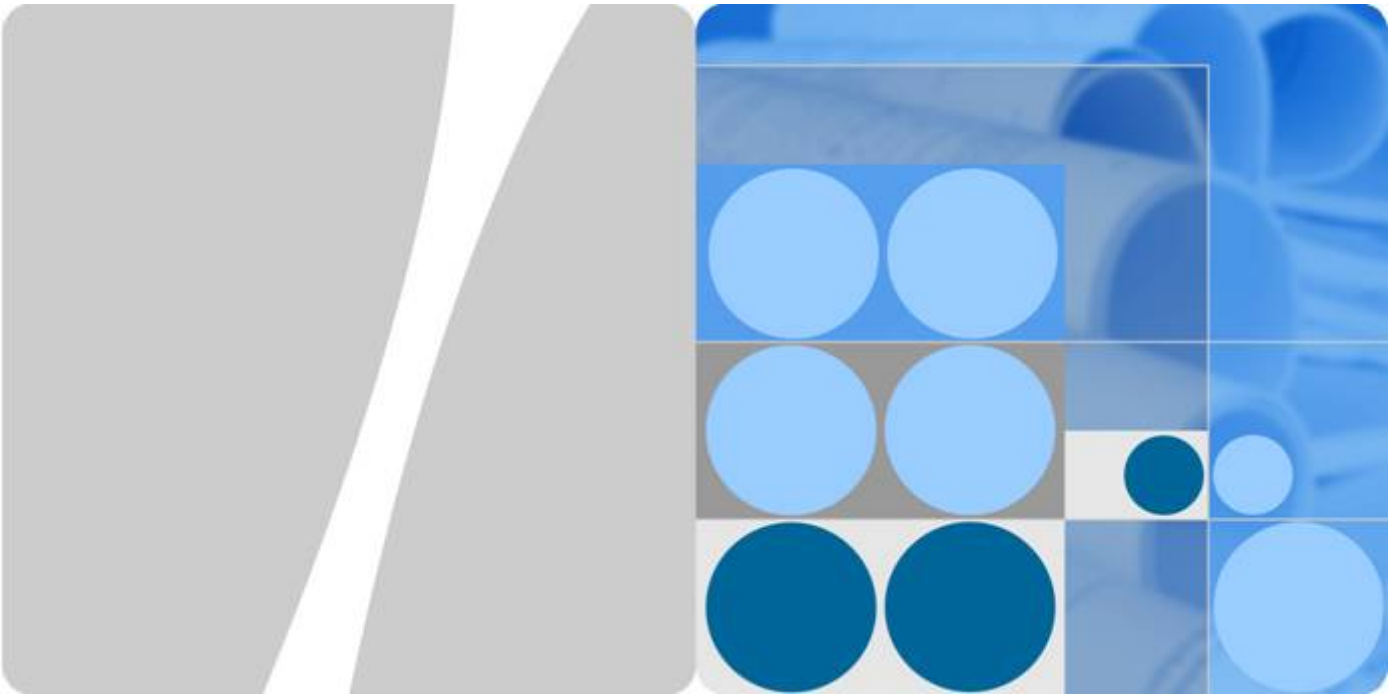

Quidway S2700/S3700/S5700/S6700 Series Ethernet Switches

V100R006C01

Glossary

Issue 01

Date 2011-10-26

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes the glossaries and abbreviation of all software and hardware features about S2700/S3700/S5700/S6700.

This document is intended for:

- Commissioning Engineer
- Data Configuration Engineer
- Network Monitoring Engineer
- System Maintenance Engineer

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all changes made in previous issues.

Changes in Issue 01 (2011-10-26)

Initial commercial release.

Contents

1 Numerics

1:1 cold backup A backup mode in which two systems with the same functions are deployed. One system is in the active state and the other system is in the standby state with the power switched off. Once the active system encounters a fault, the standby system takes over the service of the active system by manual intervention.

1+1 hot backup A backup mode in which two systems with the same functions are deployed, one in the active state and the other in the standby state with power on. The standby system backs up the data of the active system automatically. Once the active system encounters a fault, the standby system takes over the service of the active system automatically or by manual intervention.

1000BASE-X The first 1000BASE-X was developed on Gigabit Ethernet. Its design is derived from the design of the physical layer of the fiber channels[ANSI94]. 1000BASE-X series use the design for the physical layer of a fiber channel, especially the FC-0 and FC-2 sub-layers.

100BASE-FX 100BASE-FX utilizes two optical fiber cables of which one cable is used for transmission and the other cable is used for reception. With the 100BASE-FX, a method to convert the 4B/5B NRZI code groups stream into optical signals is required.

100BASE-T see **Fast Ethernet**.

100BASE-TX 100BASE-TX makes use of two pairs of twisted pair cable. One pair is used for transmission and the other pair is used for reception. Both STP and category 5 UTP are allowed.

100BASE-X For the 100BASE-X standard, a unidirectional data rate of 100 Mbit/s is achieved by transmitting data over a single link. 100BASE-X includes 100BASE-TX for shielded twisted pair (STP) or category 5 unshielded twisted pair (UTP), and 100BASE-FX for optical fiber.

802.1 ag MAC Trace Similar to traceroute or tracert, 802.1ag MAC trace works by sending test packets and waiting for a reply to test the path between the local device and the destination device and to locate faults.802.1ag MAC trace is initiated by a MEP and destined for a MEP or MIP at the same maintenance level within any MA.

802.1ag MAC Ping Similar to ping, 802.1ag MAC ping works by sending test packets and waiting for a reply to test whether the destination device is reachable. 802.1ag MAC ping is initiated by a MEP and destined for an MEP or MIP at the same maintenance level within any MA.

2 A

Abstract Syntax Notation One An integrated circuit designed to perform a particular function. To perform the function, it is defined with an interconnection of a set of basic circuit building blocks that are drawn from a library provided by the circuit manufacturer.

Access Control List An access control list (ACL) is a reference table that an operating system refers to to check the access rights of users, with regard to their rights to a particular system object, such as a file directory or individual file. ACLs are essentially traffic filters that are used on devices to identify specific types of packets based on a packet attribute, such as the IP address.

access layer The access layer functions to connect the end users (or last mile) to the ISP network. The access layer devices are cost-effective and have high-density interfaces. In an actual network, the access layer includes the devices and cables between the access points and the UPEs.

accounting The process of keeping track of a user's activity while accessing a network's resources, including the amount of time spent in the network, the services accessed during the time spent in the network, and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing and cost allocation.

acknowledgement A response sent by a receiver to indicate successful reception of information. Acknowledgements may be implemented at any level including the physical level (using voltage on one or more wires to coordinate transfer), at the link level (to indicate successful transmission across a single hardware link), or at higher levels.

ACL see **Access Control List**.

Active Interface In link aggregation, the interfaces that are responsible for forwarding data in the active state are called active interfaces.

Active Link In the link aggregation group, the links connected to active interfaces are active links.

Active Mode It is a working mode of EFM OAM. The discovery and remote loopback can only be initiated by the interface in the active mode.

active/standby backup The same two systems are deployed to improve the reliability. For example, two MPUs work in the active/standby backup mode. One MPU works in THE active state, and the other MPU works in the standby state. When the active MPU fails, the standby takes over the services immediately to realize the fast switchover of services.

adapter A fitting that supplies a passage between two sets of equipment when they cannot be directly interconnected.

address mask The address-sized quantity, configured along with an address that has 1's for the "link" portion of the address and 0's for the "node" portion of the address. A bit mask used to select bits from an IP address for subnet addressing. The mask is 32 bits long, and selects the network portion of the IP address and one or more bits of the local portion.

address resolution A protocol for mapping 32-bit IP addresses to 48-bit data link layer addresser, such as the Ethernet address. The Address Resolution Protocol (ARP) is specified in RFC 826.

Address Resolution Protocol The TCP/IP protocol used to dynamically bind a high-level IP address to a low-level physical hardware address. ARP is used across a single physical network and is limited to networks that support hardware broadcast.

Addressing mechanism The multicast data is transmitted from the multicast source to a group of receivers according to the multicast address.

AF see **assured forwarding**.

agent Entity acting on behalf of another. In network management, an agent is the server software that runs on a host or router that is being managed.

air filter A filter that can prevent dust from entering the device.

Alternate Interface It is the backup interface of the root interface. Compared with STP, it is a new role of interface added to each device in RSTP.

American National Standard Institute An organization that defines U.S standards for the information processing industry. American National Standard Institute (ANSI) participates in defining network protocol standards.

anonymous FTP A File Transfer Protocol (FTP) session that uses login name "anonymous" to access public files. A server that permits anonymous FTP often allows the password "guest".

ANSI see **American National Standard Institute**.

ESD wrist strap An anti-static wrist strap or prevention electrostatic discharge (ESD) wrist strap is a device used to prevent a person from getting affected by electrostatic discharge by safely grounding a person working on an electronic equipment. It consists of a stretchable band of fabric with fine conductive fibers woven into it. The fibers are usually made of carbon or carbon-filled rubber, and the strap is bound with a stainless steel clasp or plate. They are usually used in conjunction with an anti-static mat on the workbench, or a special static-dissipating plastic laminate on the workbench surface.

Application Specific Integrated Circuit An integrated circuit designed to perform a particular function by defining the interconnection of a set of basic circuit building blocks drawn from a library provided by the circuit manufacturer.

ARP see **Address Resolution Protocol**.

AS see **Autonomous System**.

ASIC see **Application Specific Integrated Circuit**.

ASN.1 see **Abstract Syntax Notation One**.

assured forwarding Assured Forwarding (AF) is one of the four per-hop behaviors (PHB) defined by the Diff-Serv workgroup of IETF. AF is suitable for certain key data services that require assured bandwidth and short delay. For traffic within the limit, AF assures quality in forwarding. For traffic that exceeds the limit, AF degrades the service class and continues to forward the traffic instead of discarding the packets.

authentication In a multiuser or network operating system, the process by which the system validates a user's logon information.

authorization The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

auto-negotiation An optional function of the IEEE 802.3u Fast Ethernet standard that enables devices to automatically exchange information over a link about speed and duplex abilities.

Autonomous System A portion of a network, usually within the control of one organization and usually running a single routing protocol. Routing across Autonomous Systems (ASs) is performed with an interdomain protocol.

availability It refers to the state of products that they can work or be available immediately at any time when the product is required to work. The probability measurement is called availability.

3 B

backbone network Any network that forms the central interconnection for an internet. The communication backbone for a country is WAN. The backbone network is an important architectural element for building enterprise networks. It provides a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Generally, the backbone's capacity is greater than the networks connected to it.

backbone VLAN The backbone VLAN ID refers to the VLAN ID of the provider's backbone network.

backplane A backplane is an electronic circuit board containing circuits and sockets into which additional electronic devices on other circuit boards or cards can be plugged; in a computer, generally synonymous with or part of the backplane.

backplane bandwidth see **switching capacity**.

backpressure Inform the upstream interface with an incoming traffic about the congestion so that the traffic slows down or the transmission is stopped till the congestion recedes.

Backup Interface It refers to the backup interface of the designated interface. Compared with STP, it is a new role of interface added to each device in RSTP.

Backup links To improve the reliability of the link, link aggregation introduces the mechanism of backup links. These backup links often act as inactive links. Only when the current active interface fails, the backup interface changes from inactive to active.

bandwidth The difference between the highest and lowest frequencies that an analog communication system can pass. The data transfer capacity of a digital communication system. For example, the rate of information flow in bit/s.

baud rate The number of times per second the signal can change on a transmission line. Commonly, the transmission line uses only two signal states, making the baud rate equal to the number of bits per second that can be transferred. The underlying transmission technique may use some of the bandwidth, so it may not be the case that users experience data transfers at the line's specified bit rate.

BE see **Best-Effort**.

Bearer An information transmission path with a defined capacity, delay and bit rate, and so on.

bearer network A network used to carry the messages of a transport-layer protocol between physical devices.

Best-Effort Characteristics of network technologies that do not provide reliability at the link level. IP works well over best-effort delivery hardware because IP does not assume that the underlying network provides reliability. The UDP protocol provides best-effort delivery service to application programs.

Best-effort Service Best-Effort is a unitary and simple service model. Without being approved, but after notifying the network, the application can send any number of packets at any time. The network tries its best to send the packets, but delay and reliability cannot be ensured. Best-Effort is the default service model of the Internet. It can be applied to various networks, such as FTP and E-Mail. It is implemented through the First In First-Out (FIFO) queue.

filler panel A piece of board to cover vacant slots, to keep the frame away from dirt, to keep proper airflow inside the frame, and to beautify the frame appearance.

board An electronic module consisting of chips and other electronic components mounted on a flat, rigid substrate on which conductive paths are laid between the components.

BootROM BootROM is short for Boot Read-Only Memory. It caches the startup program of communication devices.

BRAS see **Broadband Remote Access Server**.

bridge A device that connects two or more networks and forwards packets among them. Bridges operate at the physical network level. Bridges differs from repeaters because bridges store and forward complete packets, while repeaters forward all electrical signals. Bridges differ from routers because bridges use physical addresses, while routers use IP addresses.

broadband Characteristic of any network technology that multiplexes multiple, independent network carriers onto a single cable, usually using frequency division multiplexing. The advantage of broadband is less cable, and the disadvantage is the high cost for equipment at connections.

Broadband Remote Access Server It is a new type of access gateway for broadband network. As a bridge between backbone networks and broadband access networks, Broadband Remote Access Server provides methods for fundamental access and manages the broadband access network. It is deployed at the edge of network to provide broadband access services, convergence, and forwarding of multiple services, meeting the demands for transmission capacity and bandwidth utilization of different users. Hence, Broadband Remote Access Server is a core device for the broadband users' access to a broadband network.

broadcast A packet delivery system that delivers a copy of a given packet to all hosts that attach to it, is said to broadcast the packet.

broadcast address A group address that means "everyone". The 802 broadcast address is a bit string of 48 1's.

broadcast domain Broadcast domain describes a group of network stations that receives broadcast packets originating from any device within the group. Broadcasts do not pass through a router, which bound the domains. In addition, the set of ports between which a device forwards a multicast, broadcast, or unknown destination frame.

broadcast storm A phenomenon of extreme congestion, usually caused by bugs in implementations or ambiguities in protocol specifications. A broadcast storm occurs when broadcast or multicast packets flood the subnet, creating excessive traffic and degrading the network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm.

bus	A path or channel for signal transmisstion. The typical case is that, the bus is an electrical connection that connects one or more conductors. All devices that are connected to a bus, can receive all transmission contents simultaneously.
bus topology	A bus network is a multi-point connection in which stations are connected to a single cable called a bus. In bus topology, all stations share a single media. Ethernet is one of the most popular LANs that used bus topology.

4 C

cable tray Cabling rack is an indespensible and helpful component in an equipment room (ER) for modern communications. It takes the weight of all cables and provides a path for wiring and a fixed pivot for devices. At the same time, it decorates the ER.

CAPEX see **CAPital Expenditure**.

CAPital Expenditure Capital expenditures ("CAPEX") are expenditures used by a company to acquire or upgrade physical assets such as equipment, property, industrial buildings. In accounting, a capital expenditure is added to an asset account (i.e. capitalized), thus increasing the asset's basis.

CAR see **Committed Access Rate**.

carrier An analog signal of fixed amplitude and frequency that is combined with a data-carrying signal to produce an output signal suitable for transmitting data.

Carrier Ethernet The Carrier Ethernet (CE) refers to carrier-class Ethernet. CE has the same capabilities as the traditional Ethernet in terms of ensuring QoS, security, and operation and management of services. From the perspective of the provider, the CE technology extends the application of the Ethernet technology from corporate networks to telecommunication networks. From the perspective on network layers, the CE technology extends the application of the Ethernet technology from LANs to MANs and WANs.

Carrier Sense Multiple Access with Collision Detection A contention scheme for allocating bandwidth on a shared bus. A characteristic of network hardware that operates by allowing multiple stations to contend for access to a transmission medium by listening to see if the medium is idle, and a mechanism that allows the hardware to detect when two stations simultaneously attempt transmission. Examples are 802.3 and Ethernet.

CBS see **Committed Burst Size**.

CCM Termination CCMs are generated and also terminated by MEPs. A MEP forwards received CCMs at a higher level but drops CCMs at a lower level or at the same level. In this manner, CCMs from a low-level MD are confined within the bounds of the MD.

CCS see **Common Channel Signaling**.

CE see **Customer Edge**.

Central Processing Unit The Central Processing Unit (CPU) is the brains of the computer. Sometimes referred to as the processor or central processor, the CPU is where most calculations take place.

Challenge Handshake Authentication Protocol	A method to periodically verify the identity of the peer using a 3-way handshake. During the setting up of a link, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged. CHAP provides protection against playback attack.
CHAP	see **Challenge Handshake Authentication Protocol**.
checksum	A small, integer value computed from a sequence of octets by processing them as integers and computing the sum. A checksum is used to detect errors that result when the sequence of octets is transmitted from one machine to another. Generally, protocol software computes a checksum and appends it to a packet during transmission.
CIDR	see **Classless InterDomain Routing**.
ciphertext	The output of an encryption algorithm. The encrypted form of a message or data.
CIR	see **Commit Information Rate**.
circuit switching	A method of communicating in which a dedicated communication path is established between two devices through one or more intermediate switching nodes. Unlike packet switching, digital data are sent as a continuous flow of bits. Bandwidth is guaranteed, and delay is essentially limited to propagation time. The telephone system uses circuit switching.
CIST Root	CIST root refers to the root switch of CIST.
Class of Service	Class of Service is abbreviated to CoS. CoS is a rule for queuing. It classifies the packets according to the service type field or the tag in packets, and specifies different priorities for them. All the nodes in DiffServ domain forwards the packets according to their priorities.
Class Queue	In HQoS scheduling, packets of the FQ, after CQ scheduling, enter the CQ on the port, together with common packets.
Class Selector	The service class of Class Selector (CS) is identical to the IP precedence. The DSCP value for CS PHB is "XXX000" ("X" can be 0 or 1.)
Class Selector Code Point	Bits 0 to 2 in DSCP are class selector code point (CSCP) and they indicate a specific type of DSCP.
classifier	An entity which selects packets based on the content of packet headers according to defined rules.
Classless InterDomain Routing	An addressing and routing scheme that uses a group of contiguous class C addresses instead of class B addresses. CIDR was adopted as a temporary solution to the problem of class B address space exhaustion.
CLI	see **Command Line Interface**.
Client/Server	The model of interaction in a distributed system in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client. The program satisfying the request is called the server. It is usually easier to build client software than build the server software.
CODEC	CODEC means Coder-Decoder. Coder transforms analog data into a digital bit stream. Decoder transforms digital signals into analog data.
collision	A condition in which two packets are being transmitted over a medium at the same time. Their interference makes both unintelligible.

collision domain	The set of ports between which a repeater repeats a signal.
Command Line Interface	A form of interface between the operating system and the user in which the user types commands, using a special command language. Although systems with command-line interfaces are usually considered more difficult to learn and use, than those with graphical interfaces, command-based systems are usually programmable; this gives them flexibility that is not available in graphics-based systems that do not have a programming interface.
Commit Information Rate	Commit Information Rate (CIR) refers to the average rate at which tokens are placed into the token bucket. It means the average traffic rate. Commonly, the traffic rate should be slower than the committed information rate.
Committed Access Rate	Committed Access Rate is abbreviated to CAR. Token bucket is used. If the tokens in a bucket suffice to forward the packets, it is called traffic compliance or speed limit compliance; otherwise, it is called traffic non-compliance or speed limit non-compliance. CAR has three indexes namely: Committed Information Rate (CIR), Committed Burst Size (CBS), and Excess Burst Size (EBS). It measures and monitors the traffic after the evaluation on traffic according to the preset rules.
Committed Burst Size	Committed Burst Size (CBS) refers to the capacity of the token bucket. It specifies the maximum rate of burst traffic. The maximum burst size should be larger than the packet length.
Common and Internal Spanning Tree	CIST is a single spanning tree generated by STP and MSTP computing and connects all devices of a switching network.
Common Channel Signaling	The technique in which network control signals are separated from the associated voice or data path by placing the signaling from a group of voice or data paths on a separate channel dedicated only to signaling.
Common Spanning Tree	CST is a single spanning tree that connects all the MST regions in a network. Taking every MST region as a íswitchí , the CST can be regarded as their spanning tree generated with STP/RSTP.
Complex Traffic Classification	Complex traffic classification (CTC) organizes packets into different classes according to packet information contained in an Access Control List (ACL) rule. Packet information can be a quintet, which consists of the source address, source port number, protocol ID, destination address, and destination port number. Packet information can also be TCP SYN. Traffic classification is usually based on the information encapsulated in the header of a packet; it does not consider the content of a packet.
CON	see **Console**.
congestion	The phenomenon results from that the service rate is lowered because the resources do not suffice during the packet delivery. It brings in a series of negative effects, influencing the QoS.
Congestion Avoidance	Congestion avoidance is a type of flow control technique, which is used to reduce overload in the network by controlling traffic. When congestion occurs, or aggravates, the devices automatically discards packets, by watching the used network resources, such as queues and memory buffers.
congestion management	It is a flow control measure to alleviate the competition for network resources. It puts packets into a queue for caching when congestion occurs on the network, and determines the forwarding order of packets according to a queuing policy.
connection-oriented	A service in which a connection-setup procedure must be implemented before data can be exchanged between two users.

connectionless A service in which data is presented, complete with a destination address, and the network delivers it on a best-effort basis, independent of other data being exchanged between the same pair of users.

Connectivity Check Ethernet CFM can detect the connectivity between MEPs. The detection is achieved by each MEP transmitting a Continuity Check Message (CCM) periodically. This detection is called CC detection.

Console A control unit, such as a terminal, through which a user communicates with a computer. In microcomputers, the console is the cabinet that houses the main components and controls of the system, sometimes including the screen, the keyboard, or both. With the MS-DOS operating system, the console is the primary input (keyboard) and primary output (screen) device, as evidenced by the device name CON.

control bus The control bus carries control signals from the control unit to the computer components in order to control the operation of each component.

control plane The control plane performs the call control and connection control functions. Through signalling, the control plane sets up and releases connections, and may restore a connection in case of a failure. The control plane also performs other functions in support of call and connection control, such as routing information dissemination.

control unit It is an important part of the main control unit and handles all communication protocols. As the agent of users, the control unit manages the system and monitors the performance according to the instructions of users, and returns the information on the running of devices to the users. At the same time, it supervises and maintains the interface board, the switching module, fans, and the power supply.

convergence It refers to the speed and capability for a group of networking devices to run a specific routing protocol. It functions to keep the network topology consistent.

convergence layer The convergence layer is a "bridge" between the access layer and the core layer. It provides the convergence and forwarding functions for the access layer. It processes all the traffic from the access layer devices, and provides the uplinks to the core layer. Compared with the access layer, the convergence layer devices should have higher performances, fewer interfaces and higher switching rate. In the real network, the convergence layer refers to the network between UPEs and PE-AGGs.

core layer The core layer functions as the backbone of high speed switching for networks, and it provides high speed forwarding communications. It has a backbone transmission structure that provides high reliability, high throughput, and low delay. The core layer devices must have a good redundancy, error tolerance, manageability, adaptability, and they support dual-system hot backup or load balancing technologies. In a real network, the core layer includes the IP/MPLS backbone network consisting of NPEs and backbone routers.

CoS see **Class of Service**.

CPU see **Central Processing Unit**.

CRC see **Cyclic Redundancy Check**.

CS see **Class Selector**.

CSCP see **Class Selector Code Point**.

CSMA/CD see **Carrier Sense Multiple Access with Collision Detection**.

Customer Edge Customer Edge (CE) equipment that is directly connected with the service provider. In a VPN based on MPLS, a CE device can be a router, switch, or even a host.

Cyclic Redundancy Check	A type of FCS computed by treating bit strings as polynomials with binary coefficients. The CRC is the remainder resulting from division by the CRC polynomial. Packet switching network hardware computes a CRC and appends it to a packet during transmission.

5 D

D-channel D is short for data. In ISDN, D channel is the signaling channel used to carry messages on the initialization and termination of a session, caller identification, call forwarding, and call negotiation.

data bus The data bus connects multiple data processing units for the reception and transmission of the data between those units.

Data Circuit-terminating Equipment In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. The DCE may be separate equipment, or an integral part of the DTE, or of intermediate equipment. The DCE may perform other functions that are normally performed at the network end of the line.

Data Terminal Equipment Equipment consisting of digital end instruments that convert the user information into data signals for transmission, or reconvert the received data signals into user information.

datagram A service in which delivery is on a "best-effort" basis. This term is also sometimes used for a piece of information presented to a network that provides a datagram service.

DCE see **Data Circuit-terminating Equipment**.

default route The prefix that matches any address, such as the zero-length prefix in longest prefix routing.

defective packet attack Defective packet attack is used to send a defective IP packet to the destination system so that the system crashes when it processes the IP packet. The main defective packets include Ping of Death and Teardrop.

demultiplexing To separate from a common input into several outputs. Demultiplexing occurs at many levels. Hardware demultiplexes signals from a transmission line based on time or carrier frequency to allow multiple, simultaneous transmissions across a single physical cable.

Denial of Service Denial of Service (DoS) attack is used to attack a system by sending a large number of data packets. As a result, the system cannot receive requests from the valid users or the host is suspended and cannot work normally. DoS attack includes SYN flood, Fraggle, and others. The DoS attacker only stops the valid user from accessing resources or devices instead of searching for the ingresses of the intranet.

Designed Interface The designated interface of a device is the interface of its designated switch, through which the designated switch forwards BPDU to it.

Designed Switch The designated switch of a device is the one that is connected with it and forwards the BPDU to it.

Destination Address	Destination Address
DHCP	see **Dynamic Host Configuration Protocol**.
Differentiated Services	Differentiated Services is abbreviated to DiffServ. DiffServ is a multi-service model that satisfies different demands for QoS. Application programs do not need to inform the communication devices before sending packets, and the network does not need to maintain the status of each stream. DiffServ specifies the QoS for each packet, providing special services including packet classification, traffic shaping, traffic policing, and queuing. It is mainly realized through CAR and queuing.
Differentiated Services Code Point	In RFC 2474, the IETF Diff-Serv workgroup redefines bits 0 to 5 of the ToS field and IP precedence field in the IP packet header as DSCP.
Digital Subscriber Line Access Multiplexer	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually situated in the main office of a telephone company that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques.
Directly-connected Neighbor	There are no intermediate devices between two adjacent devices which are directly connected through links. The two devices are called directly-connected neighbors to each other.
distance vector routing	A class of routing update protocols that use a distributed shortest path algorithm in which each participating router sends its neighbors a list of networks it can reach and the distance to each network.
DoS	see **Denial of Service**.
dotted decimal notation	The syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10, with periods (dots) separating them. Many TCP/IP application programs accept dotted decimal notation instead of destination machine names.
DSCP	see **Differentiated Services Code Point**.
DSLAM	see **Digital Subscriber Line Access Multiplexer**.
DTE	see **Data Terminal Equipment**.
dual-homing	It is a network topology structure. Devices are connected to the network through two independent links which work in the master or slave mode. It is often used in the transmission of network that requires higher safety and reliability.
Dynamic Host Configuration Protocol	Designed as a successor to BOOTP, the Dynamic Host Configuration Protocol (DHCP) extends BOOTP in several ways. Similar to the Bootstrap Protocol (BOOTP), DHCP also works in the client/server mode. With DHCP, a client can dynamically request configuration information from a DHCP server, including the assigned IP address, the subnet mask and the default gateway. The DHCP server can reply based on a certain policy.
dynamic LACP mode l	In the dynamic LACP mode, the creation of the Eth-Trunk, the addition of member interfaces, and the selection of active interfaces are completed by negotiating parameters through LACPDUs. That is, if the dynamic LACP is enabled on two directly connected devices, you do not need to create the Eth-Trunk and specify the interfaces that are member interfaces of the aggregation group on these two devices. The link aggregation is completed automatically by negotiating parameters through LACPDUs on these two devices.

6 E

Edge Interface Edge interface refers to the interface of a region that is located at the edge of the region and is connected with another MST region or connected with another region that runs STP or RSTP.

EF see **expedited forwarding**.

EIA see **Electronics Industry Association**.

EIR see **Excess Information Rate**.

Electromagnetic Compatibility The capability of performing its individually designed function in an electromagnetic environment, without causing or suffering unacceptable degradation to or from other equipment in the same environment. It is a critical indicator of system reliability of the telecommunications equipment.

Electromagnetic Discharge An electrostatic discharge (ESD) is a sudden flow of electric current through a material that is normally an insulator. An indicator of the capability against electrostatic discharge. It is categorized into air discharge and contact discharge.

ElectroMagnetic Interference Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment.

ElectroMagnetic Shielding The process of limiting the coupling of an electromagnetic field between two locations. Typically, it is applied to enclosures, separating electrical circuits from external surroundings, and to cables, separating internal wires from the surroundings that the cable passes through.

Electronics Industry Association A standards organization for the electronics industry. Known for RS232 and RS422 standards that specify the electrical characteristics of interconnections between terminals and computers or between two computers.

embedded system Microprocessors used to control devices such as appliances, automobiles, and machines used in business and manufacturing. An embedded system is created to manage a limited number of specific tasks within a larger device or system. An embedded system is often built onto a single chip or board, and is used to control or monitor the host device-usually with a little or no human intervention and often in real time.

EMC see **Electromagnetic Compatibility**.

EMI see **ElectroMagnetic Interference**.

EMS see **ElectroMagnetic Shielding**.

encapsulation	The technique used by layered protocols in which a lower level protocol accepts a message from a higher-level protocol and places it in the data portion of the low level frame. Handing protocol A's packets, the packets are complete with A's header information, as data carried by protocol B. Encapsulated protocol A packets have a B header, followed by a A header, followed by the information that protocol A is carrying its own data. Note that A could equal to B, as in IP inside IP.
Enhanced VLAN Mapping	The enhanced VLAN mapping technology provides abundant service features and flexible networking capabilities. Different services use different 802.1p priorities, and C-VLANs with different 802.1p priorities are mapped to different S-VLANs to obtain different service qualities.
Enhanced VLAN Stacking	The enhanced VLAN stacking technology can isolate the ISP network from the user network and provide abundant service features and flexible networking capabilities. When the device adds the outer VLAN tag, the 802.1p priority of the C-VLAN is mapped from the C-VLAN to the S-VLAN. In this manner, the 802.1p priority of the C-VLAN is applied to the whole ISP network. You can reset the 802.1p priority of the S-VLAN as required.
EPLD	Erasable Programmable Logic Device (EPLD) is a programmable logic array designed to perform a user-erasable programmable function.
EPROM	Erasable Programmable Read Only Memory (EPROM) is a permanent memory which can only be read, not written or erased.
Errored fame	An errored frame second is a one-second interval during which at least one errored frame is detected.
ESD	see **Electromagnetic Discharge**.
Ethernet	The original CSMA/CD LAN invented by Xerox and standardized by Digital, Intel, and Xerox. Ethernet is a best-effort delivery system that uses the CSMA/CD technology.
Ethernet OAM at the Link Level	Ethernet OAM at the link level, such as Ethernet in the First Mile OAM (EFM OAM) defined in IEEE 802.3ah, provides the following functions for the link between the two directly connected devices: Link connectivity check, Link monitoring, Remote failure indication, Remote loopback.
Ethernet OAM at the Network Level	Ethernet OAM at the network level, such as Ethernet Connectivity Fault Management (CFM) defined in IEEE 802.1ag, provides the following functions for the network: Fault detection, Fault notification, Fault verification, and Fault location.
ETSI	see **European Telecommunications Standards Institute**.
European Telecommunications Standards Institute	European Telecommunications Standards Institute (ETSI) was co-founded by Posts, Telegraphs, Telephones (PTT), and European Community (EC). It is responsible for recommending telecom standards to Europe.
Excess Information Rate	In a specific condition, the Excess Information Rate is out of the safety threshold; it equals the result of the actual transmission rate without the safety rate.
expedited forwarding	Expedited Forwarding (EF) is the highest order QoS in the Diff-Serv network. EF PHB is suitable for services that demand low packet loss ratio, short delay, and broad bandwidth. In all the cases, EF traffic can guarantee a transmission rate equal to or faster than the set rate. The DSCP value of EF PHB is "101110".

7 F

fan frame A frame that encloses fans.

Fast Ethernet Fast Ethernet refers to any network that supports transmission rate of 100Mbits/s. The Fast Ethernet is 10 times faster than 10BaseT, and inherits frame format, MAC addressing scheme, MTU, and so on. Fast Ethernet is extended from the IEEE802.3 standard, and it uses the following three types of transmission media: 100BASE-T4: 4 pairs of phone twisted-pair cables 100BASE-TX: 2 pairs of data twisted-pair cables 100BASE-FX: 2-core optical fibers The shorthand method defined by IEEE is used here. 100 stands for rate.

Fault management The fault management of Ethernet OAM includes the connectivity detection of the network, the location and the confirmation of failures, protection switching triggered by the cooperation with automatic protection switching protocol.

Fault Notification When a link event about a fault occurs on the local interface, the local interface notifies the peer of the fault through OAMPDUs. The local interface then records the event in the log, and reports it to the NMS. This is called fault notification.

fault tolerance Fault tolerance is an attribute associated with a system that provides continuous service in the presence of faults.

fault tolerance The extent to which a functional unit continues to operate at a defined performance level, even though one or more of its components are malfunctioning.

Fault Verification If a MEP receives no CCMs from an RMEP within three consecutive intervals for sending CCMs, a connectivity fault between the MEP and RMEP is verified.

FDM see **Frequency Division Multiplexing**.

FE see **Fast Ethernet**

FEC see **Forwarding Equivalence Class**.

FIB see **Forward Information Base**.

FIFO see **First In First Out**.

File Transfer Protocol A client-server protocol which allows a user on one computer to transfer files to and fro from another computer over a TCP/IP network. It also function as the client program that the user executes to transfer files.

fireware	Similar to the partition wall used to prevent fire from spreading in the building, the Internet firewall is one or a group of system(s) to implement access control policy. It can monitor the access channels between the Trust zone (the internal network) and the Untrust zone (the external network) to prevent the hazard from external networks. Firewall, as a network security device, includes hardware and software. Firewalls filter or reject incoming and outgoing data based on specific rules defined in any layer of the OSI model.
First In First Out	A method of processing a queue, in which items are removed in the same order in which they were added- the first in, is the first out. Such an order is similar in case of a printer that has documents waiting to be printed.
Flapping	When a route in an IP network is in the down state, the router that knows about the change advertises it to neighboring routers. Those routers then recalculate their routes. Route flapping occurs when such cases occur rapidly and possibly on a large scale.
Flash Memory	Flash memory is a form of non-volatile memory that can be electrically erased and reprogrammed.
flow control	Telling the source of data to stop till there are buffers available.
Flow Queue	HQoS enables a device to perform user-specific queue scheduling. You can restrict the bandwidth of a user by setting the CIR and PIR. A user's service can be divided into eight flow queues. You can configure the PQ, or WFQ scheduling and WRED for each flow queue, and configure the traffic rate and burst size for traffic shaping.
Forward Information Base	In data communication, a table of information that provides network hardware (bridges and routers) with the directions needed to forward packets of data to locations on other networks. The information contained in a routing table differs according to whether it is used by a bridge or a router. A bridge relies on both the source (originating) and destination addresses to determine where and how to forward a packet.
forwarding capacity	It is measured according to the length of minimum packet that can be processed. For example, the length of a minimum Ethernet packet is 64 bytes plus the frame cost 20 bytes, totaled 84 bytes. For a full duplex interface at 1Gbit/s, the forwarding capacity at wire speed is 1Gbit/s/((64+20)*8bit)=1.488Mpps. For a full duplex interface at 100Mbit/s, the forwarding capacity at wire speed is 100Mbit/s/((64+20)*8bit)=0.150Mpps.
Forwarding Equivalence Class	Forwarding Equivalence Class is abbreviated to FEC. As a class-based forwarding technology, MPLS classifies the packets with the same forwarding mode, and the process is called Forwarding Equivalence Class. Packets with the same FEC are processed similarly on an MPLS network. It is flexible to divide FECs, and it can be a combination of the source address, the destination address, the source port, the destination port, the protocol type, the VPN, and so on.
forwarding table	A forwarding table contains two entries: a network number and a cost to that network from the router. Each router knows every network number on the XNS Internet. The routers assign a cost, more commonly called a hop, to each network number. The hop count is the number of routers between a router and the associated network number on the internet. Routers update their tables dynamically using the routing information protocol.
fragmentation	The act of breaking a packet into multiple pieces. These packets are then put back together in the process of reassembly. Packets are broken down because the packet must be transmitted over a link for which a packet might be too large.
frame	A group of bits that includes data plus one or more addresses, and other protocol control information. Generally refers to a link layer (OSI layer 2) protocol data unit.

Frequency Division Multiplexing	The method of passing multiple, independent signals across a single medium by assigning each signal a unique carrier frequency. The hardware used to combine signals is called a multiplexer and the hardware used to separate them is called a demultiplexer.
FTP	see **File Transfer Protocol**.
full duplex	Also called duplex. Refers to two-way electronic communication that takes place in both directions at the same time.
full mesh topology	A topology in which any two devices are connected, and there is a link between any two devices. Such a network provides a higher redundancy, and the deployment cost is very high although it prevents the single-point failure on links.

8 G

Generic Traffic Shaping Applied on the outbound interface, the General Traffic Shaping (GTS) is a traffic management technology used to restrict a certain type of traffic sent from the interface. Being the same as CAR, GTS also uses the token bucket technology to control the traffic.

Gigabit Ethernet see **Gigabit Ethernet**

Gigabit Ethernet It runs at 1000Mbit/s. Gigabit Ethernet uses a private medium, and it does not support coaxial cables or other cables. It also supports the channels in the bandwidth mode. If Gigabit Ethernet is, however, deployed to be the private bandwidth system with a bridge (switch) or a router as the center, it gives full play to the performance and the bandwidth. In the network structure, Gigabit Ethernet uses full duplex links that are private, causing the length of the links to be sufficient for backbone applications in a building and campus.

Global System for Mobile communications A second-generation digital cellular telecommunication system which was first planned in the early 1980s. GSM, originally developed as a pan-European standard for digital mobile telephony, has become the worldí»s most widely used mobile system. It is used on the 900 MHz and 1800 MHz frequencies.

grounding terminal It is a connection terminal on a communication device. It is used to connect the device with grounding cables, maintaining a tight connection between the device and the grounding electrode.

group address An address to which transmissions are sent, intended for receipt by a set of recipients.

Group Queue One group queue (GQ) consists of multiple SQs that are bound together to carry out Level-3 scheduling.GQ functions to limit the traffic rate of a group of users together. The PIR must not be less than the sum of CIRs of the SQ. Otherwise, the traffic rate of an SQ in the GQ cannot be guaranteed. GQ is also a virtual queue. Each SQ can be bound to only one GQ. If it is not bound to any GQ, the device does not perform Level-3 scheduling.

GSM see **Global System for Mobile communications**.

9 H

half-duplex Refers to two-way electronic communication that takes place unidirectionally at a time. Communication between people is half-duplex when one person listens while the other speaks.

hardware address The low-level addresses used by physical networks. Each type of network hardware has its own addressing scheme. For example, an Ethernet address is 48 bits.

hash function A function that maps a variable-length data block or message into a fixed-length value called a hash code. The function is designed in such a way that, when protected, it provides an authenticator to the data or message. Also referred to as a message digest.

Hierachical Quality of Service Hierarchical QoS (HQoS) is a type of QoS that can control the traffic of users, and perform the scheduling according to the priority of user services. HQoS has a perfect traffic statistics function, and the administrator can monitor the usage of bandwidth of each service. Hence, the bandwidth can be allocated reasonably through traffic analysis.

hops The simplest routing metric in which each link has a cost of 1. This function counts the number of times a packet must be forwarded.

Host registration A host is allowed to join or leave a multicast group statically to register the multicast members.

host route An IP destination with a 32-bit mask advertised in the routing protocol, that is, a destination that is single node.

hot plugging It is a function that allows users to take out and replace the faulty HD, power module or boards, without closing the system and powering down. This improves the capability of the system to recover from disaster, the scalability and flexibility, and so on.

HTTP see **Hyper Text Transport Protocol**.

hub An electronic device to which multiple computers attach, usually using twisted pair wiring. A hub works at physical levels, and simulates a network that interconnects the attached computers. The device acts as the center of a star topology.

Hyper Text Transport Protocol An protocol developed by IETF for web based file transfer. HTTP is used to carry requests from a browser to a Web server and to transport pages from Web servers back to the requesting browser. Although HTTP is almost universally used on the Web, it is not a secure protocol.

10 I

IAB	see **Internet Architecture Board**.
IANA	see **Internet Assigned Numbers Authority**.
ICMP	see **Internet Control Message Protocol**.
IEC	see **International Electrotechnical Commission**.
IEEE	see **Institute of Electrical and Electronics Engineers**.
IETF	see **Internet Engineering Task Force**.
IGMP	see **Internet Group Management Protocol**.
IGP	see **Interior Gateway Protocol**.
in-band networking	It is the antonym of out-band networking. See in-band networking.
in-band signaling	In-band signaling is the act of transmitting metadata and network control information together with regular data sent.
Inactive Interface	In link aggregation, the interfaces that do to forward data in the inactive status are called inactive interfaces.
Inactive Link	In the link aggregation group, the links connected to inactive interfaces are inactive links.
information center	A specialized type of computer system dedicated to information retrieval and decision-support functions. The information in such a system is usually read-only and consists of data extracted or downloaded from other production systems.
Institute of Electrical and Electronics Engineers	A membership-based organization based in New York City that creates and publishes technical specifications and scientific publications. The standards organization works for most of the layer 2 protocols.
integrated routing	Using a single routing protocol to carry information about multiple network layer protocols.
Integrated Service	Integrated Service is abbreviated to IntServ. IntServ is an integrated service model that reserves network resources by exchanging signaling before transmitting packets. The network meets the demand of application programs for QoS if the following packets are in the given range of traffic. It is mainly realized through Resource Reservation Protocol (RSVP).

interface	A shared boundary, for example, the boundary between two subsystems or two devices. Specifically, it refers to the part used by communication devices to exchange data with other devices on the network and devices use the boundary to interact. It functions to exchange data between the device that the interface is located and other network devices.
Interior Gateway Protocol	The generic term applied to any protocol used to propagate network reachability and routing information within an autonomous system. The most commonly used IGPs are the RIP, OSPF, and IS-IS.
Intermediate System to Intermediate System	A protocol used by network devices (routers) to determine the best way to forward datagrams or packets through a packet-based network, a process called routing.
Internal Spanning Tree	An MST region has an Internal Spanning Tree (IST), which is a fragment of CIST and is also called MSTI0.
Internation Telecommunication Union	A United Nations Agency with the purpose of defining standards for telecommunications, TV frequency, satellite and telephone, network architecture, and tariff for global communication. It also employs technical experts and provides equipment for developing countries to help they improve technically.
International Electrotechnical Commission	The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards function as a basis for national standardization and as references when drafting international tenders and contracts.
International Organization for Standardization	A Geneva-based international organization that comprises of the national standards of 130 countries. The ISO aims to develop internationally accepted technical standards to promote information exchange and barrier-free trade worldwide.
International Telecommunication Union - Telecommunication Standardization Sector	The ITU Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. Prior to 1992, it was known as the International Telegraph and Telephone Consultative Committee (CCITT, from the French name "Comité consultatif international téléphonique et télégraphique").
Internet	Largest global internetwork, connecting tens of thousands of networks worldwide and having a "culture" that focuses on research and standardization based on real-life use. Many leading-edge network technologies come from the Internet community.
Internet Architecture Board	A small group of people who set policies and directions for TCP/IP and global Internet. It is an elected body that listens to formal appeals and writes network architecture documents.
Internet Assigned Numbers Authority	The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
Internet Control Message Protocol	An integral part of the Internet Protocol (IP) that handles error and control messages. Specifically, routers and hosts use ICMP to send reports of problems about packets that return to the original source that sent the packet. ICMP also includes an echo request/ reply used to test whether a destination is reachable and responding.
Internet Engineering Task Force	A group of people closely connected to the IAB who work on the design and engineering of TCP/IP and global Internet. The IETF is divided into regions, with each having an independent manager. Regionsare further divided into working groups.

Internet Group Management Protocol	A protocol that hosts use to keep local routers apprised of their membership in multicast groups. When all hosts leave a group, routers no longer forward packets that arrive for the group.
Internet Protocol	The TCP/IP standard protocol that defines the IP packet as the unit of information sent across an internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two fundamental protocols. IP is standardized in RFC 791.
Internet Service Provider	An ISP is a business or organization that sells access to the Internet and related services to consumers.
interrupt	A temporary break in the CPU's normal execution of program instructions, to allow it to handle a request from a peripheral.
intersectant rings	It is a concept in geometry. There are more than two public nodes between two ring networks. The network is more complex if there are many intersecting nodes. Most devices support that two rings are intersected at two nodes. Thus, a node in the forwarding state is called an Active node, and the other in the blocking state is called a Standby node.
IP	see **Internet Protocol**.
IP address	An exclusive 32-bit address that is allocated to the host attached to the Internet. It is abstracted from the physical address. An IP address consists of two parts: one is the network ID, and the other is the host ID. The structure effectively facilitates routing. IP addresses are allocated by the Network Information Center (NIC) under the Defense Data Network (DDN) of U.S.A.
IP spoofing attack	To get an access right, an intruder generates a packet carrying a bogus source address which can make an unauthorized client access the system applying the IP authentication even in the root authority. In this way, the system can also be destroyed even though the response packet does not reach the system.
IPTV	In the IPTV system, video is transmitted in IP packets. Also called "TV over IP", IPTV uses streaming video techniques to deliver scheduled TV programs or video-on-demand (VOD). Unlike transmitting over the air or through cable to a TV set, IPTV uses the transport protocol of the Internet for delivery and requires either a computer and software media player or an IPTV set-top box to decode the images in realtime.
ISO	see **International Organization for Standardization**.
ISP	see **Internet Service Provider**.
ITU	see **Internation Telecommunication Union**.
ITU-T	see **International Telecommunication Union - Telecommunication Standardization Sector**.

11 L

label A label is a set of symbols that is invented so as to identify the data blog or programm segment. In the MPLS network, the label is a short identifier with a fixed length and local meanings, and is used to mark the FEC that a packet belongs to.

LACP Preemption In the static LACP mode, when a link of active links fails, the system chooses the link of the highest priority from slave links to replace the faulty one. After a period, the replaced faulty link recovers, and the priority of this link is higher than the link that replaces the faulty one. In this case, the recovered link switches to the active state, and the slave link returns to its original state. This is called LACP Preemption.

LACP Preemption Delay The LACP preemption delay refers to the period for triggering the preemption.The LACP preemption delay is set to prevent instable data transmission of the Eth-Trunk due to frequent change of the status of certain links.

LAN see **Local Area Network**.

last mile The 'Last Mile'is the final leg of delivering connectivity from an ISP network to a customer. It is the smallest branch of the network tree and is often the hardest element to satisfy cost-effectively.

Layer 2 Multicast When Ethernet is used as the link layer, Layer 2 multicast uses multicast MAC addresses for traffic transmission. Therefore, a technology must exist to map the IP multicast address to the multicast MAC address.

Link Aggregation Control Protocol Link aggregation refers to a method of bundling a group of physical interfaces together as a logical interface to increase bandwidth and reliability. For related protocols and standards, refer to IEEE 802.3ad.

Link Aggregation Control Protocol Data Unit LACP exchanges information with the peer through LACPDUs.

Link Aggregation Group The logical link that is created by bundling several physical links together is called link aggregation group or trunk.

Link Layer Discovery Protocol The Link Layer Discovery Protocol (LLDP) is an L2D protocol defined in IEEE 802.1ab. Using the LLDP, the NMS can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand.

Link Monitoring Link monitoring is a mechanism for an interface to notify the peer of the fault through OAMPDUs when the interface detects that the number of errored frames, errored codes, or errored frame seconds reaches or exceeds the specified threshold.

Linktrace Message	The message sent by the initiator MEP of 802.1ag MAC Trace to the destination MEP is called Linktrace Message(LTM). LTM includes the Time to Live (TTL) and the MAC address of the destination MEP2.
Linktrace Reply	For 802.1ag MAC Trace, the destination MEP replies with a response message to the source MEP after the destination MEP receives the LTM, and the response message is called Linktrace Reply(LTR). LTR also includes the TTL that equals the result of the TTL of LTM minus 2.
LLC	see **Logical Link Control**.
LLDP Agent	An LLDP agent is the protocol entity that manages LLDP operations for an interface.
LLDP Local System MIB	The LLDP local system MIB stores information about the local station, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.
LLDP Management Address	The LLDP management address (hereinafter referred to as the management address) is used by the NMS to identify device and implement network management. The management address identifies a device. This facilitates the layout of the network topology and network management with a clear view of the topology status. The management address is carried in the management address Type-Length-Value (TLV) field in an LLDP frame to be transmitted to neighbor stations.
LLDP Remote System MIB	The LLDP remote system MIB stores information about adjacent stations, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.
LLDP Traps	When the LLDP local system MIB or the LLDP remote system MIB changes, the device sends trap message to the NMS for updating the topology.
LLDPDU	The LLDPDU is the data unit that carries the local device information encapsulated in the data field in an LLDP frame.
load balancing	Load balancing is an approach to balance the load. It imporves the available resources for a computer system, network or HD sub-system. This enables even allocation of the data or configurations. For example, a group of physical links form a logical link, which balances the transmission of services over member links during data forwarding. This increases the bandwidth utilization and improves the reliability of links.
Local Area Network	A communication network that provides interconnection of a variety of data communicating devices within a small area. Examples include Ethernet and FDDI.
Local MEP	For the devices on the network enabled with Ethernet CFM, their MEPs are called local MEPs.
Logical Link Control	A sub layer of the data link layer defined by the IEEE 802 committee. A part of LLC defines the multiplexing fields. The other part gives optional types of service that can be run over 802 LANs.
Loop Protection	In MSTP, the re-selection of the root interface may result in a loop when the topology is changed. The loop-protection function can prevent network loop. If the root interface cannot receive the BPDU from the uplink device after the protection function is enabled, the root interface is set to be blocked. The previous blocked interface becomes the root interface and enter into the forwarding state if it can receive BPDU; it retains the state of being blocked and cannot forward packets if it cannot receive BPDU. This prevents the occurrence of a network loop.
Loopback Message	It refers to the loopback packet sent by the node that supports 802.2ag MAC Ping to the destination node. LBM message carries its own sending time.

Loopback Reply	For 802.2ag MAC Ping, the destination MEP replies with a response message to the source MEP after the destination MEP receives the LBM, and the response message is called Loopback Reply. The LBR carries the sending time of LBM, the receiving time of LBM and the sending time of LBR.
Low Priority Queuing	Queue scheduling is classified in the following descending order: PQ scheduling, WFQ scheduling, and Low Priority Queuing (LPQ). After packets are given PQ and WFQ scheduling, the remaining bandwidth can be assigned for LPQ scheduling.

12 M

MA A Maintenance Association (MA) is part of an MD. An MD can be divided into one or multiple MAs.

MAC see **Medium Access Control**.

MAC address The layer 2 address on IEEE LANs. For example, the 6-byte Ethernet address.

main control unit The full name is main control unit. It is also called main processing board. In a centralized system, the main control unit runs VRP to manage and monitor the parts. It also runs other protocols and processes packets, determining the forwarding and routing. Generally, the main control unit consists of CPU, switching or routing module, power module, and control module. For a distributed system, the main control unit focuses on the control of parts.

maintainability A measure that is easy and speedy, with which a system can be restored to operational status following a failure.

maintainability It refers to the capability of products to keep or be recovered to the normal state after repairing according to the given process and methods in a given time under the stipulated conditions.

major alarm An alarm indicating that the system has encountered faults that affect the quality of service, such as impairment of the capability of the device or resources. Treatment measures must be taken immediately to eliminate the faults during working hours.

MAN see **Metropolitan Area Network**.

Management Information Base Management Information Base (MIB) is a database of network performance information that is stored on a network agent for access by a network management station through SNMP packets. Managers can fetch or store these into databases.

management plane The management plane performs management functions for the transport plane, the control plane and the system as a whole. It also provides coordination between all the planes.

Manual Load Balancing Mode The manual load balancing mode is the most basic mode of link aggregation. In the manual load balancing mode, you must manually create the Eth-Trunk, add member interfaces to the Eth-Trunk, and specify active interfaces. The Link Aggregation Control Protocol Data Units (LACPDUs) are not involved. All the member interfaces forward data and perform load balancing.

mask see **address mask**.

Master Interface	Master interface is the interface in an MST region that is connected to the CIST root on the shortest path.
Maximum Transmission Unit	The largest amount of data that can be transferred across a given physical network. The MTU is determined by the network hardware.
MD	The Maintenance Domain (MD) refers to the network or the part of the network for which connectivity is managed by CFM. The devices in an MD are managed by a single ISP.
MD5	see **Message Digest Algorithm 5**.
Mean Time Between Failure	It is a key index to reflect the reliability of a product (particularly electric products). It embodies the capability of the product to retain its performance, and the measuring unit is hours. Specifically, it refers to the average working time between two failures, so it is also called Mean Failure Interval. It is only applicable to maintainable products. At the same time, the ratio of the total working hours over the number of failures of the product is the MTBF.
Mean Time To Repair	The average time that a device takes to recover from a failure.
Medium Access Control	A general reference to the low-level hardware protocols used to access a particular network. The term MAC address is often used as a synonym for physical addresses.
MEP	A Maintenance association End Point (MEP) is an end point within an MA.
MEP Database	There is a MEP database on each device enabled with Ethernet CFM. Each MEP database contains the local MEPs and RMEPs.
mesh topology	It is a network topology consisting of manageable segments in which redundant links are used between important devices. It effectively prevents the single-point failure on critical paths.
message	In data communication, messages are usually in an standard format with a heading, which establishes the address to which the message is sent and the text which is the actual message. It may also contain certain information to signify the end of the message.
Message Digest Algorithm 5	A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations of MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
Metropolitan Area Network	Any of the several new physical network technologies that operate at high speeds over distances sufficient for a metropolitan area.
MIB	see **Management Information Base**.
minor alarm	An alarm indicating that the system has encountered faults that does not have immediate effect on the quality of service. Troubleshooting must be done and measures must be taken on time to prevent the faults from causing adverse results.
MIP	A Maintenance association Intermediate Point (MIP) is an intermediate point within an MA.
mirror	It is an action to store a copy of a file to another archive site to release the load of the original site, or to provide an archive site closer to the users geographically.
Mirroring	The duplication of data for backup or to distribute network traffic among several computers with identical data.
Modem	Modulator-Demodulator. Modulator transforms a digital bit stream into an analog signal. Demodulator transforms an analog signal into a digital bit stream.

modulation	The process by which certain characteristic of one wave is varied in accordance with another wave or signal.
MP	Either a MEP or a MIP is called a Maintenance Point (MP).
MPLS	see **MultiProtocol Label Switching**.
MSAP Identifier	The MAC service access point (MSAP) identifier consists of the chassis ID and the port ID. The identifier is used as an index in the MIB.
MTBF	see **Mean Time Between Failure**.
MTTR	see **Mean Time To Repair**.
MTU	see **Maximum Transmission Unit**.
multi-homed host	A host using TCP/IP that has connections to two or more physical networks.
multicast	Multicast is a method to send a packet to multiple hosts at the same time. Multicast packet uses Class-D IP addresses as the destination, namely, from 224.0.0.0 to 239.255.255.255. Each multicast address stands for a multicast group, not a host.
Multicast Dynamic Forwarding entry	Dynamic forwarding entries are maintained by analyzing IGMP messages between hosts and the router through protocols that run on the link layer device. Dynamic forwarding entries are removed if they are not updated when the aging time expires.
Multicast MAC Address	The IANA specifies the high-order 24 bits of a multicast MAC address as 0x01005e, the 25 bit of a multicast MAC address as 0, and the low-order 23 bits as the low-order 23 bits of a multicast IP address.
Multicast routing	A multicast distribution tree is set up for transmitting packets from the multicast source to the receiver.
Multicast routing protocol	Multicast routing protocol is used to set up and maintain multicast routes, and to correctly and effectively forward multicast packets. The multicast route sets up a loop-free transmission path from the source to multiple receivers, that is, the multicast distribution tree.
Multicast Source Discovery Protocol	MSDP is a mechanism to propagate information about sources--hosts sourcing any type of data to a multicast group and associated multicast groups to all the multicast networks.
Multicast Static forwarding entry	Static forwarding entries are configured statically and do not age.
Multiple Spanning Tree Instance	Multiple spanning trees can be generated in an MST region. Every MST is independent of one another and is mapped with VLANs. Such a spanning tree is called an MSTI.
Multiple Spanning Tree Protocol	Multiple Spanning Tree Protocol (MSTP) is a new spanning tree protocol defined in IEEE802.1s. MSTP employs the concepts of region and instance. A big network is divided into regions according to different requirements. Instances are created in the regions and are mapped to VLAN. Network bridges transmit BPDU messages with information about regions and instances. Network bridges judge whether they belong to the region specified in the BPDU. RSTP with multiple instances are used within a region; while protocols, which RSTP are compatible with, are used between regions.
Multiple Spanning Tree Region	An MST region consists of several devices in a LAN and the network segments between them.
multiplexing	Sharing a communications channel by transmitting messages for multiple destinations with some indication of the intended recipient.

MultiProtocol Label Switching	Adding extra information to a layer 3 protocol. Developed due to a demand to make layer 3 forwarding decisions based on a small header with small addresses but is considered more useful as a method to mark packets for quality of service or fixing paths for traffic engineering.

13 N

NAT	see **Network Address Translation**.
NAT	see **Network Address Translator**.
Network Address Translation	An IETF standard that allows an organization to present itself to the Internet with lesser number of IP addresses than the number of nodes on its internal network. The NAT technology, which is implemented in a router, firewall or PC, converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of them through internal tables that it builds. When packets return from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine.
Network Address Translator	An admittedly useful kludge that sits between the network and the Internet, and translates network layer addresses so that your intranet can survive without addresses that are globally unique addresses.
Network Interface Card	The board that enables a computer to connect to a network.
Network Managememt System	A Network Management System (NMS) is a combination of hardware and software used to monitor and administer a network. Individual network elements (NEs) in a network are managed by an element management system.
network self-healing	The self-healing ability is an emergent behavior which is created out of the dynamic merging of the primary task of the network and behavior based on the current network status. When the service disruptions occur because the channels are faulty, the network switches the services to the standby channel through network self-healing so that the services can be restored in a short time.
Next Generation Network	A packet-based network that provides telecommunication services and utilizes multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access to users through different service providers. It supports generalized mobility which allows consistent and ubiquitous provision of services to users.
NGN	see **Next Generation Network**.
NIC	see **Network Interface Card**.

14 O

OAM see **Operation, Administration and Maintenance**.

OAMPDU OAM Protocol Data Unit

OC-3 see **Optical Carrier level**.

octet A unit of data that consists of exactly 8 bits, regardless of the number of bits a computer uses to represent a small amount of information such as a character.

Open Shortest Path First Link-state, is a hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol. See IS-IS.

Open System Interconnection Network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are implemented in hardware and software whereas the upper five layers are implemented only in software. The highest layer (the application layer) is closest to the user. The OSI reference model is used universally as a method for teaching and understanding network functionality. Similar in certain respects to SNA.

OPerating Expenditure Refer to Operating Expenditures, the on-going costs for running a product, business, or system.

Operating Support System Operating Support System (OSS) is originally used in the telecommunication world to describe the processes and teams that monitor the underlying networks. Predominantly looks after the functional and non-functional requirements of solutions/systems. Monitoring, end-to-end design, and error handling tend to be the main areas of work.

Operating System Operation System is abbreviated to OS. OS is the interface between users and computers. It manages all the system resources of the computer, and also provides an abstract computer for users. With the help of OS, users can use the computers without any direct operation on hardware. For the computer system, OS is a set of programs used to manage all system resources; for users, OS provides a simple and abstract method to use the system resources.

Operation, Administration and Maintenance A group of network management functions that provide network fault indication, performance information, and data and diagnosis functions.

OPEX	see **OPerating Expenditure**.
Optical Carrier level	Optical Carrier levels are defined for SONET by the ANSI to distinguish the bandwidth categories in SONET optical fiber network. The general rule for calculating the speed of optical carrier is as follows when a specification is given as OC-n, the speed equals n x 51.8 Mbit/s. For example, the optical interface speed of OC-3 is level 3, and is called Synchronous Transport Signal level 3 (STS-3). The speed is 155.52 Mbit/s that equals the STM-1 of ITU-T.
optical fiber	A thin filament of glass or other transparent material, through which a signal-encoded light beam may be transmitted using total internal reflection.
OS	see **Operating System**.
OSI	see **Open System Interconnection**.
OSS	see **Operating Support System**.
out-band networking	Outband networking uses the communication channel provided by the devices other than the managed devices to transport NMS information and to achieve the NM networking. Compared with in-band networking, it provides more reliable device management channel to locate and monitor devices on the network in real time when the managed device fails.
out-band signaling	It is the antonym of in-band signaling. See in-band signaling.

15 P

packet A group of bits that include data and control information. Generally refers to a network layer (OSI layer 3) protocol data unit.

Packet Discarding It refers to the function to discard the packets from unknown VLAN domain or broadcast packets. Packet Discarding is used to prevent the situation where unknown packets or broadcast packet utilize the bandwidth originally belonging to the links, improving the reliability of service transmission.

packet forwarding capability It is also called interface throughput. It refers to the capability of an interface on a device to forward packets. The unit is packet per second (pps). For low-end devices, the packet forwarding capability ranges only from one-figure number to two-figure number kpps, but the high-end devices can reach two-figure numbers or even three-figure number Mpps.

Packet Switched Network Packet Switched Network (PSN) is a data communication network that is based on the principles of packet switching. see packet switching.

packet switching A method of transmitting messages through a communication network, in which long messages are subdivided into short packets. The packets are then transmitted in the same method as in message switching.

parity bit A check bit appended to an array of binary digits to make the sum of all the binary digits, including the check bit, always odd or always even.

Passive Mode It is a working mode of EFM OAM. The interface in the passive mode cannot initiate the discovery and remote loopback.

patch A piece of executable object code used to repair a deficiency in the functionality of a program. Through patching, the software can be upgraded while the normal running of the system is not interrupted. Compared with loading the upgrade software, patching is a better way to enhance the quality of service.

PBX see **Private Branch Exchange**.

PE see **Provider Edge**.

Peak Information Rate It refers to the maximum rate of information passing through a virtual circuit. The unit is kbit/s.

Per-Hop Behavior	IETF Diff-Serv workgroup defines forwarding behaviors of network nodes as per-hop behaviors (PHB), such as, traffic scheduling and policing. A device in the network should select the proper PHB behaviors, based on the value of DSCP. At present, the IETF defines four types of PHB. They are class selector (CS), expedited forwarding (EF), assured forwarding (AF), and best-effort (BE).
Performance management	Performance management is used to measure the packet loss ratio, delay, and jitter during the transmission of packets. It also collects statistics on various types of traffic. Performance management is performed at the access point of users. By using the performance management tools, the ISP can monitor the network status and locate faults through the Network Management System (NMS). The ISP checks whether the forwarding capacity of the network complies with the Service Level Agreement (SLA) signed with users.
PGND	see **protection ground**.
phase	The relative position in time within a single period of a signal.
PHB	see **Per-Hop Behavior**.
PING	PING is short for Packet InterNet Groper. It uses the ICMP Echo message and its response to test if a network device on an IP network is reachable.
PIR	see **Peak Information Rate**.
plaintext	The input to an encryption function or the output of a decryption function.
plug-and-play	Plug and Play is s Windows technology that automatically detects and configures most of the adapters and peripherals that can be connected to a PC. For communication networks, fast discovery of network topology can help the newly attached devices communicate with the nodes on the network, without the need to configure the new devices.
Point Of Presence	It refers to the location of the device that accesses the carrier switch.
point-to-point	A configuration in which two stations share a transmission path.
POP	see **Point Of Presence**.
port	It has two meanings. One is that it refers to the specific part on the interface board of communication devices, and the other is that it refers to the application service interface in TCP and UDP protocols.
Port Isolating	Multiple user services can be mapped to an MP2MP service instance. An MP2MP service instance also corresponds to multiple physical interfaces. The port isolating can prevent the traffic of multiple interfaces from communication with each other.
port isolation	The port isolation isolates the unidirectional or bidirectional Layer 2 communication between interfaces.
power module	Module that provides power supply to operate other boards or modules.
prefix	A method of summarizing a large number of addresses in a compact manner. The prefix, which would be at most the length of an address, specifies all addresses that start with the specific prefix.
Priority Queue	The Priority Queuing (PQ) is a queue scheduling algorithm based on the absolute priority. According to the PQ algorithm, services of higher priorities are ensured with greater bandwidth, lower latency, and less jitter. Packets of lower priorities must wait to be sent till all packets of higher priorities are sent. In this manner, services of higher priorities are handled earlier than others.

Private Branch Exchange	A telephone exchange on the user's premises. Provides a switching facility for telephones on extension lines within the building as well as access to the public telephone network.
protection ground	A grounding point on the metal surface of the cabinet and the devices in the cabinet. It ensures sound lightning proof, electricity shockproof, and disturbance proof capabilities of the equipment.
protection switchover	Protection Switchover is a transmission entity that enables data on a failed facility to be moved to an alternate facility. This feature may be either revertive or nonrevertive.
protocol	A set of rules that govern the operation of functional units for communication. Protocols can describe low-level details of machine-to-machine interfaces, or high-level exchanges between application programs. Most protocols include both intuitive descriptions of the expected interactions as well as more formal specifications using finite state machine models.
Protocol Data Unit	A set of data specified in a protocol of a given layer and consisting of protocol control information of that layer, and possibly the user data of that layer.
Protocol Independent Multicast	Protocol Independent Multicast (PIM) is widely used on a network as a multicast routing solution.
Protocol Independent Multicast Dense Mode	One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces till pruning and truncation occurs. In the dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and probably use the datagrams that are forwarded to them. The cost of using the dense mode is its default flooding behavior.
Protocol Independent Multicast Sparse Mode	PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In the sparse mode, receivers are widely distributed, and the assumption is that downstream networks do not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
protocol type	A multiplexing field that defines the type of packet in which only a single field appears in the packet. In contrast, a SAP type of multiplexing field has a source SAP and a destination SAP. The two SAP values are numberically unrelated.
Provider Edge	A Provider Edge (PE) device is located at the edge of the backbone MPLS VPN network. PE is responsible for VPN user management, establishment of LSPs between the PE devices and exchanges of routing information between sites of the same VPN. PE performs the mapping and forwarding of the packets from the private network to the public-network tunnels and that are in the reverse order. Based on the location, PE can be further divided into UPE, PE-AGG, and NPE.
Pseudo Wire Emulation Edge-to-Edge	Pseudo-Wire Emulation Edge to Edge (PWE3) is a type of end-to-end Layer 2 transmitting technology. It emulates the essential attributes of a telecommunication service such as ATM, FR or Ethernet in a Packet Switched Network (PSN). PWE3 also emulates the essential attributes of low speed Time Division Multiplexed (TDM) circuit and SONET/SDH. The simulation approximates to the real situation.
PSN	see **Packet Switched Network**.
PSTN	see **Publich Switched Telephony Network**.

Publich Switched Telephony Network	The public network cable/private network cable is the core of the world's public circuit-switched telephone networks, in much the same way that the Internet is the core of the world's public IP-based packet-switched networks.
PWE3	see **Pseudo Wire Emulation Edge-to-Edge**.

16 Q

QinQ

QinQ protocol is a layer 2 tunnel protocol based on IEEE 802.1Q technology. The frames transferred in the public network have two layer 802.1Q tags (a public network tag and a private one), that is, 802.1Q-in-802.1Q. This protocol is called QinQ protocol in short.The main idea of this protocol is to encapsulate the userí»s private network VLAN tags in the public network VLAN tags. The packets pass through the backbone network of the internet service provider (ISP) with double tags. In this way, the protocol provides the users with relatively simple layer 2 VPN tunnel.

QoS

see **Quality of Service**.

Quality of Service

A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

17 R

RADIUS see **Remote Authentication Dial in User Service**.

Random Early Detection Random Early Detection (RED) algorithm can be used to prevent the global TCP synchronization by employing the random packet dropping policy. When the packets of a TCP connection are dropped and sent at a low rate, other TCP connections are still being sent at a relatively higher rate. The packets of certain TCP connections are sent at a relatively higher rate. This improves the utilization of network bandwidth.

Rapid Spanning Tree Protocol Rapid Spanning-Tree Protocol (RSTP) is described in detail in IEEE 802.1w. RSTP is based on and supplements STP. Currently, RSTP is applied in the network as a substitute for STP.

re-mark To change the Differentiated Services Code Point (DSCP) of a packet, usually performed by a marker in accordance with a traffic conditioning agreement.

reassembly The process of collecting all the fragments of an IP packet and using them to setup a copy of the original packet. The ultimate destination performs reassembly.

RED see **Random Early Detection**.

redundancy It refers to the scheme to add more than one channels, elements or parts that have the same functions with the counterparts in the system or device at a critical place. When a fault occurs, the system or device can work well, and the reliability is then improved.

redundancy backup see **redundancy**.

Regional Root The region root includes CIST region root and MSTI region root. The CIST region root is the root of IST, and the MSTI region root is the root of every MSTI.

Relative Humidity Relative humidity may be defined as the ratio of the water vapor density (mass per unit volume) to the saturation water vapor density, usually expressed in percent.

reliability It refers to the capability of a product to complete the specific functions in given time under the stipulated conditions. The probability measurement is called reliability.

reliability Reliability provides a measure of the number of times the positioning requests that satisfy QoS requirements are successful.

Remote Authentication Dial in User Service	RADIUS was originally used to manage the scattered users who use the serial interface and modem, and it has been widely used in NAS. NAS delivers the information of users on authentication, authorization and accounting to the RADIUS server. RADIUS stipulates how the user and accounting information is transferred between NAS and RADIUS. The RADIUS server is responsible for receiving the connection request from users to complete authentication, and returning the configurations of the users to NAS.
Remote Loopback	When the local interface sends non-OAMPDUs to the peer, instead of forwarding non-OAMPDUs based on their destination MAC addresses, the peer loops back non-OAMPDUs to the local interface. This is called remote loopback. Remote loopback can be used to locate faults and test link performance.
Remote MONitor	Remote MONitor is abbreviated to RMON. It is a widely used network management standard defined by the IETF, and it enhances the MIB II standard greatly. It mainly functions to monitor the data traffic over a network segment or the entire network. RMON is completely based on the SNMP architecture, including the NMS and the Agent running on each network device.
Remote Neighbor	If two adjacent devices are not directly connected but through immediate devices, they are called remote neighbors.
Remote Procedure Call	A technique in which a program invokes services across a network by making modified procedures calls.
Replication of Multicast VLAN	After the replication of multicast VLAN is configured, you can configure different VLANs to be a user VLAN of a multicast VLAN on Layer 2 devices, when multicast on demand is performed for hosts that are connected to Layer 2 devices and that belong to different VLANs. You only need to enable Layer 2 multicast function in the multicast VLAN.By using the replication of multicast VLAN, you can send multicast packets in different VLANs. This makes it easy to manage and control the multicast source and the multicast group members, and reduces the wastage of bandwidth.
reverse path forwarding	A technique for reducing the overhead of flooding, in which a router accepts a packet with source address S only from link L, if L is the link which the router would use for forwarding S.
RFC	Request For Comments: The name of series of notes that contain surveys, measurement, ideas, techniques, and observations, as well as proposed and accepted TCP/IP protocol standards.
RH	see **Relative Humidity**.
ring topology	A local network topology in which stations are attached to a closed loop. Data are transmitted in one direction or both directions around the ring, and can be read by all attached stations. The typical ring network is a Fiber Distribution Data Interface (FDDI) and token ring.
RIP	Routing Information Protocol: A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth.
RMEP	For the other devices in the same MA, their MEPs are called the Remote Maintenance association End Points (RMEPs).
RMON	see **Remote MONitor**.
Root Interface	On each non-root switch, the interface that is the nearest to the root switch is called its root interface. The root switch has no root interface.

route	A route is the path that network traffic takes from its source to its destination. In a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.
router	A special device that is attached to two or more networks and forwards packets from one to the other. In particular, an IP router forwards IP packets among the networks to which it connects. A router uses the destination address on a packet to choose a next-hop to which it forwards the packet.
routing	The determination of a path that a data unit (frame, packet, message) traverses from source to destination.
routing table	A table that stores and updates the locations (addresses) of network devices. Routers regularly share routing table information to be up to date. A router relies on the destination address and on the information in the table that gives the possible routes--in hops or in number of jumps--between itself, intervening routers, and the destination. Routing tables are updated frequently as new information is available.
RPC	see **Remote Procedure Call**.
RPF	see **reverse path forwarding**.
RS232	A standard by EIA that specifies the electrical characteristics of slow speed interconnections between terminals and computers or between two computers.

18 S

safety authentication An act conducted to ensure safety of the equipment and safety of the operators, generally compliant with applicable standards such as EN60950.

SAP see **Service Access Point**.

scalability Capability of a software system when it runs on the hardware platforms of different sizes and grades.

scanning and snooping attack Scanning and snooping attack is used to point out a potential target by identifying an existing system in the network by means of ping scanning (including ICMP and TCP). Through TCP and UDP port scanning, the attacker can detect the running system and the monitoring service, and then get a general idea of the service type and the potential security defect of the system to prepare for further intrusion.

SDH see **Synchronous Digital Hierarchy**.

security Protection of a computer system and its data from harm or loss. A major focus of computer security, especially on systems accessed by many people or through communication lines, is preventing system access by unauthorized individuals.

segment The unit of transfer sent from TCP on one device to TCP on another device. Each segment contains a part of a stream of bytes being sent between the machines as well as additional fields that identify the current position in the stream and a checksum to ensure validity of the received data.

selective QinQ The selective QinQ function expands the QinQ function. It enables the interfaces to add an outer tag with different public VLAN ID to the frames flexibly according to the private network VLAN ID of the frames.

self-healing The ability to recover from anomalies.

server On a local area network, a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client.

Service Access Point A term that can be employed for the address of a user of a service. The destination address plus the destination SAP (DSAP) define the recipient of a packet. The SAP differs from a protocol type in the aspect that the assumption is that the source SAP (SSAP) and DSAP are numerically unrelated.

service interface card	It is also called interface unit or service processing board. It provides external physical interfaces for service transmission, completing the task of packet receiving and transmitting. For a distributed system, it partially has the functions of protocol process and switching or routing.
Service Level Agreements	A service contract between a customer and a service provider that specifies the forwarding service a customer should receive. A customer may be a user organization (source domain) or another differentiated services domain (upstream domain). A SLA may include traffic conditioning rules which constitute a traffic conditioning agreement as a whole or partially.
session	Session is the term that strictly applies to a logical connection between two nodes on a network for the exchange of data, though generally, it can apply to any alternatively, any link between any two data devices. A session is also used simply to describe the connection time.
shaping	The process of delaying packets within a traffic stream to cause it to conform to certain defined traffic profile.
Shielded Twisted Pair	Shielded Twisted Pair (STP) is a special type of copper telephone wiring used in certain business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground.
Shortest Path First	The term often used for the Dijkstra algorithm, in which paths to all destinations are computed and provide complete information in the graphical form.
Simple Network Management Protocol	Simple Network Management Protocol is abbreviated to SNMP. It is a protocol that stipulates how to manage the nodes on a network. SNMP uses an agent to monitor the transmission of network information and maintain the management information base (MIB). However, its safety performance is limited. SNMP model includes four components: management node, management station, management information, and management protocol.
Simple Traffic Classification	Simple traffic classification (STC) organizes data packets into multiple priorities or multiple service classes. A network administrator can set STC policies. An STC policy can include the IP precedence or the DSCP value of an IP packet, the EXP value of an MPLS packet, or the 802.1p value of a VLAN packet.
simplex	Refers to a one-way electronic communication that takes place unidirectionally always.
single pass	Single pass refers to a communication failure. In the traditional telephony communication, single pass means that one party cannot hear the other party in the communication. In data communication, single pass means that the packets are received and sent normally in one direction, and abnormally on the other direction. As a result, the communication on both ends fails.
single point failure	As a failure type, it is also called single-site failure. It stops data transmission over network and cannot recover automatically if it occurs. The site can refer to an interface, a board, a device or link.
SLA	see **Service Level Agreements**.
sliding window	Characteristics of protocols that allow a sender to transmit more than one packet of data before receiving an acknowledgement. After receiving an acknowledgement for the first packet sent, the sender "slides" the packet window and sends another. The number of outstanding packets or bytes is known as the window size. Increasing the window size can improve throughput.

slow-start	A congestion avoidance scheme in TCP in which TCP increases its window size as ACKs arrive. Slow-start can achieve high throughput by using exponential increases.
SNMP	see **Simple Network Management Protocol**.
Source Address	Source Address
source route	A route that is determined by the source. A source route in IP consists of a list of routers a packet should visit. The route is specified as an IP option. Source routing is most often used for debugging.
spanning tree	A subset of a network in which exactly one path exists between any pair of nodes.
Spanning Tree Protocol	Spanning-Tree Protocol (STP) is a protocol used in the local area network (LAN) to eliminate loops.
SPF	see **Shortest Path First**.
spoofing attack	see **IP spoofing attack**.
star topology	A topology in which all stations are connected to a central switch. Two stations communicate through circuit switching.
static LACP mode	The static LACP mode refers to a link aggregation method of selecting active and inactive interfaces by negotiating aggregation parameters through LACPDUs. In the static LACP mode, LACP determines active and inactive links of the link aggregation group. It is also called the M:N mode, that is, M active links and N backup links. The M:N mode provides higher reliability and load balancing can be implemented among M links.
STP	see **Shielded Twisted Pair**.
subnet addressing	An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks. Outside the site using subnet addressing, routing continues as usual by dividing the destination address into a network portion and host portion. Using subnet addressing, devices inside a site interpret the host portion of the address by dividing it into a physical network portion and host portion.
subnetwork	A collection of equipment and physical transmission media that forms an autonomous whole and can be used to interconnect systems for communication purposes.
Subscriber Queue	A subscriber queue (SQ) is a virtual queue.Each SQ maps eight types of FQ priority and can be configured with one to eight FQs. Idle queues cannot be used by other SQs, that is, one to eight FQs share the total SQ bandwidth.
switch	The process of interconnecting functional units, transmission channels or telecommunication circuits for the required duration, to convey signals. Any process through which, data is moved from one location to another.
switch	A switch is a device with multiple ports, which accepts packets from one port, examines the destination address, and then transmits the packets to the intended port having a host with the same destination address.
switch unit	As a critical component of the main control unit, the switch unit is also called the switch module (or switch network), with the functions of switching, allocation, scheduling, and control for packets between interface boards. Generally, the switch unit uses ASIC chips of high performance to provide line rate forwarding for packets.

switching capacity	It is also called backplane bandwidth or switching bandwidth. The switching capacity is the maximum data that can be processed by the interface processor of a switch and the data bus. The backplane bandwidth indicates the overall data switching capability of a switch, in Gbit/s. The higher the switching capacity of a switch is, the more powerful it is in processing data. But the design is costly. The result of twice the output by multiplying the interface capacity by the interface number should be less than the switching capacity, realizing full duplex switching without congestions.
Synchronous Digital Hierarchy	SDH is a transmission scheme that follows ITU-T G.707, G.708, and G.709. It defines the transmission features of digital signals such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN. It interleaves the bytes of low-speed signals to multiplex the signals to high-speed counterparts, and the line coding of scrambling is only used only for signals. SDH is suitable for the fiber communication system with high speed and a large capacity since it uses synchronous multiplexing and flexible mapping structure.

19 T

tangent rings It is a concept in geometry. There is a public node between two ring networks. The public node often brings in single-point failure.

TCP see **Transmission Control Protocol**.

TDM see **Time Division Multiplexing**.

TE see **Traffic engineering**.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC854.

terminal It refers to a device that only has the keyboard, monitor and disk drive, but can connect to other devices through serial interfaces.

TFTP see **Trivial File Transfer Protocol**.

throughput see **packet forwarding capability**.

Time Division Multiplexing It is a multiplexing technology. TDM divides the sampling cycle of a channel into time slots (TSn, n=0, 1, 2, 3¡), and the sampling value codes of multiple signals engross time slots in a certain order, forming multiple multiplexing digital signals to be transmitted over one channel.

Time To Live A technique used in best-effort delivery systems to prevent packets that loop endlessly. The TTL is set by the sender to the maximum time the packet is allowed to be in the network. Each router in the network decrements the TTL field when the packet arrives, and discards any packet if the TTL counter reaches zero.

timeout It refers to that an event is expected in a certain time. An event that indicates that a predetermined amount of time has elapsed without some other expected event taking place.

token Something that is passed between users. In token-oriented LANs, possession of the token gives the possessor permission to transmit packets.

Token Bucket To control traffic, there must be a mechanism that can measure the traffic that flows through a device. This method is called granular control. The token bucket (TB, or bucket for short) is a popular method to measure traffic. It is used in the CAR and traffic shaping technologies to control the traffic rate.

token bucket algorithm The token bucket is a container for tokens. The capacity of a token bucket is limited, and the number of tokens determines the traffic rate of permitted packets. The token bucket polices the traffic. Users place the tokens into the bucket regularly according to the preset rate. If the tokens in the bucket exceed the capacity, no tokens can be put in. Packets can be forwarded when the bucket has tokens, otherwise they cannot be transferred till there are new tokens in the bucket. This scheme adjusts the rate of packet input.

topology The structure, consisting of paths and devices that provide the communication interconnection among nodes of a network. The topology structure of a network describes the way in which devices are connected together.

topology discovery Techniques to accurately determine the exact layout of a network using a few assumptions about the network architecture and simple tools.

TOS see **Type of Service**.

traceroute A program that prints the path to a destination. Traceroute sends a sequence of datagrams with the time-to-live (TTL) set to 1,2, etc., and uses ICMP time exceeded messages that return to determine routers along the path.

Traffic classification It identifies the expected packets according to specific rules, paving the way for differentiated services.

Traffic Engineering Traffic Engineering (TE) encompasses traffic management, capacity management, traffic measurement and modelling, network modelling, and performance analysis.

Traffic mirroring A switching feature that allows the packet to be replicated to the monitor port for network detection and fault removal

Traffic policy It is a scheme that supervises the specific traffic entering the communication devices. By policing the speed of traffic that enters the network, it "punishes" the traffic out of the threshold, so the traffic going into network is limited to a reasonable range, protecting the network resources and the interests of the carriers.

Traffic shaping It is a way of controlling the network traffic from a computer to optimize or guarantee the performance and minimize the delay. It actively adjusts the output speed of traffic in the scenario that the traffic matches network resources provided by the lower layer devices, avoiding packet loss and congestion.

Transmission Control Protocol The TCP/IP standard transport level protocol that provides the reliable, full duplex, flow service on which many application protocols depend. TCP allows a process on one device to send a data flow to a process on another. TCP is connection-oriented in the sense that before transmitting data, participants must establish a connection. TCP segments are divided and encapsulated into many IP packets and travel across the Internet using IP packets.

Tree topology A local network topology in which stations are attached to a shared transmission medium. The transmission medium is a branching cable emanating from a headend, with no closed circuits. Transmissions propagate throughout all branches of the tree, and are received by all stations.

Trivial File Transfer Protocol A small and simple alternative to FTP for transferring files. TFTP is intended for applications that do not need complex interactions between the client and server. TFTP restricts operations to simple file transfers and does not provide authentication. TFTP is small enough to be contained in ROM to be used for bootstrapping diskless machines.

TTL see **Time To Live**.

Tunneling A technique in which a packet is encapsulated in a high-level protocol and passed across a public network. The tunneling technique can be used to implement VPN solution.

twisted pair	It is a four-pair wire medium-composed of pairs of wires - used in a variety of networks.
Type of Service	The header of each IP packet includes a field that allows the sender to specify the type of service desired. The Type of Service (TOS) is used for internet service quality selection. The type of service is specified along the abstract parameters precedence, delay, throughput, and reliability. These abstract parameters are to be mapped into the actual service parameters of the particular networks the datagram traverses.
Type-Length-Value	TLVs constitute an LLDPDU. TLV specifies the type, length, and value fields of an information element.

20 U

UDP	see **User Datagram Protocol**.
UL	see **Underwriters Laboratories**.
Underwriters Laboratories	The most authoritative institute of authentication and safety test in USA.
unicast	The data is delivered to an exclusive destination.
Uniform Resource Locator	A string that gives the location of a piece of information. The string begins with a protocol type followed by the identification of a specific information. For example, the domain name of a server and the path name to a file on that server.
Unshielded Twisted Pair	The standard cabling used for telephone lines as well as Ethernet, whose standard IEEE 802.3, 10BaseT, defines use of over Unshielded Twisted Pair (UTP) for rates up to 10Mbit/s. A pair of insulated wires that are not enclosed in a metal sheath, to protect against EMI.
upgrading smoothly	Process of upgrading the system files without service interruption.
URL	see **Uniform Resource Locator**.
User Datagram Protocol	The TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. User Datagram Protocol (UDP) uses IP to deliver datagrams. UDP provides application programs with the unreliable connectionless packet delivery service. Thus, UDP messages can be lost, duplicated, delayed, or delivered out of order.
UTP	see **Unshielded Twisted Pair**.

21 V

Versatile Routing Platform Versatile Routing Platform (VRP) is a network Operating System (OS) used by data communication products of Huawei. As the core engine of the software for Huawei products such as all series of routers, Ethernet switch, and service gateway, VRP provides a uniform user interface and management interface, including the real-time OS core, IP soft-forwarding engine, route processing and configuration management planes. It provides the function of control plane, and specifies the standard for forwarding plane interface, implementing the interaction between the forwarding plane of products and the control plane of VRP. At the same time, VRP provides network layer interface to interconnect the link layer to the network layer.

Virtual Leased Line Virtual Leased Line (VLL) is the emulation of the traditional leased line service. It uses the IP network to emulate the leased line to provide unsymmetrical and cost-effective DDN services. From the viewpoint of users on both sides of VLL, VLL is similar to the traditional leased line.

Virtual Local Area Network VLAN refers to the end-to-end logical network that is built through a network management software on the basis of a switching LAN. It can traverse different network segments and networks. In fact, a VLAN is a logical subnet, namely, a logical broadcast domain. It can cover many network devices.

Virtual Port Virtual Port belongs to a logic terminal used to access communication devices through Telnet.

Virtual Private Network A network that is constructed using public wires to connect nodes, set up solely for the users of a single company. These Virtual Private Networks (VPNs) use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

Virtual Terminal In open systems, a virtual terminal (VT) is an application service that: 1. Allows host terminals on a multi-user network to interact with other hosts regardless of terminal type and characteristics. 2. Allows remote log-on by local area network managers for the management purposes. 3. Allows users to access information from another host processor for transaction processing. 4. Serves as a backup facility.

VLAN see **Virtual Local Area Network**.

VLAN Mapping	VLAN mapping is used to implement VLAN convergence by mapping one or more downstream VLANs to an upstream VLAN. The downstream VLAN is the VLAN that the interface at the user side belongs to and is used to identify a user or a class of users. The downstream VLAN is also called the Customer-VLAN (C-VLAN). The upstream VLAN is specified by the Internet Service Provider (ISP) at the network side and is used to identify a type of service. The upstream VLAN is also called the Service-VLAN (S-VLAN).
VLAN Mapping Table	An attribute of the MST region, is used for describing the mapping relationship between VLAN and MSTI.
VLAN Stacking	The VLAN stacking technology adds a layer of VLAN tag to the incoming packet. The VLAN stacking technology implements transparent transmission of C-VLANs in the ISP network to realize the application of Layer 2 Virtual Private Network (VPN).
VLAN Switch	The VLAN switch technology sets up the switching table based on the interface and VLAN. Based on the switching table, the device replaces the incoming VLAN tag of a received packet with the outgoing VLAN tag to implement the point-to-point transmission for Ethernet services.
VLL	see **Virtual Leased Line**.
VoIP	VoIP (voice over IP) is an IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in a digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network (PSTN).
VPN	see **Virtual Private Network**.
VRP	see **Versatile Routing Platform**.
VT100	See **Virtual Terminal**. VT100 is a type of virtual terminals, and the other includes ANSI, VT52, and VTNT.

22 W

WAN see **Wide Area Network**.

Weighted Fair Queuing Weighted Fair Queuing (WFQ) is a fair queue scheduling algorithm based on bandwidth allocation weights. This scheduling algorithm allocates the total bandwidth of an interface to queues, according to their weights and schedules the queues cyclically. In this manner, packets of all priority queues can be scheduled.

Weighted Random Early Detection Based on the RED technique, WRED sets the low threshold and drop probability for normal packets and packets with a high drop probability in each queue.

well-known port Any of a set of protocol port numbers preassigned to specific uses by transport level protocols such as TCP and UDP. Each server listens at a well-known port, and the clients can locate it.

Wide Area Network Any physical network technique that spans large geographic distances. WANs use communication circuits to connect intermediate nodes. A major factor affecting WAN design and performance is a requirement that they lease communication circuits from telephone companies or other communication carriers.

wire speed Wire speed refers to the maximum packet forwarding capacity on a cable. The value of wire speed equals the maximum transmission rate capable on a given type of media.

working mode of EFM OAM The working mode of EFM OAM is an attribute of the interface enabled with EFM OAM. EFM OAM has two working modes: active mode and passive mode.

World Wide Web The large-scale information service that allows a user to browse information. World Wide Web (WWW) offers a hypermedia system that can store information as text, graphics, audio, etc.

WTR time If the protection group is in revertive mode, services are not immediately switched back when the working tunnel recovers. Services are switched back from the protection tunnel to the working tunnel after a period of time which is called WTR time.

WWW see **World Wide Web**.

23 X

XModem An error-correcting protocol for modem that was created in 1978 by Ward Christensen and became a de facto standard. Modems that agree on using the Xmodem protocol send data in 128-byte blocks. If a block is received successfully, a positive (ACK) acknowledgement is returned. If an error is detected, a negative (NAK) acknowledgement is returned and the block is resent. Xmodem uses the checksum method of error checking.