This document could be used in the technical development process to stimulate interests and innovation, to be used in the NM standardization process as reference criteria for evaluating NM proposals, and it could also be used in implementation process as assessment, testing and compliance references.

Future Network: Problem Statement and Requirements – Part X: Network Model – TCP/IP/M

1. Scope

This Technical Report (TR) is about Network Model Schemes, an important subject field in the standardization of Future Network in ISO/IEC. It describes the general characteristics of Future Network Naming and Addressing Schemes including overview, three/four layer network model, synchronization time difference, Address Resolution Protocol, and protocol suite of TCP/IP/M.

2. References

2.1 Normative reference

ISO/IEC PDTR 29181-1, Future Network: Problem Statement and Requirements – Part 1: Overall Aspects.

RFC 1955, New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG

3. Definitions

This Technical Report (TR) uses the following terms and definitions.

3.1 Network

Circuit or part of an electrical circuit. In the electrical system, circuit or the part of the circuit is called network that is composed of several components to make electrical signals transmission according to certain requirements.

3.2 Sub-circuit

Part of the network, consists of one or more elements of both ends in series.

3.3 CIRCUIT

Circuit is a wire connection with each other through several components, can also called network. More specifically, the circuit is closed loop network that can be formed. In a circuit, any component to branch to represent, any two line or two branches of the crossings are called node.

3.4 Analog Circuit

The continuity of physical nature produced by the nature, it will be converted to continuity electrical signals.

3.5 Digital Circuit

Digital circuit also called logic circuit; it is a circuit that converts a continuity of an electrical signal into discontinuous and quantitative electrical signals operated. The digital circuit, signal is not continuous and

quantitative voltage state. The quantitative signal is processed using Boolean logic circuit mostly. The typical digital circuit, oscillator, register, adder, subtraction device, etc calculates the discontinuity of quantitative signal.

3.6 Virtual Circuit

A virtual circuit is a link among two or more endpoints in a packet-switched hash network. It provides temporary or dedicated connection-oriented session between two endpoints. Its inherent characteristics, there is the intended path through a multi-path network. A path defined in advance, you can improve performance and eliminate the demand for frames and group head, thereby increasing throughput. From a technical point of view, packet-switched network via the physical path to change in order to avoid congestion and failure line, but the two end systems to maintain a connection, and if necessary change the path description.

3.7 Permanent Virtual Circuit (PVC)

The virtual logical connection is created among the hosts of users that ensure the correctness and order of the packets. It is necessary to create the virtual circuit before communication and remove the virtual circuit after communication. PVC (Permanent Virtual Circuit) is virtual circuit established when the network init. The virtual circuit has been maintained straight, is defined in advance; basically do not need any time to establish a connection between the endpoint sites.

3.8 Switched Virtual Circuit (SVC)

It is a temporary connection between the endpoints and sites. These connections has been maintained for only the time required, packet-switched service allows the user to define dynamically according to their own needs.

3.9 Virtual Real Circuit

One kind of virtual circuit, statistical compound time division circuit isolated from many time-division circuits.

4. ABBREVIATIONS

FN Future Network

IMP Internet Mixed Protocol

IP Internet Protocol

MAC Media Access Control

TCP Transmission Control Protocol

UDP User Datagram Protocol

SNMP Simple Network Management Protocol

SMTP Simple Mail Transfer Protocol

FTP File Transfer Protocol

RPC Remote Procedure Call Protocol

ICMP Internet Control Message Protocol

ARP Address Resolution Protocol

RARP Reverse Address Resolution Protocol

FDDI Fiber Distributed Data Interface

ATM Asynchronous Transfer Mode

TCP/IP Transmission Control Protocol/Internet Protocol

OSI Open System Interconnect

QoS Quality of Service

M Mixed Protocol

5. Overview

TCP/IP/M is the future of network protocol, which preserves the existing four-layer network model of the Internet, and created a new three-layer network model. In FN, routine use of four-layer model to achieve fast data transfers, special use of three-layer model to achieve smooth communication for voice, video, radio and other, so that meet the different needs.

Four-layer of the packet switching protocol structure is similar to the existing TCP/IP, but virtual circuit-switched based on three-layer is essentially different from TCP/IP. The composite time division circuit is established first In three-layer structure, bandwidth reserved for different time-division circuit through synchronous time-division differences. The flow of information is based on connection-oriented, reliable, and uninterrupted in three-layer structure, data transmission is not packet switching but the circuit transmission essentially, it is called Virtual Real Circuit. It is a pre-built based on the actual needs of the transmission circuit channel; the bandwidth is fixed exclusively and did not need the QoS of existing systems to ensure data flow to achieve a certain performance level. Such as online movies, according to a predetermined bandwidth, seamless transfer omitted the procedure (the movie broken down into multiple packets, assembling data, and then reaches a certain buffer during playback). Three/four mixed network architecture design solve the voice quality, content and transmission bandwidth allocation, packet transmission and circuit transmission, routing capacity of compatibility problems. The specific works are shown below.

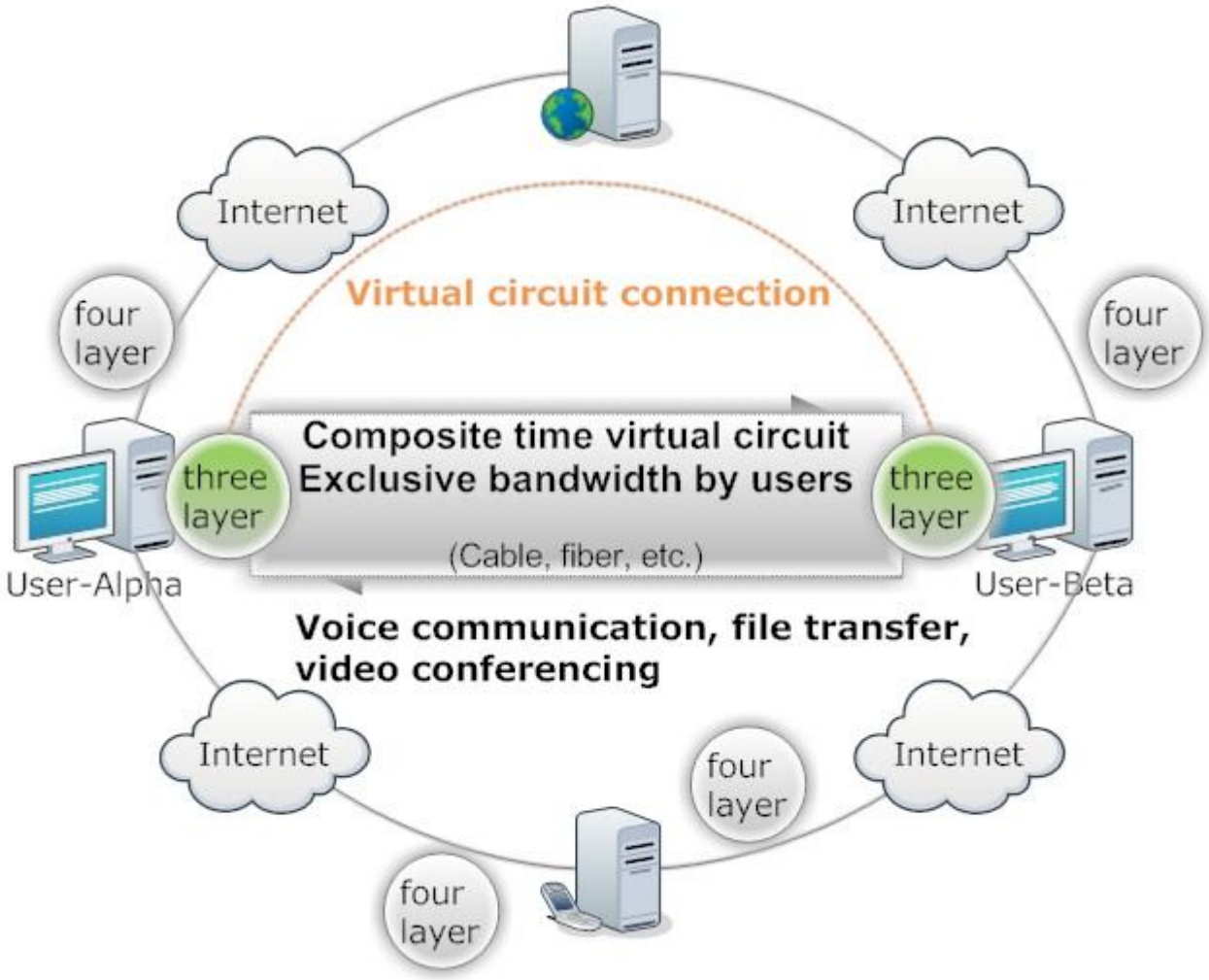

Figure 1. TCP/IP/M Working Principle

5.1 The Basic Structure

The current means of communication include the circuit transmission and the packet transmission, but TCP/IP is mainly used on the packet transmission. FN will be involved in data transmission and video broadcasting and voice integration needs, we believe that integration system can solve the above problems including the three-tier structure of virtual real circuit and the four-tier structure of the IP transport. Three-tier architecture for video broadcasting and voice calls, and IP data transport are still using four-tier structure. See chart.

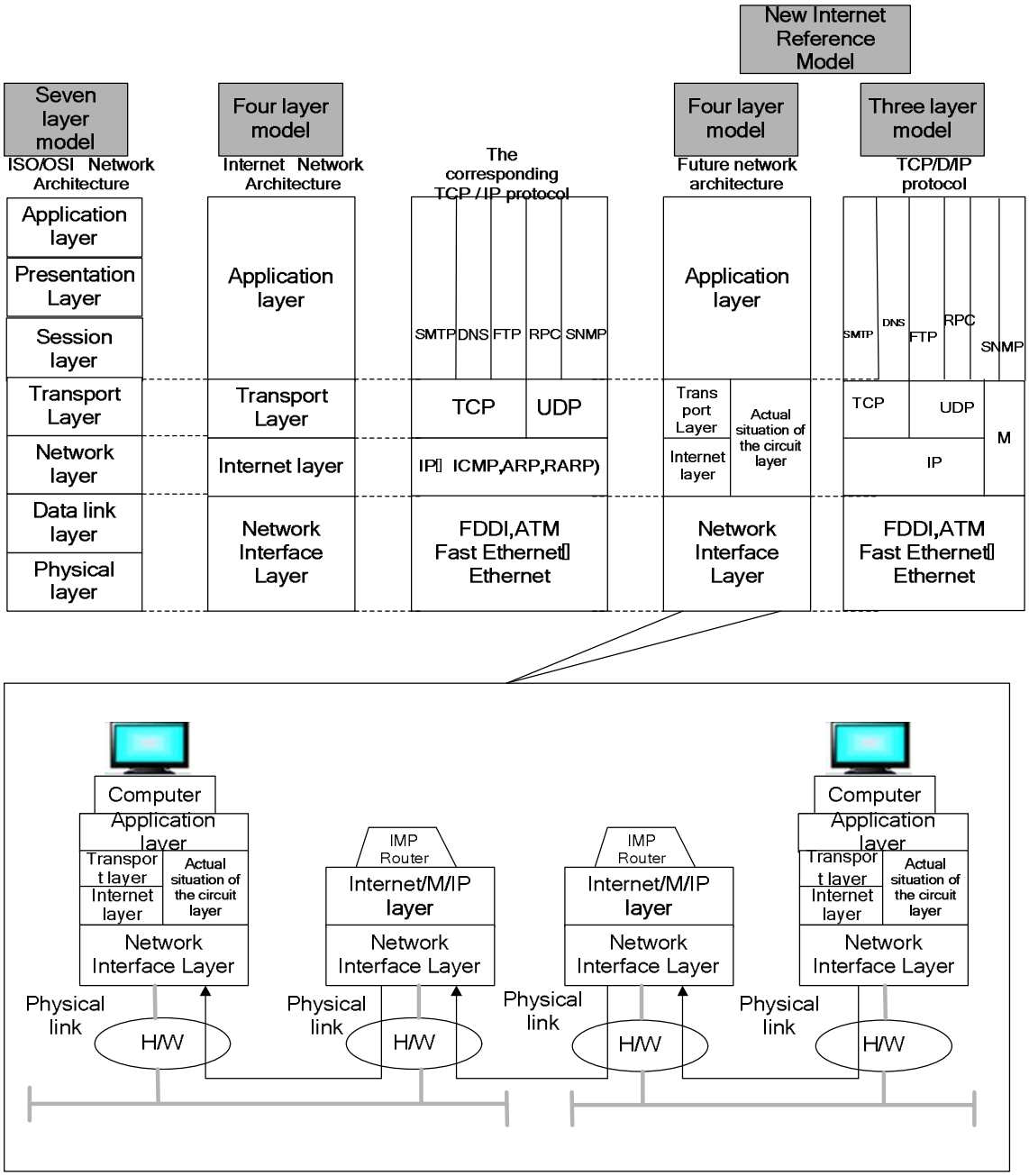

Figure 2. Network Model for the future

Future network model characteristics are as follows:

1) Unique dual-mode network structure, including the existing four-layer model of the Internet and new three-layer model.

2) The composite time difference will be formed when time division of transmission stagger time node, in order to form the multi-channel virtual circuit of a composite time division, multi-layer transmission problem will be solved in the same statistical time division, packet and circuit data transmission as needed in the same link.

3) The proposed concept of virtual real circuit, completely solve the existing problems including high-quality video and voice communications.

4) Backward compatibility, the new and the existing network to network are interconnected, a smooth transition from the existing network to the new network.

5) The composite time difference circuit of transmission combine the advantages of circuit and packet switching to achieve high-speed network, stable and energy saving, environmental protection in FN.

6) FN will be Efficient, fast, stable, energy-saving, environmental protection, it will accelerate the relations between people, information exchange, will promote economic, technological and even military development.

5.2 Data Transfer

5.2.1 TCP/IP Data Transfer

Let us see the case of flow when it passes through the TCP protocol stack as shown, when an application uses TCP (Transmission Control Protocol), data will be transferred between the application and the TCP module. When an application uses UDP (User Datagram Protocol), data will be transferred between the application and the UDP modules. FTP (File Transfer Protocol) is a typical application using the TCP packet, the protocol stack is FTP/TCP/IP/ENET in this example. SNMP (Simple Network Management Protocol) is an application using UDP, the protocol stack is SNMP/UDP/IP/ENET in this example.

TCP module, UDP module, and Ethernet drivers are n-to-1multiplexers. As multiplexers, they reuse a lot of input to one output. They are also 1-to-n-de-multiplexers. As multiplexers, they generates a lot of output from an input through the protocol head.

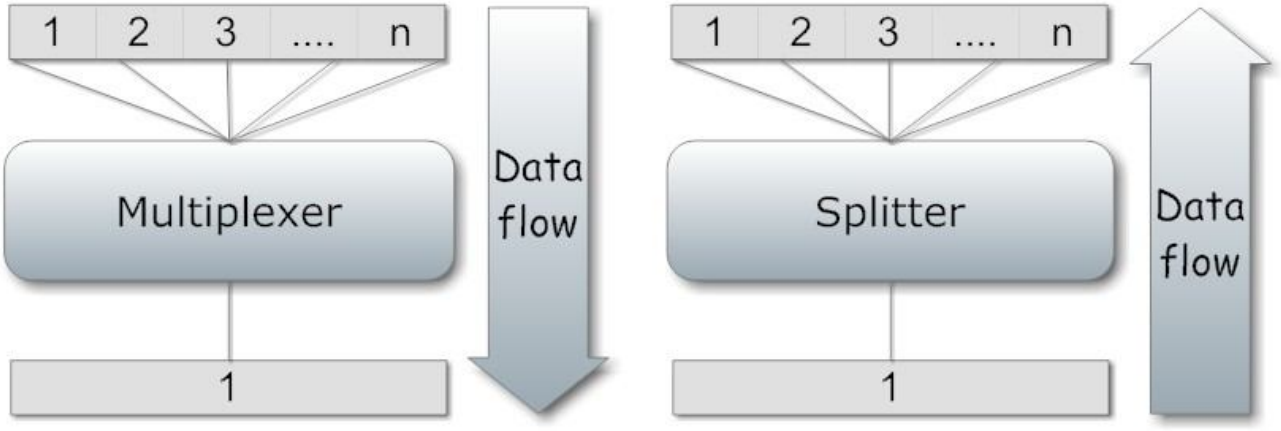

Figure 3. n-1 multiplexer 和 1-n splitter

If the Ethernet frame leave the network card to enter into an Ethernet driver, the package can be passed upwards to the ARP (Address Resolution Protocol) module or to the IP (Internet Protocol) module. The field attribute of Ethernet frame determines whether the Ethernet frame is passed to the ARP or IP modules.

If the IP message enter into the IP packet, it is passed up to TCP or UDP, which is determined by the field property of the IP header. If the UDP message enter into the UDP, the application message is passed up to the network application, which is determined by the port value of the UDP header. If the TCP message enter into the TCP, the application message is passed up to the network application, which is determined by the port value of the TCP header.

Downward multiplexing is easy to achieve, because there is only one downward path from each starting point; each protocol module adds its header information, so that packages can be separated on the destination computer.

Data from the application compound the TCP or UDP to the IP module, and then was sent to the lower layer.

Although Internet technology supports many network media, our examples are all discussed based on the Ethernet, because the Ethernet is the most common physical network of IP-based. In Figure 1, the computer has only an Ethernet connection. Physical address for each Ethernet interface is unique. They are stored in the underlying Ethernet driver interface.

5.2.2 M Data Transfer

New mixed protocol (M) without TCP/IP protocol, it is a data transmission channel; there is no concept of reuse and shunt. M and TCP/IP data differentiate through the IP header information, points to a different protocol for processing.

5.3 Network Interface

If a computer connects with two separate Ethernet, it looks like Figure 4.

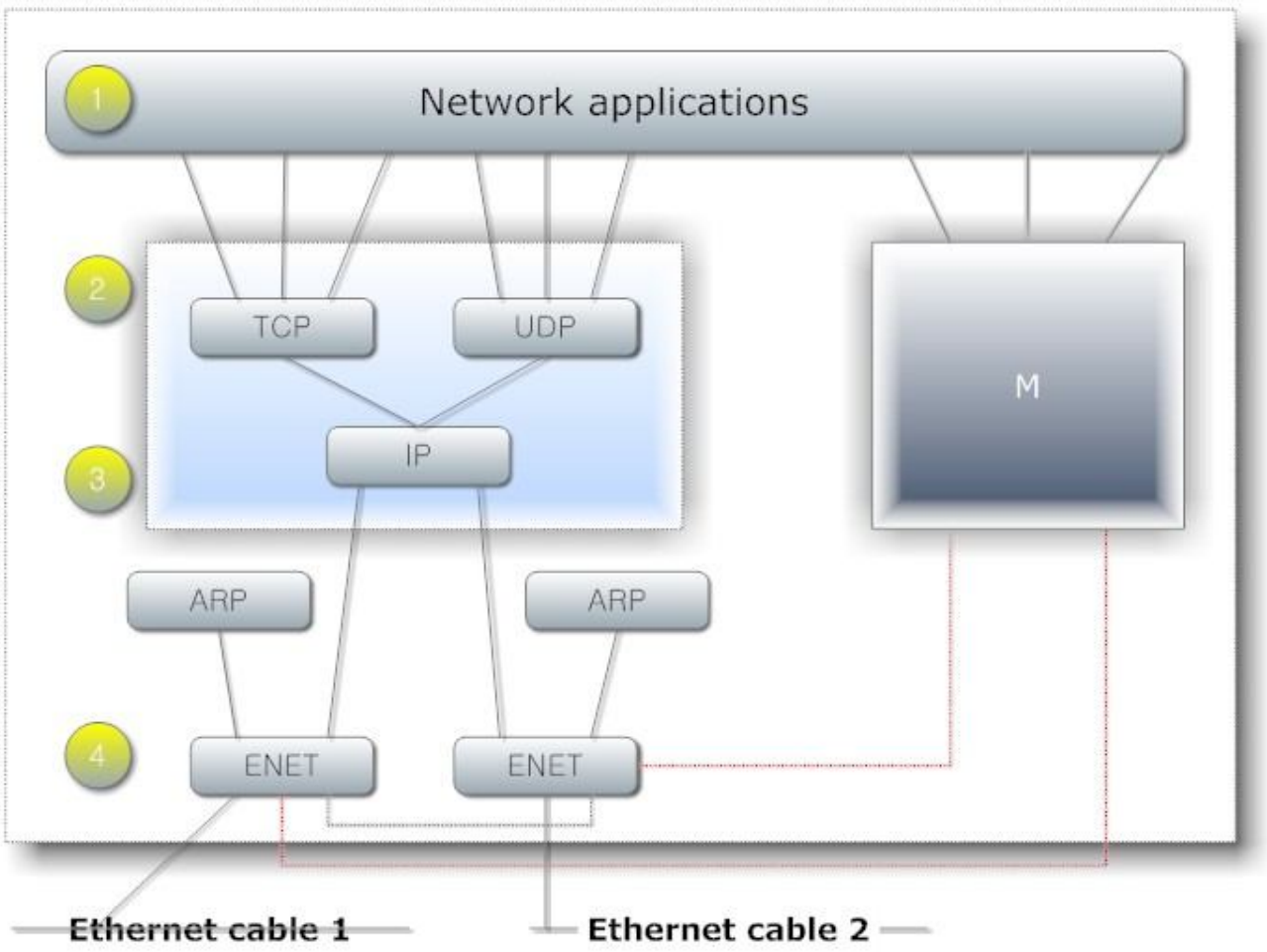

Figure 4. Two network interfaces of TCP/IP/M

Please note that this computer has two physical addresses and two IP addresses. From the structure in Figure 4, we found that the computer has more than one physical network interface, the IP module of TCP model is the combination of n_to_m multiplexer and m_to_n splitter.

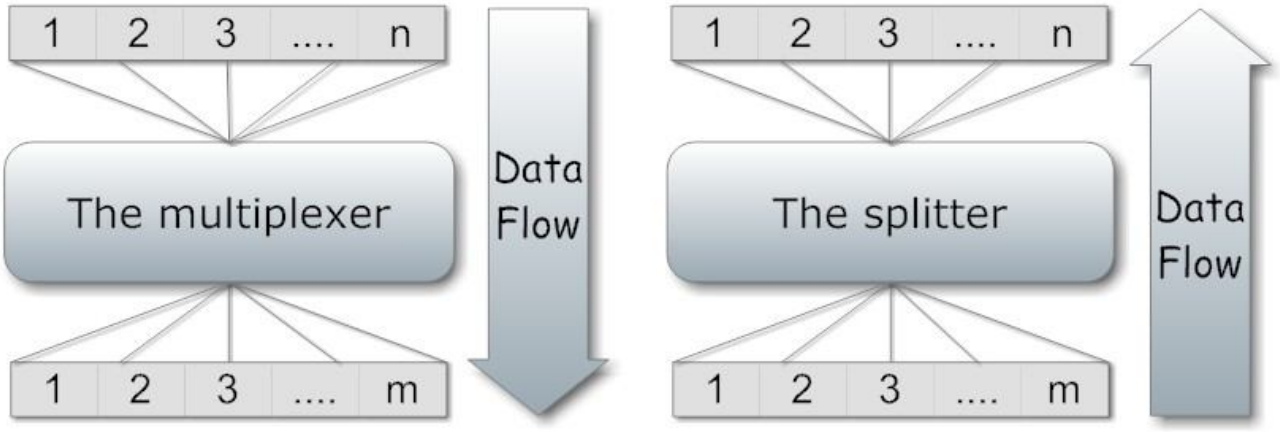

Figure 5. TCP n-m Multiplexer and m-n Splitter

From the above, we can see that this multiplexing can receive and send data from any direction, the IP module of more than one network interface is complex than the example that the data pass from one network to another network.

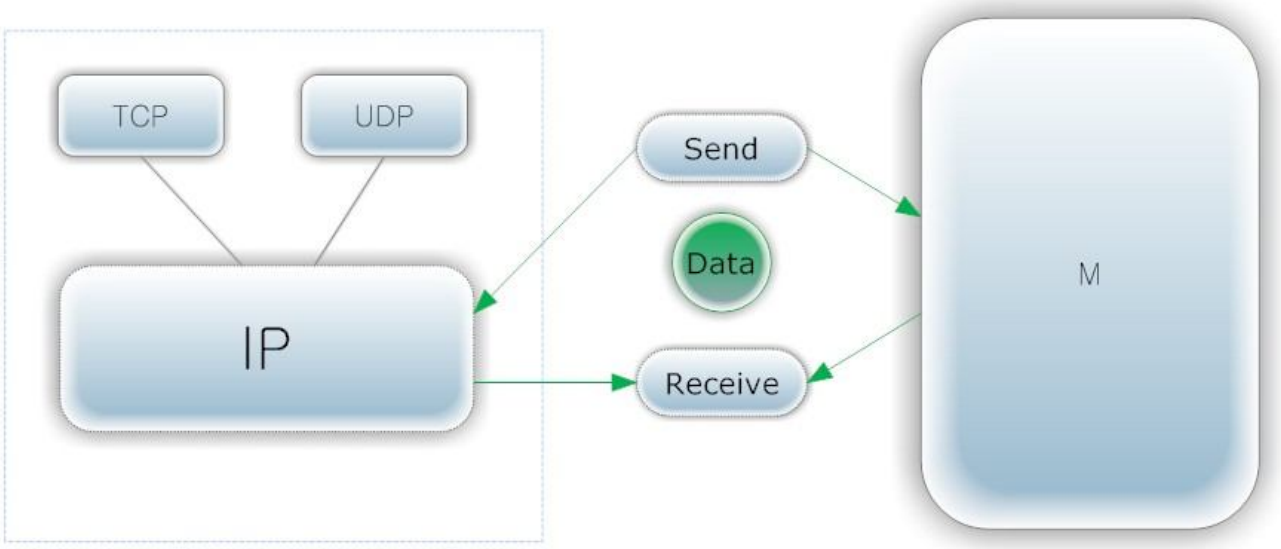

Figure 6. Send and receive IP packet example

For the four-layer models, the process sending IP packets to another network called IP packet transmission, a specialized computer used to pass IP packets called "router". As you can see from the figure, passing the IP packet on the router does not involve TCP and UDP modules, some routers do not need the TCP or UDP module.

For the three-layer model, M package is only transferred between any computers.

5.4 Generate specific logical network by IP

IP module is central to the success of internet technology, when the message pass down the protocol stack, each module or driver will add his head to the message. Each module or driver remove the corresponding header from the message, when the message is uploading along the protocol stack. The IP header contains many IP address to distinguish the unique logical network from the physical network, interconnected physical network is an integral part of the internet, the physical network contact with each other to form the internet network.

5.5 Independent of physical network

Net application hides the underlying network hardware by IP, if the new physical network comes into use, you only need use the new driver. Thus, despite the hardware technology is changing, the network application is still not perfect and vulnerable.

5.6 Communicate with each other

If the two computers can communicate with each other, it says they are "interoperable". If the internet is unblocked, it says they have "interoperability". There are many computer users benefiting from the Internet, because the interoperability of the computer in the market. In general, when you buy a computer, it can communicate with each other. If the computer does not have interoperability, the computer would have no market competitiveness

6. TCP / IP / M three / four-layer model

TCP / IP protocol stack is reference model of the U.S. Defense Advanced Research Projects Agency computer network (ARPANET) and its subsequent use of the Internet. ARPANET is the U.S. Department of Defense -sponsored research network. Initially, the beginning, it only connects four universities within the United States. During the following years, it connected hundreds of universities and government departments via leased telephone lines. ARPANET eventually become the world's largest interconnected network - the Internet. The original ARPANET shut down permanently in 1990.

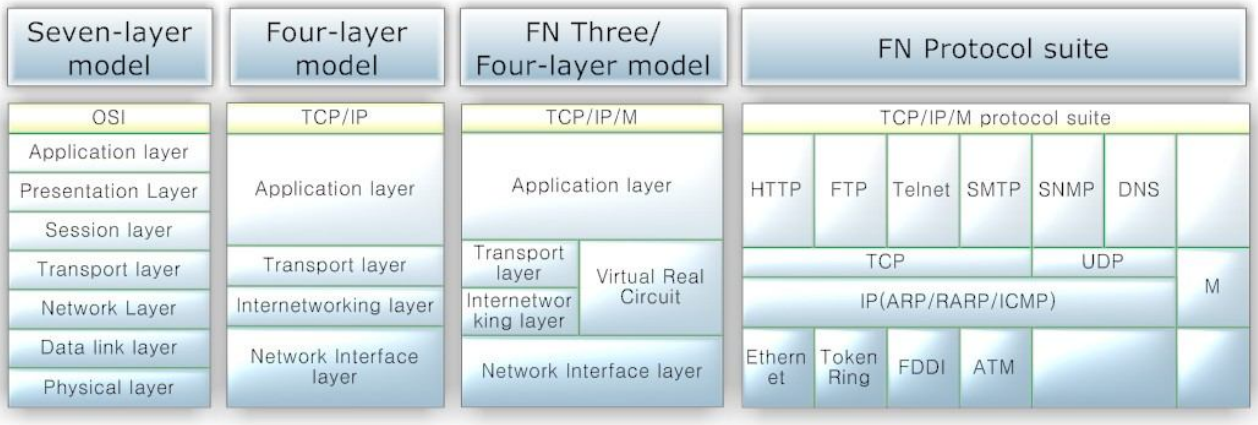

Figure 7. TCP/IP/M Reference Model

As shown above, TCP / IP reference model is divided into four layers: application layer, transport layer, internetworking layer and the network interface layer. The new TCP / IP / M reference model is divided into three layers: application layer, the actual situation the circuit layer and the network interface layer, combine the transport layer, internetworking layer circuit layers into the actual situation. This is the TCP / IP protocol hierarchy on the computer in the Internet that uses Internet technology to communicate with each other so that each computer has a hierarchical structure. This hierarchy determines the mode of computers communicate with each other on the internet. Data transmit from the upper to the ground floor using this Hierarchical structure, and then transmit the data through the network cable out.

The main function of each layer is introduced below.

6.1 Application Layer

Application-layer corresponds to the high-level of OSI reference, needed to provide users with a variety of services such as: FTP, Telnet, DNS, SMTP, etc.

6.2 Transport Layer

Transport layer corresponds to the transport layer of OSI reference model, providing the end to end communication of application layer entities. This layer defines the two main protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

TCP protocol provides a reliable, connection-oriented data transmission services; UDP protocol provides an unreliable, connectionless data transfer service.

6.3 Internetworking Layer

Internetworking layer corresponds to the network layer of the OSI reference model, mainly to solve the problem of host to host communication. This layer has four main protocols: Internet Protocol (IP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP) and Internet Control Message Protocol (ICMP).

Internetworking layer IP protocol is the most important protocol; it provides an unreliable, connectionless datagram delivery service.

6.4 Network Interface layer

Network Interface layer corresponds to data link layer and physical layer of the OSI reference model. In fact, TCP/IP itself does not define any protocol for the level, in the interconnection, every networks use their own physical layer and data link layer protocol, and then connect with the TCP / IP network interface layer.

6.5 Virtual Real Circuit layer

6.5.1 Virtual circuit switching

Switched Virtual Circuit (SVC) is a class of virtual circuit needs to dynamically set. An SVC can be conceptually translated into a dial-up connection.

Correspond with the actual circuit, virtual circuit is defined as the physical link for data transmission occupancy distribution; and packet-switched data transmission refers to the format.

6.5.2 Circuit Switched

1) Uses a static allocation strategy, establish a connection by connection-oriented.

2) The two sides established communication path fails, it can re-dial connection.

3) The transmission line has a fixed bandwidth; data transfer can be to get rid of instability.

4) No unpacking, group packages, more transmission efficiency.

The current virtual circuit transmission is still a packet data, circuit-switched rather than real.

6.5.3 Packet Switching

Using store and forward technology, based on the mark, data can be transmitted without establishing connection first, therefore, packet switching is an efficient, flexible, reliable, fast, etc., but the transmission delay larger than the circuit-switched, not practical in real-time data transmission.

6.5.4 Message Switching

Corresponding to the connectionless service, do not establish a connection before transferring data, each group may choose a different route for a small amount of data transfer, and reliability is not high.

6.5.5 Virtual Real Circuit Switching

Combine the advantages of Virtual circuit and real circuit , the three-tier structure first create compound hours virtual circuit, pre-reserve bandwidth for different hours circuit, through the composite hours method, to achieve using creating connection by virtual circuit ,and transmitting data by real circuit.

6.5.6 Virtual Real Circuit, Virtual Circuit, Datagram's contrast

types	actual situation circuits	virtual circuits	datagram's
Transmit method	Complex division circuit	Statistical time division circuit	Statistical time division circuit
Transmit Content	Circuit data, packet data	Packet data	Packet data
Synchronization time	No Synchronization	Synchronization	Synchronization
Establish connection	must	must	no
Backup virtual circuit	must	no	no
Destination address	Use only in connection establishment phase, a short circuit data using a virtual circuit number	Use only in the connection establishment phase, each group using short virtual circuit number	Each group has the full address of the destination station
bandwidth	Once the bandwidth is determined not to change the general,	Selected only on the first router, other routers can not determine the bandwidth of the first router selected	Only determined by the bandwidth
Congestion control	No, a smooth way	Have, but ineffective	Random block
Network storage node	No	8 Bytes	15Bytes
Transition quantity	Good	general	bad
Transition cost	low	general	high
Transition efficiency	high	No high	low
routing	Same time with the actual situation circuits connection is established, all the	Same time with the virtual circuit connection is established, all the p	Each group independently selected route

	circuit data transmission have the same route and the same bandwidth a, and have more than one backup route	ackets sent have the same route, but can not guarantee there will be clogging the transmission quality	
When a router fault	All the fault of the router via a virtual circuit can work from the backup route	All through the failure of the router's virtual circuits are not working	Failure of the router packet may be lost, some routes may change
Group of order	Actual situation is no packet transmission ci rcuit reliability, but the virtual circuit packet data can be defined QOS and packet sent	Always arrive at the destination station by s ending the order	Arrive at the destination station may not send the order by
Data transfer circuit	Can transmit data circuit, but if the first route router failure, the second routing will sen d the circuit data to the destination order by order, but the virtual circuit packet data can be sent by defined QOS and packet	No data transmission system ci rcuit	No data transmission system circ uit
Error handling end to end	Responsible by the communication network, but the QOS data is responsible by the communication subnet, packet data is responsible by host	Responsible by communication subnet	Responsible by host
Flow control end to end	Responsible by the communication network, but the QOS data is responsible by the communication subnet, packet data is responsible by host	Responsible by comm unication subnet	Responsible by host

6.6 Three-and four-layer model of integration

Taking into account the smooth transition and future network compatibility the old network, our network model includes both the future of four-layer models and three-layer models. Then, three models and four models coexistence and the trigger mechanism is a question worth exploring, we need to let the application notify the transmission network framework when transmitting IP packets and M data, the network can use a different framework network model to process and transmit data. Perfect scenario is a computer and another computer can be a communication between the IP packet and M data see below.

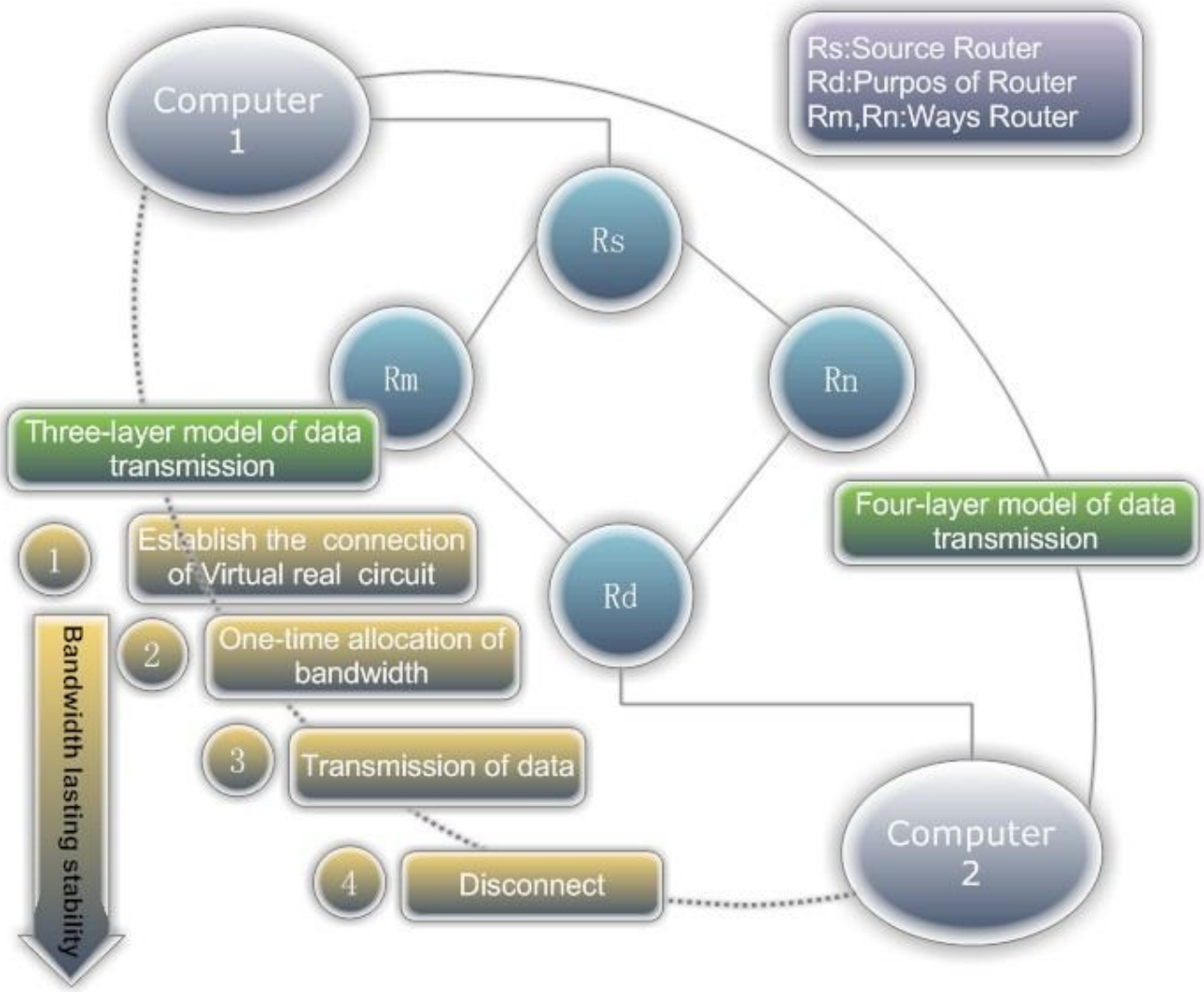

Figure 8. Three / four-layer model of integration

7. TCP / IP / M protocol stack

7.1 Net Application

TCP and UDP provide different services; most applications use only one of them. Of course you select the most suitable for your protocol. If you need reliable data transfer, TCP may be the best choice. If you need a packet service, UDP is the best. If you need effective long path, TCP may be the best. If you need faster network response time, UDP may be the best. If you do not want to classify, the "best" choice is ambiguous. However, the application can compensate for the lack of choice. For example, if you select UDP, but you need the reliability, the reliability of the application can be added to the. If you select TCP, but you need to mark the service, then the application must be in the byte stream to add tags.

The number of network applications is a continuous growth. Since the internet technology began to have some applications of: TELNET and FTP. The other is relatively new: X-WINDOWS and SNMP. Here are some web applications.

7.1.1 TELNET

TELNET provides a remote login service. With its operation and appearance is similar to the phone dial. The user types on the command line: "TELNET DELTA" will receive from the "delta" to the login prompt.

TELNET so good, it makes an old application that has a wide range of applications. TELNET usually work between different operating systems. For example, TELNET client to VAX / VMS system, and the server is a UNIX system.

7.1.2 FTP

File Transfer Protocol (FTP), is as old as TELNET and web applications, but also a wide range of applications. From the operating point of view if you log on the remote computer. But you must use a special command on the command used to replace you. FTP commands allow you to copy files between two computers.

7.1.3 RSH

Remote shell (rsh or remsh) is one of all remote UNIX-type command family. UNIX copy command - CP, into a RCP. UNIX command "who landed" WHO becomes RWHO. This series have been turned into "R" series of commands.

R* commands mainly work on UNIX systems and is designed to interoperate between the host trusted, Security is rarely considered, but they provide a convenient user environment.

To a remote computer called delta, execute the command "cc file.c", type "rsh delta cc file.c", to copy the file to delta, type "rcp file.c delta". To login to delta, type "rlogin delta", if you are in a particular way to manage this computer, you will not have the login prompt.

7.1.4 NFS

Network File System, developed by the U.S. SUN, using UDP, it is between different computers on a UNIX system file upload is very good. A diskless workstation to access the server's hard drive through as if the disk is local. The host "alpha" as a single database on the host can be "beta" as long as the database file using the upload using NFS in "beta" on.

NFS adding large amounts of information to the network, so that the connection is slow, but it has the advantage that the main. NFS client implementation in the kernel, allowing the use of NFS disk as if in the same local.

7.1.5 SNMP

Simple Network Management Protocol (SNMP) uses UDP, is designed to manage from a central network point. It is well known, it is sufficient if the data, network administrators will be able to find and diagnose network problems. The center use SNMP to collect data from on-line computer. SNMP defines the format of this data. The center or network administrator to interpret such data.

7.1.6 X-WINDOW

X-WINDOW system, the X WINDOW TCP-based protocol to draw the bitmap on the workstation display window. X WINDOW not just painting the window, it can be used to design the user interface.

7.2 Transport Protocol

7.2.1 UDP (User Datagram Protocol)

UDP is one of the two main protocols on top of IP layer. It provides the service for user network applications, web applications use UDP are: NFS (Network File System) and SNMP (Simple Network Management Protocol). UDP services only added a little bit on the basis of the IP.

UDP is a connectionless datagram service without loss of detection. UDP does not maintain point to point connection with remote UDP module, it only send and receive the packets, careless of send and receive loss.

UDP add two properties in the IP based, one is the port number, and the other is to check data integrity checksum.

7.2.1.1 Ports

The communication paths between applications and UDP are UDP port. The port is a numeric representation, starting from 0. Service applications with specific port number to wait for the message to enter. The Server continuously scans the client's requests.

For example, such as SNMP, called an SNMP agent, always waits on port 161 for messages. Each computer can have only one SNMP agent because there is only one UDP port number 161. This port number is well known, it is fixed, is assigned a unique network number. If the SNMP client requests a service, then it sends a UDP packet to the destination computer's port 161.

When an application sends a UDP packet, then the remote receives a unit. For example, if an application made five UDP packets, the remote will read five times. Of course, the hair of five packages and read the five packets of equal size.

UDP save each complete packet, it does not add the two messages in one application, nor to a package split into two.

7.2.1.2 Checksum

Display in the IP header fields "UDP", UDP IP packets will be sent to the UDP module. When the UDP module receives the UDP packet it checks its checksum. If its checksum is 0, it means that the sender checksum is not calculated, can be ignored. Therefore, it does not matter if the computer sending the UDP dates without producing checksum. If the physical frame is communicating between two UDP modules in a network, you do not need to generate a checksum. However, we recommend using the checksum because the routing table changes may lead to unreliable data through the medium.

If the checksum is correct or is 0, the destination port will check it. UDP packets transmitted to the port, it is queued for processing the application, or UDP packets will be discarded. If the UDP packet arrives faster than the speed of the application can handle or UDP packet to wait for the queue fills up, UDP packet will be discarded by UDP module. UDP modules will always dropping UDP packets until the queue has the extra space.

7.2.2 TCP(Transmission Control Protocol)

TCP provide different services from UDP, TCP provides a connection of the bit stream, unlike the connectionless datagram service. TCP to ensure reliable transmission, but UDP does not guarantee.

TCP is called by the network application to ensure reliable transmission and no timeout and misinformation. There are two typical network applications FTP (File Transfer Protocol) and TELNET. Other popular TCP network applications include: X-WINDOW system, rcp (remote copy), and r-series commands.TCP pays these prices for its power: it requires more CPU and network bandwidth. TCP module is much more complex than UDP module.

Similar to the UDP, TCP connected to network applications by port. Specific port number corresponds to a specific application. For example TELNET server uses port 23. TELNET client can only connect to a specific port on the computer 23 to be successful.

When the application starts using TCP, the TCP module on the client side and server-side TCP module communicate with each other, these two TCP endpoints modules form virtual circuits. This virtual circuit consumes resources at both ends. The virtual circuit is Two-way, the data in both directions simultaneously to pass. Applications write data to TCP port, the remote application control the data through the network.

TCP packets can be divided into any size, no boundaries between packages and packages. For example, if an application send data to the TCP port 5 times, a remote application may have to read 10 times, or it will read only once. The number and size written on the one end and the other is not associated.

TCP has a timeout and resend the sliding window protocol. The package sent must be confirmed by the remote. Confirmation message can carry on the packet. It can control two remote receiving ends, to prevent buffer overflow.

For all of the sliding window protocol, there is a window size; window size determines the receipt of confirmation can be sent before the total data. For TCP, this number is not the number of TCP segments but the number of bytes.

7.3 IP Protocol

IP (Internet Protocol) is the heart of TCP / IP is the most important protocol in the network layer.

IP layer receives packets from the lower layer (layer such as Ethernet network interface device driver) and the packet is sent to the higher level --- TCP or UDP layer; opposite, IP layer receives the data packet from the TCP or UDP layer and send the packet to the lower level. IP packets are unreliable, because the IP does not do anything to make sure the packet is sent or not or has been destroyed. IP packet contains the address of the host to send it (source address) and the address of its receiving host (destination address).

When High-level TCP and UDP services receiving data packets, it is usually assumed in the packet source address is valid. The same can be said, IP address forms the basis of many services certification, and these services believe that a valid data packet is sent to the host. IP conformance include an option called IP-source-routing, can be used to specify a direct path between source and destination addresses. For some TCP and UDP services, the IP packet use this option is considered as coming from the faked system, rather than from its true location. This option test indicating that it can be used to cheat the system for accepting connection usually prohibited. So, many services rely on IP source address will have to confirm the problem and may be illegal invasion.