Lucent Technologies
Bell Labs Innovations

TAOS

Glossary

Part Number: 7820-0648-005
For software version 9.0
January 2001

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change.

Safety, Compliance, and Warranty Information

Before handling any Lucent Access Networks hardware product, read the *Edge Access Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security Statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

Copyrights for Third-Party Software Included in Lucent Access Networks Software Products

Ordering Information

You can order the most up-to-date product information and computer-based training online at http://www.lucent.com/ins/bookstore.

Feedback

Lucent Technologies appreciates your comments, either positive or negative, about this manual. Please send them to techpubs@ascend.com.

Lucent Technologies

Customer Service

To obtain product and service information, software upgrades, and technical assistance, visit the eSight™ Service Center at `http://www.esight.com`. The center is open 24 hours a day, seven days a week.

Finding information and software

The eSight Service Center at `http://www.esight.com` provides technical information, product information, and descriptions of available services. Log in and select a service. The eSight Service Center also provides software upgrades, release notes, and addenda. Or you can visit the FTP site at `ftp://ftp.ascend.com` for this information.

Obtaining technical assistance

The eSight™ Service Center at `http://www.esight.com` provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone.

If you need to contact Lucent Technologies for assistance, make sure that you have the following information available:

- Active contract number, product name, model, and serial number
- Software version
- Software and hardware options
- If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or eSight Live chat. Select one of these sites when you log in to `http://www.esight.com`.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information on eSight or if you have a very urgent need, contact TAC. Access the eSight Service Center at `http://www.esight.com` and click `Contact Us` below the Lucent Technologies logo for a list of telephone numbers inside and outside the United States.

You can alternatively call (800) 272-3634 for a menu of Lucent services, or call (510) 769-6001 for an operator. If you do not have an active services agreement or contract, you will be charged for time and materials.

About This Guide

How to use this guide

This guide contains definitions of technical terms and acronyms commonly found in True Access™ Operating System (TAOS) documentation. Use this guide as a reference when installing, configuring, or maintaining your system.

Warning: Before installing your TAOS unit, be sure to read the safety instructions in the *Access Networks Safety and Compliance Guide*. For information specific to your unit, see the "Safety-Related Electrical, Physical, and Environmental Information" appendix in your unit's hardware installation guide.

Documentation conventions

Following are all the special characters and typographical conventions used in this manual:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)

Convention	Meaning
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.
 **Warning:**	Warns of danger of electric shock.

Alphabetic list of terms

Numeric

2DS—A variant of the standard G.703 framing required by most E1 DPNSS providers in the U.K. See also *G.703*.

2-wire continuity test—In a Signaling System 7 (SS7) network, a test in which a TAOS unit sends a 2010Hz tone (for a T1 line) or a 2000Hz tone (for an E1 line) and expects to receive a 1780Hz tone in order to verify that the physical link between the Central Office (CO) switch and the unit is available. The TAOS unit supports both incoming and outgoing 2-wire continuity checks for T1 and E1 lines. You can select the type of check to perform on a per-line basis. Both the native 2-wire continuity check (GR-246-CORE Section B.2) and 4-wire-to-2-wire emulation (GR-246-CORE Section B.3) are supported. Compare with *4-wire continuity test*. See also *4-wire-to-2-wire continuity test, continuity test, SS7 network*.

3DES-CBC—Triple Data Encryption Standard-Cypher Block Chaining. 3DES-CBC is a variant of DES-CBC. 3DES-CBC encrypts each block of data three times, using a different key each time. See also *40DES-CBC, DES-CBC.*

3.1kHz audio-bearer service—A service that sends a data call over a voice trunk. Because echo cancellation corrupts data transmitted on voice trunks, each switch should turn off echo cancellation on the trunks handling 3.1kHz audio-bearer service. The 3.1kHz audio-bearer service is sometimes referred to as *Data Over Subscriber Bearer Service (DOSBS)*.

4-wire continuity test—In a Signaling System 7 (SS7) network, a test in which a TAOS unit verifies that the physical link between the Central Office (CO) switch and the unit is available. For a T1 line, the TAOS unit sends a 2010Hz tone and expects to receive a 2010Hz tone in return. For an E1 line, the TAOS unit sends a 2000Hz tone and expects to receive a 2000Hz tone in return.

The 4-wire continuity test requires one end of a line to place a channel into loopback state while the other end sends the tone. The check concludes successfully if the tone sent on the outgoing path is received on the return path within acceptable quality and timing limits. The 4-wire check procedure cannot detect potential inadvertent loops in the line path or in line facilities, and cannot be used when the other exchange is analog. For these reasons, the procedure known as a *2-wire continuity test* is recommended by the International Telecommunications Union Telecommunication Standardization Sector (ITU-T).

Compare with *2-wire continuity test, 4-wire-to-2-wire continuity test.* See also *continuity test, SS7 network*.

4-wire-to-2-wire continuity test—In a Signaling System 7 (SS7) network, a test in which a TAOS unit sends a 1780Hz tone and expects to receive a 2010Hz tone (for a T1 line) or a 2000Hz tone (for an E1 line) in order to verify that the physical link between the Central Office (CO) switch and the unit is available. Compare with *4-wire continuity test*. See also *2-wire continuity test, continuity test, SS7 network*.

7-bit mode—See *ASCII mode*.

10Base2—A 50-ohm coaxial RG-58u cable with a data rate of 10Mbps and a maximum length of 180 meters. 10Base2 does not include a built-in transceiver. It is also known as *thin Ethernet* or *thinnet*.

10Base5——A 50-ohm coaxial RG-6 cable with a data rate of 10Mbps and a maximum length of 500 meters. It is also known as *thick Ethernet* or *thicknet*.

10BaseT—The 802.3 IEEE standard for operating a 10Mbps Ethernet network with twisted-pair cabling and a wiring hub. 10BaseT is also known as *UTP Ethernet* and *twisted-pair Ethernet*. See also *10BaseT hub*.

10BaseT hub—A hub providing a common termination point for hosts connected to 10BaseT wiring. See also *10BaseT*.

40DES-CBC—40-bit Data Encryption Standard-Cypher Block Chaining. 40DES-CBC is the same algorithm as DES-CBC, but it uses a 40-bit key. See also *3DES-CBC, DES-CBC*.

40-bit Data Encryption Standard-Cypher Block Chaining—See *40DES-CBC*.

100BaseFX—A dual-fiber cable standard designed for 100Mbps Fiber Distributed Data Interface (FDDI). Compare with *100BaseT*, *100BaseT4*, *100BaseTX*.

100BaseT—The 802.3 IEEE standard for operating a 100Mbps Ethernet network. 100BaseT differs from the 10BaseT standard by requiring higher-grade cable or more wiring pairs, with cable lengths that are only a tenth as long as 10BaseT cable lengths. Compare with *100BaseFX*, *100BaseT4*, *100BaseTX*. See also *10BaseT*.

100BaseT4—A 4-pair, category-3, half-duplex cable with a data rate of 33.3Mbps per pair, and a maximum length of 100 meters. Compare with *100BaseFX*, *100BaseT*, *100BaseTX*.

100BaseTX—A 2-pair, category-5, half-duplex cable with a data rate of 33.3Mbps per pair, and a maximum length of 100 meters. The 100BaseTX standard was designed for 100Mbps Fiber Distributed Data Interface (FDDI) and Copper Distributed Data Interface (CDDI). Compare with *100BaseFX*, *100BaseT*, *100BaseT4*. See also *CDDI*, *FDDI*.

802.2—An IEEE protocol specification for the Media Access Control (MAC) header of an IPX frame in NetWare 3.12 or later. An 802.2 frame contains the Logical Link Control (LLC) header in addition to the MAC header. Compare with *802.3*, *Ethernet II*, *SNAP*. See also *IPX frame, LLC, MAC*.

802.3—An IEEE protocol specification for the Media Access Control (MAC) header of an IPX frame in NetWare 3.11 or earlier. An 802.3 frame does not contain the Logical Link Control (LLC) header in addition to the MAC header. The 802.3 frame is also called *Raw 802.3*. Compare with *802.2*, *Ethernet II*, *SNAP*. See also *IPX frame, LLC, MAC*.

802.5—An IEEE protocol specification for the physical layer and Media Access Control (MAC) sublayer of a token-ring topology. 802.5 implements token passing over Shielded Twisted Pair (STP) cabling and offers data rates of 4 or 16Mbps. See also *STP cable*.

802.6—An IEEE Media Access Control (MAC) standard used on Local Area Networks (LANs). 802.6 is also known as *Distributed Queue Dual Bus (DQDB)*.

A

AAL—ATM Adaptation Layer. The AAL is a protocol that translates higher-layer data from its native size and format to the size and format of an Asynchronous Transfer Mode (ATM) cell, enabling engineers to adapt the ATM layer to particular services. The AAL consists of two sublayers: the Convergence Sublayer (CS) and the Segmentation And Reassembly (SAR) sublayer. See also *ATM*, *ATM layer*, *CS*, *SAR*.

ABR—(1) Area Border Router. An ABR is an Open Shortest Path First (OSPF) router that belongs to both a regular area and the backbone area. See also *area*, *backbone area*, *OSPF*.

(2) Available Bit Rate. ABR is an Asynchronous Transfer Mode (ATM) service class that handles bursty LAN traffic and data that is tolerant of delays and cell loss. ABR is a best-effort, managed service. Compare with *CBR*, *UBR*, *VBR-NRT*, *VBR-RT*. See also *ATM*.

absolute congestion—In a Frame Relay network, a congested condition that occurs when the queue length reaches the threshold of 64 buffers, and no room remains in the queue. When the Average Queue Length (AQL) exceeds the threshold for absolute congestion, all incoming frames are discarded, and the Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) bits are set. Compare with *mild congestion*, *severe congestion*. See also *BECN*, *congestion*, *FECN*.

Accept Packet Pass-Through Call message—See *ACCP message*.

Access-Accept packet—A packet sent by the RADIUS server to inform the TAOS unit that a client's request for access has been granted. See also *RADIUS server*.

Access-Challenge packet—A request for the user to enter a password in a hand-held token card. The token-card server sends the Access-Challenge packet through the RADIUS server and the TAOS unit to the user. See also *RADIUS server*, *token card*, *token-card server*.

access concentrator—A device that efficiently forwards data, handling incoming calls for a network Point Of Presence (POP). In general, an access concentrator supports dial-in modem calls, ISDN connections, dedicated links, Frame Relay traffic, and multiprotocol routing. See also *dedicated circuit*, *dial-in modem access*, *Frame Relay concentrator*, *ISDN*, *POP*.

access link—See *A-link*.

Access-Password-Ack packet—A response from the RADIUS server, informing the TAOS unit that it has accepted a new password. See also *RADIUS server*.

Access-Password-Reject packet—A response from the RADIUS server, informing the TAOS unit that it has rejected a new password. See also *RADIUS server*.

Access-Password-Request packet—A password-change request that a TAOS unit sends to the RADIUS server. See also *RADIUS server*.

access rate—The data rate of the user access channel.

Access-Reject packet—A packet the RADIUS server sends to inform the TAOS unit that it has not granted a client's request for access. The RADIUS server sends an Access-Reject packet if the user enters an unknown username, fails to enter the correct password, or enters an expired password. See also *RADIUS server*.

Access-Request packet—A packet that a TAOS unit sends to the RADIUS server on behalf of a client attempting to establish a connection. See also *RADIUS server*.

access router—A device that supports basic routing protocols and enables remote users to gain access to a corporate backbone network.

Access SS7 Gateway Control Protocol—See *ASGCP*.

Access Tandem switch—See *AT switch*.

accounting—A way to log information in RADIUS about Start session, Stop session, and Failure-to-start session events. When a TAOS unit recognizes one of these events, it sends an accounting request to RADIUS. When the accounting server receives the request, it combines the information into a record and timestamps it. Each type of accounting record contains attributes associated with an event type, and can show the number of packets the TAOS unit transmitted and received, the protocol in use, the username and IP address of the client, and other session information. See also *accounting server*, *Failure-to-start session*, *Start session*, *Stop session*.

accounting checkpoint—A RADIUS feature that provides periodic session information to enable accurate session billing even if the RADIUS accounting server does not receive a Stop packet. Typically, when RADIUS accounting is enabled and a Point-to-Point Protocol (PPP) connection terminates, the TAOS unit sends a Stop packet to the RADIUS accounting server, which stores the packets for use in billing. If the checkpoint feature is also enabled and the RADIUS accounting server fails to receive a Stop packet for any reason, it can still close off the session billing on the basis of the last Checkpoint packet it received. See also *accounting*, *Checkpoint packet*, *Checkpoint record*.

Accounting-Request—A request for accounting information. A TAOS unit sends an Accounting-Request packet to the RADIUS accounting server. See also *accounting server*, *RADIUS*.

Accounting-Response—A packet containing accounting information. A RADIUS accounting server sends an Accounting-Response packet to the TAOS unit. See also *accounting server*, *RADIUS*.

accounting server—The RADIUS daemon with accounting enabled. See also *accounting*, *RADIUS daemon*.

ACCP message—Accept Packet Pass-Through Call message. A call-confirmation message sent by a TAOS unit to a Signaling System 7 (SS7) signaling gateway. An ACCP message verifies the call-setup information that the TAOS unit used for routing the call to its destination. Compare with *RCCP message*. See also *signaling gateway*, *SS7*.

ACD—Automatic Call Distributor. An ACD is a telephone service that handles incoming calls on the basis of the number called. Many companies offering sales and service support use ACD to validate callers, make outgoing responses or calls, forward calls to the correct party, enable callers to record messages, gather usage statistics, and balance the use of telephone lines.

ACE authentication—A form of token-card authentication in which RADIUS forwards a connection request to a Security Dynamics ACE/Server. The ACE/Server sends an Access-Challenge packet back through the RADIUS server and the TAOS unit to the user dialing in. The user sees the challenge message, obtains the current token from his or her card, and enters the token.

The token travels back through the TAOS unit and the RADIUS server to the ACE/Server. The ACE/Server sends a response to the RADIUS server, specifying whether the user has entered the proper username and token. If the user enters an incorrect token, the ACE/Server returns another challenge, and the user can again attempt to enter the correct token. The server sends up to three challenges. After three incorrect tries, the TAOS unit terminates the call.

See also *ACE token*, *authentication*, *RADIUS server*, *token*, *token card*, *token-card authentication*, *token-card server*.

ACE token—A randomly generated access code that a user obtains from a SecurID token card. The code changes every 60 seconds. See also *ACE authentication*, *token card*.

ACF message—Admission Confirmation message. Upon successful call authentication, an H.323 Registration, Admission, and Status (RAS) message sent by the MultiVoice™ Access Manager (MVAM) device to a MultiVoice gateway in response to an Admission Request (ARQ) message. An ACF message contains the network routing information that an ingress MultiVoice gateway uses to connect the call. See also *H.323*, *MultiVoice™*, *MVAM*, *RAS*.

ACK—Acknowledgment. An ACK is a packet that the system uses to acknowledge a successful transmission. When a device receives a packet, it sends back either an ACK packet or a NAK packet to the sending device. If all the data arrived without corruption, the receiving device sends an ACK. If some of the data is missing or corrupted, the receiving device sends a NAK, which acts as a request that the sender retransmit the data.

Acknowledge Request Test Echo—See *ARTE*.

Acknowledge Send Tones message—See *ASTN message*.

acknowledgment—See *ACK*.

ACM—Address Complete Message. An ACM is sent from a signaling gateway to the SS7 network to acknowledge that the gateway has received the information required to route the call. See also *signaling gateway*, *SS7 network*.

ACR—Allowed Cell Rate. In an Asynchronous Transfer Mode (ATM) configuration, an Available Bit Rate (ABR) service value specifying the maximum rate (in cells per second) at which a device is allowed to send data. See also *ABR*, *ATM*.

ACR message—Release Channel Completed message. An Internet Protocol Device Control (IPDC) call-control message sent between the Remote Access Server (RAS) and the signaling gateway, reporting that the call channel is closed. At a minimum, this message reports the cause code that identifies how the call was terminated and the source port type, source module number, source line number, and source channel number assigned to that call. Compare with *RCR message*. See also *IPDC*, *RAS*, *signaling gateway*.

active hub—A multiport device that amplifies Local Area Network (LAN) transmission signals on a network, enabling them to be transmitted over a much greater distance than is possible with a passive hub. Compare with *passive hub*, *smart hub*. See also *hub*.

active open—A client-initiated operation that enables a device to establish a TCP link with a server at a fixed IP address.

A-D conversion—Analog-to-digital conversion. A-D conversion is a process in which an analog signal is modified into a digital signal. A-D conversion takes place, for example, when an analog modem call reaches a digital modem. Compare with *D-A conversion*. See also *analog signal*, *digital modem*, *digital signal*, *modem*.

add-on number—One or more numbers that a TAOS unit uses to build a multichannel MP, MP+, AIM, or BONDING call.

A multichannel call begins as a single-channel connection to one telephone number. The calling unit then requests additional numbers to connect additional channels, and stores the add-on numbers it receives from the answering unit. To add channels to the call, the calling unit integrates the add-on numbers with the telephone number it dialed initially. Typically, the numbers assigned to the channels share a group of leading digits. The add-on numbers are the rightmost digits identifying each telephone number, excluding the digit(s) that the telephone numbers have in common.

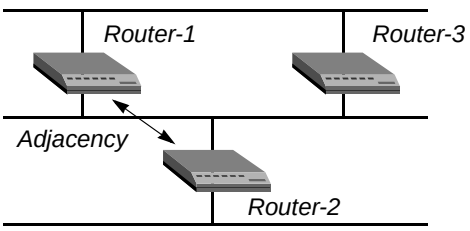
Address Complete Message—See *ACM*.

address resolution—A method of mapping a logical address (such as an IP address) to a hardware address (such as a MAC address). See also *ARP*, *hardware address*, *IP address*, *logical address*, *MAC address*.

Address Resolution Protocol—See *ARP*.

adjacency—A relationship formed between neighboring Open Shortest Path First (OSPF) routers for the purpose of exchanging routing information. An OSPF router dynamically detects its neighboring routers by sending Hello packets to the multicast address `AllSPFRouters`. It then attempts to form adjacencies (Figure 1).

Figure 1. Adjacency between neighboring routers



Neighbors exchange databases and build a consistent, synchronized database between them. When an OSPF router detects a change on one of its interfaces, it modifies its link-state database and multicasts the change to its adjacent neighbor, which in turn propagates the change to its adjacent neighbor, until all routers within an area have synchronized link-state databases. This method of updating routing information results in quick convergence among routers.

See also *area*, *convergence*, *link-state database*, *OSPF*, *router*.

Admin Cost—An Asynchronous Transfer Mode (ATM) routing metric that measures the administrative cost associated with the logical port. See also *ATM*, *CDV*, *End-to-End Delay*, *logical port*.

administrative weight—In a Private Network-to-Network Interface (PNNI) configuration, a value used to specify preferential use of a link or node for a specific service category. Administrative weight is one of the elements of topology-state information exchanged among the nodes. Other such elements include a dynamic assessment of available bandwidth, assigned metrics, and other possible attribute values. All the elements affect how the most efficient link is chosen at a given time. See also *PNNI*.

Admission Confirmation message—See *ACF message*.

Admission Reject message—See *ARJ message*.

Admission Request message—*ARQ message*.

ADSL—Asymmetric Digital Subscriber Line. ADSL is a standard that enables devices attached to twisted-pair copper wiring to transmit data at rates from 1.5Mbps to 9Mbps downstream, and 16Kbps to 640Kbps upstream. ADSL devices can transmit data at distances of up to 18,000 feet. ADSL configurations can use more bandwidth in one direction than the other. Compare with *HDSL*, *IDSL*, *RADSL*, *SDSL*, *VDSL*. See also *DSL*.

ADSL Transceiver Unit—See *ATU*.

Advanced Mobile Phone Service—See *AMPS.*

AEP—AppleTalk Echo Protocol. AEP is a Transport-layer protocol that enables the network to determine whether two nodes are connected and capable of receiving transmissions.

AESA format—ATM End System Address format. AESA format can be the format used for an ATM end-point address assigned to a TAOS unit's ATM interface. AESA addresses are required for IP over ATM.

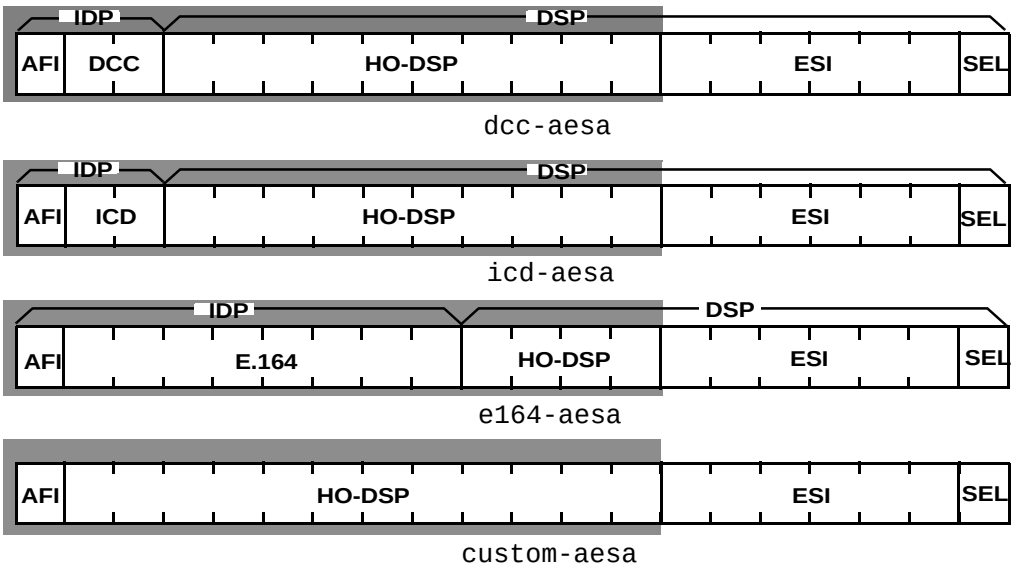
An AESA address is a 20-byte, 40-digit hexadecimal number. The first 13 bytes are the *address prefix*, or network portion of the address. The last 7 bytes are the host portion of the address. Depending on the AESA format chosen, the content of each byte of the address varies, as shown in Figure 2. All of the supported AESA formats divide the address into the Initial Domain Part (IDP) and the Domain-Specific Part (DSP).

AESA addresses use one of the following formats:

AESA format	Description
DCC AESA	Data Country Code (DCC) is specified in the address, identifying the country in which the address is registered. Country codes are standardized and defined in ISO Reference 3166.
ICD AESA	International Code Designator (ICD) is specified in the address, identifying an international organization. The British Standards Organization administers these values.
E164 AESA	E.164 address is specified using the international format.
Custom AESA	Custom authority and format identifier (AFI) and byte order.

Figure 2 shows how each format divides the 20-byte address into subfields. The shaded portion represents the address prefix, which is always the first 13 bytes.

Figure 2. Subfields in the AESA address formats



See also *ATM, Custom AESA format, DCC AESA format, E.164 AESA format, ICD AESA format*.

AFI—Authority and Format Identifier. The AFI is part of the network-level address header of an Asynchronous Transfer Mode (ATM) cell. It is a subfield of the Initial Domain Part (IDP) of an ATM End System Address (AESA). The AFI identifies the type of AESA address in use: Custom AESA, Data Country Code (DCC) AESA, E.164 AESA, or International Code Designator (ICD) AESA. Compare with *IDI*. See also *AESA format, ATM, Custom AESA format, DCC AESA format, E.164 AESA format, ICD AESA format, IDP*.

agent—A network device that provides Simple Network Management Protocol (SNMP) information to a manager application running on another computer. The agent and manager share a database of information, called the *Management Information Base (MIB)*. The manager polls the agent for information at regular intervals. When an unusual system event occurs, the agent can use a message called a *traps-PDU* to send unsolicited information to the manager. See also *manager, MIB, SNMP, traps-PDU*.

AH—Authentication Header. AH is an Internet Protocol Security (IPSec) protocol that uses a shared secret to run portions of a data packet through digest algorithms to create a digital fingerprint. The receiving system performs the same process and compares the fingerprints. Matching fingerprints verify that the packet was sent by the right source and was not altered in transit. AH works with the Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA1), Message Digest 5–Keyed-Hashing for Message Authentication (MD5-HMAC), and SHA1-HMAC authentication algorithms. Compare with *ESP*. See also *IPSec*, *MD5*, *MD5-HMAC*, *SHA1*, *SHA1-HMAC*.

AIM—Ascend Inverse Multiplexing. AIM manages the connection of two remotely located inverse multiplexers. See also *inverse multiplexer*, *inverse multiplexing*.

AIM port—A port that supports Ascend Inverse Multiplexing (AIM) and BONDING (Bandwidth ON Demand Interoperability Group) functionality. See also *AIM*, *BONDING*.

AIS—Alarm Indication Signal. An AIS is an all-ones signal that a device sends when it detects an error condition or receives an error notification.

alarm—A signal that indicates that the system has detected a security violation or error. See also *Blue Alarm signal*, *RAI*, *Red Alarm signal*.

Alarm Indication Signal—See *AIS*.

alarm relay—A mechanism whose contacts remain open on the back panel's terminal block during normal operation. If you enable them, the alarm relay contacts close during loss of power, hardware failure, or a system reset. You can also specify whether the contacts close when the bit error rate exceeds a certain value, or when all T1 PRI lines go out of service.

A-Law—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for sampling data by means of Pulse Coded Modulation (PCM). A-Law is most commonly used outside of North America and Japan. Compare with *U-Law*. See also *PCM*.

A-link—Access link. In a Signaling System 7 (SS7) configuration, an A-link is a signaling link that does not carry any data traffic. See also *SS7*.

Allowed Cell Rate—See *ACR*.

Alternate Mark Inversion—See *AMI*.

alternate path—An Open Shortest Path First (OSPF) path on which the system reroutes a Permanent Virtual Circuit (PVC) if a trunk fails.

ALU—Average Line Utilization. ALU is the average amount of bandwidth used on a line over a user-specified period of time. A TAOS unit uses ALU when determining whether to add or subtract bandwidth from a multichannel call. See also *DBA*.

Always On/Dynamic ISDN—See *AO/DI*.

amber frame—A type of packet frame that enables you to identify packets passing through the Frame Relay network. The network forwards amber frames with the Discard Eligibility (DE) bit set, enabling the network to discard the packet if it passes through a congested node. Congested nodes that must discard packets use color designations to determine which frames to discard. Red frames are discarded first, followed by amber frames, and then green frames. Compare with *green frame, red frame*. See also *congestion, DE, Frame Relay*.

AMCP message—Accept Modify Packet Pass-Through Call message. On a MultiVoice network, an AMCP message is sent by a TAOS unit to a Signaling System 7 (SS7) signaling gateway and specifies that the unit modifies one or more of the following values for a Voice over IP (VoIP) call:

- VoIP encoding type
- Packet loading rate in frames per packet
- Source port type
- Destination port type
- Listen Internet Protocol (IP) address
- Listen Real-Time Transport Protocol (RTP) port number
- Send IP address
- Send RTP port number

Compare with *RMCP message*. See also *MultiVoice™*, *SS7*.

American National Standards Institute—See *ANSI*.

AMI—Alternate Mark Inversion. Used on T1 lines, AMI is a signaling method in which the 1 bits have alternating priority. See also *T1 line*.

AMPS—Advanced Mobile Phone Service. AMPS is a standard system for analog cellular telephone service. Introduced by AT&T in 1983, AMPS is the most widely used cellular system in the United States. The service uses frequency ranges between 800MHz and 900MHz. Each provider can use half of the 824MHz to 849MHz range for receiving signals, and half the 869MHz to 894MHz range for transmission.

analog data—Data that can change continuously and have any value in a range. Examples of analog data are the time of day represented by clock hands and the temperature represented by a liquid thermometer. Compare with *digital data*. See also *analog signal*.

analog line—A line that transmits data by means of an analog signal. See also *analog signal*.

analog loopback—A test that checks whether the modem or Data Terminal Equipment (DTE) is causing errors in data transmission. During an analog loopback, the system sends data between the local modem and the local DTE. Errors in transmission indicate a problem with the modem, DTE, or the interface between them. Compare with *digital loopback*. See also *local loopback*, *loopback*, *remote loopback*.

analog signal—A type of signal that encodes data transmitted over wire or through the air, commonly represented as an oscillating wave. An analog signal can transmit analog or digital data. It takes any value in a range, and changes smoothly between values. A radio station uses analog signals to send analog music data, while a modem uses analog signals to transmit digital data. Compare with *digital signal*. See also *analog data*.

analog-to-digital conversion—See *A-D conversion*.

ANI—Automatic Number Identification. ANI is a mechanism that informs the called party of the calling party's telephone number.

Annex A—See *Frame Relay Annex A*.

Annex D—See *Frame Relay Annex D*.

ANSI—American National Standards Institute. ANSI creates standards for networking and communications. It is the U.S. representative to the International Standards Organization (ISO). See also *ISO*.

ANSI T1.617 Annex D—See *Frame Relay Annex D*.

answer number—The telephone number used for routing incoming calls. See also *call routing*.

AO/DI—Always On/Dynamic ISDN. AO/DI is a networking service that enables you to send and receive data through a dedicated X.25 connection over an ISDN D channel, ISDN B channel, or dedicated 56K line.

In a traditional ISDN environment, data moves across B channels, and signaling information moves across the D channel. Because signaling information uses a small percentage of available D-channel bandwidth, AO/DI was developed to maximize bandwidth usage while reducing the necessity that all data travel over the B channels.

A TAOS unit uses switched ISDN B channels only when required, on the basis of increased bandwidth use. Through its use of AO/DI, X.25, and Bandwidth Allocation Control Protocol (BACP), a TAOS unit avoids dial-up charges and the use of switched B channels whenever it sends or receives data over the X.25 connection. Among the functions that can use AO/DI are the following:

- Transfer of email
- Reception of news broadcasts
- Automated collection of data

For TAOS units, AO/DI enables you to use X.25 bandwidth of up to 9600bps. If a data transfer requires more bandwidth, the TAOS unit adds dial-up B channels by means of BACP. See also *BACP*, *B channel*, *D channel*, *X.25*.

APP—Ascend Password Protocol. APP is a User Datagram Protocol (UDP) that enables a user to respond to password challenges received from an external authentication server.

applet—A small software module that runs on a Java Virtual Machine (JVM) inside a Web browser. See also *JVM*.

AppleTalk—Apple's protocol suite that enables Macintosh computers to function on a network. AppleTalk works with such network operating systems as TOPS (from Sun Microsystems) and AppleShare. See also *AppleTalk router*, *AppleTalk routing*, *ARA*.

AppleTalk Control Protocol—See *ATCP*.

AppleTalk Echo Protocol—See *AEP*.

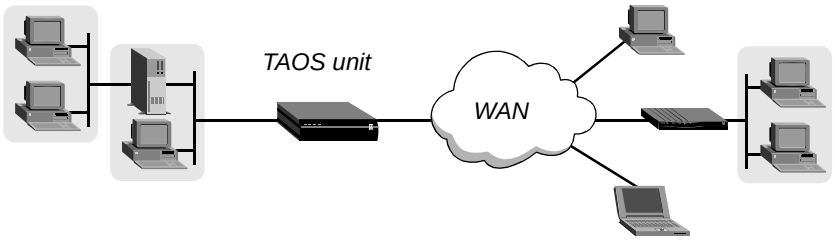
AppleTalk Remote Access—See *ARA*.

AppleTalk Remote Access Protocol—See *ARAP*.

AppleTalk router—A device that sends AppleTalk packets from a source to a destination by various paths. See also *AppleTalk*, *AppleTalk routing*, *ARA*.

AppleTalk routing—A routing configuration in which Macintosh computers can share files and services on a network. A TAOS unit configured for AppleTalk routing can receive dial-in connections from AppleTalk Remote Access (ARA) client software, Point-to-Point Protocol (PPP) dial-in software that supports AppleTalk, and AppleTalk-enabled TAOS units. Figure 3 shows a TAOS unit that routes AppleTalk between WAN interfaces and a local AppleTalk interface.

Figure 3. Routing AppleTalk between LAN and WAN interfaces



You can use AppleTalk PPP and ARA over a modem or V.120 ISDN TA connection. You can also use AppleTalk PPP over synchronous PPP when the calling unit is a TAOS router. See also *AppleTalk*, *AppleTalk router*, *ARA*, *PPP*.

Application layer—The highest layer of the OSI Reference Model. The Application layer provides applications with access to the network. File transfer, email, and network management software are examples of Application-layer programs. Protocols such as File Transfer Protocol (FTP), Rlogin, Simple Network Management Protocol (SNMP), and Telnet provide Application-layer services. See also *FTP*, *OSI Reference Model*, *Rlogin*, *SNMP*, *Telnet*.

APX 8000™—A carrier-class Remote Access Server (RAS), a unit that combines a fault-tolerant design with high port density.

AQL—Average Queue Length. AQL is a time-average algorithm that the Frame Relay switch executes each time it queues a frame for transmission. The AQL value is compared against a precalculated threshold. When the AQL is less than or equal to the threshold, maximum throughput and minimum delay occur. See also *absolute congestion*, *congestion*, *congestion management*, *mild congestion*, *severe congestion*.

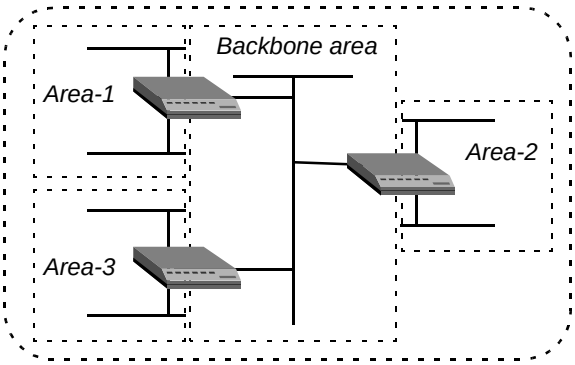
ARA—AppleTalk Remote Access. ARA enables a remote Macintosh workstation to gain access to an IP network. You can use ARA over a modem or V.120 connection. You can also use synchronous PPP when the calling unit is an AppleTalk-enabled TAOS unit. A client can dial in using ARA client software or a PPP dialer that supports AppleTalk. See also *AppleTalk*, *AppleTalk router*, *AppleTalk routing*, *modem*, *PPP*, *V.120*.

ARAP—AppleTalk Remote Access Protocol. ARAP is an AppleTalk protocol that enables a remote Macintosh computer to connect to a LAN. See also *AppleTalk*.

ARCnet—Attached Resource Computer Network. ARCnet is a baseband network architecture with a transmission rate of up to 2.5Mbps. Because it is relatively inexpensive and easy to set up, ARCnet is typically used for smaller networks.

area—A portion of an Open Shortest Path First (OSPF) Autonomous System (AS). An area acts as its own network. All area-specific routing information stays within the area, all routers within an area have a synchronized link-state database, and each database within an area is unique. On a TAOS unit, an area number uses dotted decimal notation, but it is not an IP address. To tie the areas together, some routers belong to a backbone area and one other type of area. These routers are called *Area Border Routers (ABRs)*. In Figure 4, all of the routers are ABRs.

Figure 4. Dividing an AS into areas



See also *ABR*, *AS*, *backbone area*, *link-state database*, *normal area*, *NSSA*, *OSPF*, *router*, *stub area*.

Area Border Router—See *ABR*.

area ID—See *area number*.

area number—A portion of a Switched Multimegabit Data Service (SMDS) address, or a number denoting an Open Shortest Path First (OSPF) area. In an SMDS address, the area number can be four bytes long, and is sometimes referred to as an *area ID*. An OSPF area number is expressed in dotted decimal notation, but it is not an IP address. See also *OSPF*, *SMDS*.

ARJ message—Admission Reject message. An H.323 Registration, Admission, and Status (RAS) message sent by the MultiVoice Access Manager (MVAM) device to a MultiVoice gateway in response to an Admission Request (ARQ) message if the call was not authenticated. Compare with *ACF message*, *ARQ message*. See also *H.323*, *MultiVoice™*, *MVAM*, *RAS*.

ARP—Address Resolution Protocol. ARP is a protocol in the TCP/IP protocol suite. By mapping an IP address to a physical hardware address, ARP enables a unit to identify hosts on an Ethernet LAN. See also *Ethernet*, *proxy ARP*, *TCP/IP*.

ARQ message—Admission Request message. An H.323 Registration, Admission, and Status (RAS) message sent from a MultiVoice gateway to a MultiVoice Access Manager (MVAM) device, requesting authorization for a calling end point. When the multiple logical gateway feature is enabled on a MultiVoice gateway, an incoming call request causes the gateway to send an ARQ message that includes:

- Dialed Number Information Service (DNIS), when available
- Automatic Number Identification (ANI), when available
- Trunk group and DS0 status changes

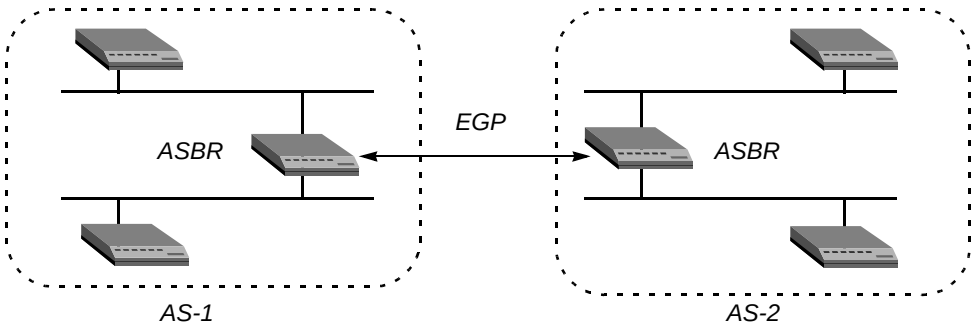
Compare with *ACF message*, *ARJ message*. See also *H.323*, *MultiVoice™*, *MVAM*, *RAS*.

ARTE—Acknowledge Request Test Echo. An Internet Protocol Device Control (IPDC) heartbeat message sent by a signaling gateway in response to a Request Test Echo (RTE) message from a TAOS unit. See also *IPDC*, *RTE*.

AS—Autonomous System. An AS is a group of Open Shortest Path First (OSPF) routers that exchange information, typically under the control of one company. An AS can include a large number of networks, all of which share the same AS number. All information exchanged within the AS is interior. See also *OSPF*, *router*.

ASBR—Autonomous System Border Router. An ASBR is an Open Shortest Path First (OSPF) router that handles communication between Autonomous Systems (ASs) by using an Exterior Gateway Protocol (EGP), as shown in Figure 5.

Figure 5. Autonomous System Border Routers (ASBRs)



ASBRs perform calculations related to external routes. A TAOS unit imports external routes by means of Routing Information Protocol (RIP) when it establishes a WAN link with a caller that does not support OSPF, and the ASBR calculations are always performed.

Compare with *ABR*. See also *AS*, *EGP*, *external route*, *OSPF*.

Ascend-Access-Event-Request packet—A packet containing either a notification that the TAOS unit has started up or a request for the RADIUS server to record the number of open sessions. See also *RADIUS server*.

Ascend-Access-Event-Response packet—A response from the RADIUS server, either reporting that the TAOS unit has started up or specifying the number of open sessions and informing the TAOS unit that the server has received and recorded the unit's ID. See also *RADIUS server*.

Ascend-Access-New-Pin packet—A response from the RADIUS server, informing the TAOS unit that it should request access again, but with the next Personal Identification Number (PIN) in the sequence. See also *RADIUS server*.

Ascend-Access-Next-Code packet—A response from the RADIUS server, informing the TAOS unit that it should request access again, but with the next password in the sequence. See also *RADIUS server*.

Ascend callback—A callback method in which a TAOS unit uses a username and password to detect callback during the authentication phase (after going off hook). The originating caller is charged for the initial call. Compare with *CBCP callback*, *CLID callback*, *DNIS callback*. See also *callback*.

Ascend Inverse Multiplexing—See *AIM*.

Ascend-Password-Expired packet—A response from RADIUS server to the TAOS unit, indicating that the password the user entered matches the one in the user profile, but has expired. (That is, the Access-Request packet sent a valid but expired password.) See also *RADIUS server*.

Ascend-Terminate-Session packet—A response from the RADIUS server, informing the TAOS unit that it should terminate the session and display the message sent in the packet. See also *RADIUS server*.

Ascend Tunnel Management Protocol—See *ATMP*.

ASCII—American Standard Code for Information Interchange. ASCII is a character-encoding system used on Local Area Networks (LANs). The 128 standard ASCII characters are composed of seven bits and have the values 0–127. The extended ASCII character set contains another 128 values.

ASCII mode—A Telnet mode for terminal-server users. In ASCII mode, bit 8 is set to 0 (zero). ASCII mode is also called *standard 7-bit mode* or *Network Virtual Terminal (NVT) ASCII*. This mode is the default if no other mode is specified. Compare with *Binary mode*, *Transparent mode*. See also *Telnet*, *Telnet mode*.

ASCII text file—A file that contains only letters, numbers, and punctuation symbols. An ASCII text file cannot include hidden text-formatting codes. See also *ASCII*.

ASE—Autonomous System External. A TAOS unit uses the term ASE to denote external routes it imports into its Open Shortest Path First (OSPF) database. The TAOS unit redistributes these routes by means of OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers running Routing Information Protocol (RIP). See also *external route*, *OSPF*, *RIP*, *router*.

ASE Type-5—Autonomous System External Type-5. ASE Type-5 is an external route originated by an Area Border Router (ABR) as a Link State Advertisement (LSA). An Open Shortest Path First (OSPF) normal area allows Type-5 LSAs to be transmitted throughout it. A Not So Stubby Area (NSSA) and a stub area do not receive or originate Type-5 LSAs. However, for NSSAs, all routes imported to OSPF have the P-bit set (P stands for *propagate*). When the P-bit is enabled, ABRs translate Type-7 LSAs to Type-5 LSAs, which can then be transmitted to the backbone. These external routes are considered Type-7 LSAs. Compare with *ASE Type-7*. See also *ABR*, *AS*, *ASE*, *external route*, *LSA*, *normal area*, *NSSA*, *OSPF*, *stub area*.

ASE Type-7—Autonomous System External Type-7. ASE Type-7 is a type of Link State Advertisement (LSA) defined for Not So Stubby Areas (NSSAs) in Open Shortest Path First (OSPF) version 2. For NSSAs, all routes imported to OSPF have the P-bit set (P stands for *propagate*). When the P-bit is enabled, ABRs translate Type-7 LSAs to Type-5 LSAs, which can then be transmitted to the backbone. These external routes are considered Type-7 LSAs. Compare with *ASE Type-5*. See also *AS*, *ASE*, *LSA*, *NSSA*, *OSPF*, *stub area*.

ASGCP—Access SS7 Gateway Control Protocol. ASGCP enables you to integrate a TAOS unit into a Signaling System 7 (SS7) network. With an ASGCP-Q.931+ license, a TAOS unit can decrease congestion on the Public Switched Telephone Network (PSTN) caused by users connecting to the Internet. Compare with *IPDC*. See also *PSTN*, *SS7*, *SS7 network*.

ASN.1—Abstract Syntax Notation One. In the OSI Reference Model, ASN.1 is a notation for describing data structures on a network. It provides a consistent syntax when transferring data between different systems. See also *OSI Reference Model*.

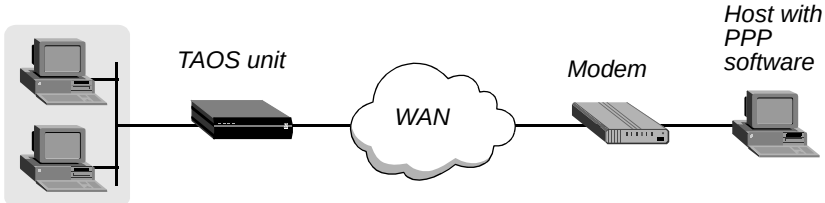
ASTN message—Acknowledge Send Tones message. A message sent by a TAOS unit to a Signaling System 7 (SS7) signaling gateway to confirm that the call-progress tones or voice announcements requested by a Send Tones (STN) message have been played. Compare with *STN message*. See also *signaling gateway*, *SS7*, *VoIP*.

Asymmetric Digital Subscriber Line—See *ADSL*.

asynchronous communications server—A LAN server that enables a network user to dial out of the network and into the Public Switched Telephone Network (PSTN), or to access dedicated lines for asynchronous communications. An asynchronous communications server is also called a *dial-in/dial-out server* or a *modem server.* See also *asynchronous transmission*.

asynchronous PPP—A mode for sending Point-to-Point Protocol (PPP) packets. In asynchronous mode, the characters that form the data packets are sent at irregular intervals, without a clocking signal. Figure 6 illustrates a single-channel asynchronous PPP call in which the calling device is a modem.

Figure 6. Asynchronous PPP connection



Asynchronous PPP is commonly used in lower-speed transmission and less-expensive transmission systems. See also *asynchronous transmission*, *PPP*.

Asynchronous Transfer Mode—See *ATM*.

asynchronous transmission—A mode in which the sending and receiving serial hosts know where a character begins and ends because each byte is framed with additional bits, called a *start bit* and a *stop bit*. A start bit indicates the beginning of a new character. It is always 0 (zero). A stop bit marks the end of the character. It appears after the parity bit if parity bits are in use.

An asynchronous link uses the type of serial communication provided by a PC COM port. A dial-in modem or V.120 Terminal Adapter (TA) initiates an asynchronous host-to-network or host-to-host connection. The call can use Point-to-Point Protocol (PPP) encapsulation, V.120 encapsulation, or raw (unencapsulated) Transport Control Protocol (TCP).

A TAOS unit routes an asynchronous call to a digital modem as a voice call, and then to the terminal-server software. If the terminal server does not detect a PPP packet, it begins a login sequence. If the terminal server detects a PPP packet, it passes the call on to the router, where it is handled as a regular PPP connection. The caller never sees the terminal-server interface.

See also *asynchronous PPP*, *digital modem*, *PPP*, *TCP*, *terminal server*, *V.120*, *V.120 TA*.

async PPP—See *asynchronous PPP*.

AT command set—A set of standard instructions used to activate functions on a modem. Originally developed by Hayes Microcomputer Products, the AT command set is now used by almost all modem manufacturers. See also *modem*.

AT switch—Access Tandem switch. A tandem switch that provides equal-access connections for carriers by linking local end-office switches. An AT switch aggregates voice and data calls from several local switches, then connects to a tandem switch in another area's network to move calls from one region to another. Typically, the tandem switch receives toll traffic and uses its trunks to process and route the traffic to and from another service provider's end-office switch.

ATCP—AppleTalk Control Protocol. A protocol that enables you to route AppleTalk packets that are encapsulated in Point-to-Point Protocol (PPP).

ATM—Asynchronous Transfer Mode. ATM is a packet-switched, broadband network architecture central to Broadband ISDN (B-ISDN). It ensures reliable delivery of packets and provides very high bandwidth, enabling data, voice, and video transmissions to occupy the same line.

ATM is based on connections, not channels. The term *asynchronous* refers to the way in which ATM achieves its unchannelized bandwidth allocation. ATM sends data associated with a connection only when there is actual data to send. This functionality is in contrast to that found in channelized or Time Division Multiplexing (TDM) networks, in which a special bit pattern must be sent in every time slot representing a channel, even when the connection is idle.

In the past, companies built large voice, data, and television networks to accommodate each specific kind of data transmission. Duplication of effort and tremendous cost outlays resulted. Because many of these networks were built for peak load conditions, the average usage was typically very low, leading to excessive costs. Many organizations needed to find ways to use a single network infrastructure and assign bandwidth on an as-needed basis.

ATM lets both private corporations and public service providers build unchannelized networks to make more efficient use of the underlying bandwidth on the network. By offering scalable rates from 1.5Mbps to 155Mbps or higher, ATM services can make the WAN transparent for applications. And unlike Frame Relay or other data services, ATM can easily accommodate delay-sensitive traffic such as voice and video.

ATM uses very short, fixed-length packets called *cells*. The ATM cell is 53 bytes long, consisting of a 5-byte header containing an address, and a fixed 48-byte information field. To handle the various data types on a network, ATM supports five service classes: Constant Bit Rate (CBR), Variable Bit Rate-Real Time (VBR-RT), Variable Bit Rate Non-Real Time (VBR-NRT), Available Bit Rate (ABR), and Unspecified Bit Rate (UBR).

ATM is also known as *cell relay.* See also *ABR, ATM, B-ISDN, broadband, CBR, cell, packet-switched network, packet switching, UBR, VBR-NRT, VBR-RT*.

ATM Adaptation Layer—See *AAL*.

ATM cell—A 53-byte, fixed-length Asynchronous Transfer Mode (ATM) data packet that contains the following fields:

- Generic Flow Control (GFC)
- Virtual Path Identifier (VPI)
- Virtual Channel Identifier (VCI)
- Payload Type (PT)
- Cell Loss Priority (CLP)
- Header Error Control (HEC)
- Payload

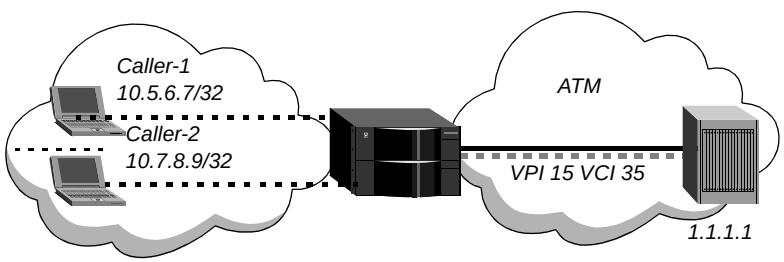
See also *ATM, CLP, GFC, HEC, Payload, PT, VCI, VPI.*

ATM circuit—A point-to-point Permanent Virtual Circuit (PVC) established on the TAOS unit. An ATM circuit can make use of any two physical interfaces in the system.

ATM contract—See *QoS contract*.

ATM-direct—A feature that enables a TAOS unit to concentrate incoming Point-to-Point Protocol (PPP) calls onto an Asynchronous Transfer Mode (ATM) interface. ATM-direct aggregates multiple PPP connections and forwards them as a combined data stream. An upstream device then examines the packets and routes them appropriately. In Figure 7, the TAOS unit forwards the data stream from two PPP dial-in hosts across the same ATM link.

Figure 7. ATM-direct concentrating PPP calls to an ATM interface



An ATM-direct connection is not a full-duplex tunnel between a PPP dial-in user and a remote device. Although the TAOS unit does not route the packets onto the ATM link, it must use the router to send packets received across ATM back to the appropriate PPP caller. For this reason, ATM-direct connections must enable IP routing.

See also *ATM*, *IP routing*, *PPP*.

ATM direct trunk—A logical-port configuration that enables you to make a direct trunk connection between two Asynchronous Transfer Mode (ATM) switches. See also *ATM*.

ATM End System Address format—See *AESA format*.

ATM Flow-Control Processor—An Asynchronous Transfer Mode (ATM) network-management system that uses binary, hop-by-hop, closed-loop flow-control algorithms that shift network congestion to the edge of the network. See also *ATM*.

ATM framer—A device that multiplexes Asynchronous Transfer Mode (ATM) cells into the SONET payload and extracts cells from the SONET payload for reassembly into packets. See also *SONET*.

ATM IISP-DCE—Asynchronous Transfer Mode Interim Inter-switch Signaling Protocol–Data Circuit-terminating Equipment. A logical-port configuration that enables you to connect two ATM switches by means of IISP DCE ports. This service routes Switched Virtual Circuits (SVCs) through a mixed-vendor switch network. Compare with *ATM IISP-DTE*. See also *ATM*, *logical port*, *SVC*.

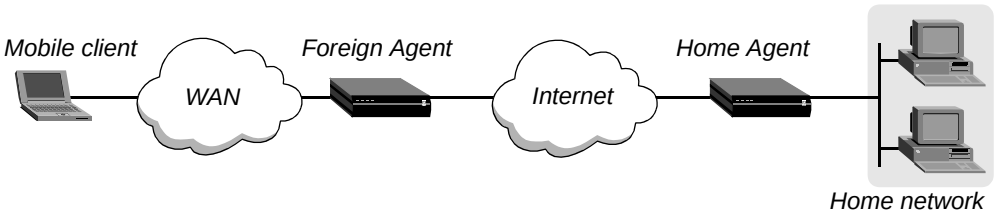
ATM IISP-DTE—Asynchronous Transfer Mode Interim Inter-switch Signaling Protocol–Data Terminal Equipment. A logical-port configuration that enables you to connect two ATM switches by means of IISP DTE ports. This service routes Switched Virtual Circuits (SVCs) through a mixed-vendor switch network. Compare with *ATM IISP-DCE*. See also *ATM*, *logical port*, *SVC*.

ATM layer—The core layer of the Asynchronous Transfer Mode (ATM) standard. The ATM layer routes the cells across the network, performing both multiplexing and demultiplexing functions. See also *AAL*, *ATM*.

ATMP—Ascend Tunnel Management Protocol. ATMP provides a tunneling mechanism between two TAOS units across the Internet or a Frame Relay network. The protocol uses standard Generic Routing Encapsulation (GRE) and is based on the User Datagram Protocol (UDP) and Internet Protocol (IP). ATMP provides a Virtual Private Network (VPN) solution over the backbone resources of Internet Service Providers (ISPs) and carriers. Without ATMP, each mobile client and remote user has to dial directly into the network, resulting in long-distance charges. With ATMP, users can make a local call and have the transmission securely tunneled.

Figure 8 shows an ATMP tunnel between two TAOS units. A mobile client, such as a traveling salesperson, initiates the connection. The unit that authenticates the mobile client is the ATMP Foreign Agent. The unit that gains access to the home network is the ATMP Home Agent. The home network is the destination network for mobile clients. In Figure 8, the mobile client is a salesperson who logs in to an ISP (the Foreign Agent) to access her home network.

Figure 8. ATMP tunnel across the Internet



As described in RFC 1701, GRE hides packet contents and enables transmission of packets that the Internet would otherwise not accept. When you use ATMP with a TAOS unit, you can transmit either IP packets that use unregistered addresses or IPX packets from roaming clients. See also *Foreign Agent*, *Frame Relay*, *GRE*, *Home Agent*, *home network*, *IP*, *IPX*, *ISP*, *mobile client*, *UDP*, *VPN*.

ATM service class—A method of designating the type of Asynchronous Transfer Mode (ATM) service in use. ATM supports five service classes to handle the various data types on a network. Each service class ensures optimal network usage and guaranteed end-to-end delivery. The five ATM service classes are Constant Bit Rate (CBR), Variable Bit Rate-Real Time (VBR-RT), Variable Bit Rate Non-Real Time (VBR-NRT), Available Bit Rate (ABR), and Unspecified Bit Rate (UBR). See also *ABR*, *ATM*, *CBR*, *UBR*, *VBR-NRT*, *VBR-RT*.

ATM service interworking feeder—A feature that enables the system to feed Frame Relay network traffic into an ATM network so that a Frame Relay end user can communicate with an ATM end user. See also *ATM*, *Frame Relay network*.

ATM Setup message—An Asynchronous Transfer Mode (ATM) signaling message that enables a device to select the desired bandwidth and Quality of Service (QoS) levels when establishing a connection. The Setup message is sent by the calling user to the network and by the network to the called user. Key information elements of the Setup message include the following:

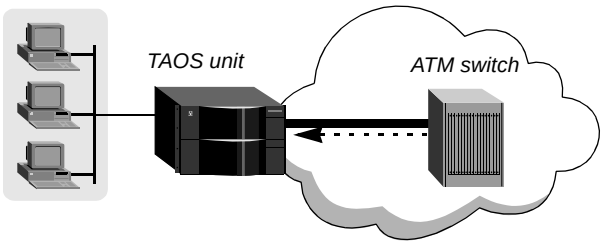
- ATM Adaptation Layer (AAL) parameters
- ATM user cell rate
- Broadband bearer capability
- Called-party number
- Calling-party number
- Connection identifier
- QoS class

See also *ATM*, *called-party number*, *CLID*, *QoS*.

ATM SVC—Asynchronous Transfer Mode Switched Virtual Circuit. An ATM SVC is a point-to-point switched connection between ATM interfaces. An ATM SVC provides a lower-cost, usage-based alternative to an ATM Permanent Virtual Circuit (PVC). Like other types of switched connections, SVCs can be initiated by a dial-in or a dial-out call.

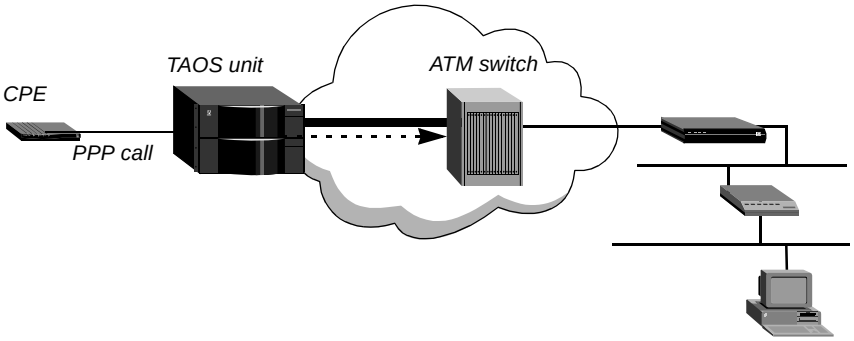
A dial-in ATM SVC terminates locally. The TAOS unit receives the call on an ATM interface. An example of a terminating SVC is shown in Figure 9.

Figure 9. Terminating SVC on an ATM interface



A dial-out ATM SVC is initiated as an outgoing call on an ATM interface. Dial-out can be initiated explicitly, or it can take place on the basis of IP routing. Figure 10 shows a Pipeline™ unit using Point-to-Point Protocol (PPP) to dial in to a MAX TNT® unit. The MAX TNT unit establishes the incoming call and then dials out on an ATM interface on the basis of IP routing, just as it would for another type of switched dial-out call.

Figure 10. Dial-out SVC on an ATM interface



Unlike PVCs, which require dedicated connections, SVCs are on-demand connections and must use ATM end-point addresses to identify the interface and route to it. See also *ATM*, *PPP*, *PVC*, *SVC*.

ATM UNI–DCE—Asynchronous Transfer Mode User-to-Network Interface–Data Circuit-terminating Equipment, a configuration in which the logical port communicates with ATM Customer Premises Equipment (CPE) over Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). Compare with *ATM UNI–DTE*. See also *ATM*, *CPE*, *PVC*, *SVC*.

ATM UNI–DTE—Asynchronous Transfer Mode User-to-Network Interface–Data Terminal Equipment, a configuration in which the logical port communicates with an ATM switch over Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). Compare with *ATM UNI–DCE*. See also *ATM*, *CPE*, *PVC*, *SVC*.

Attached Resource Computer Network—See *ARCnet*.

attenuation—The reduction in the strength of a signal over distance, expressed in decibels per kilometer (dB/km) or per 100 feet. Factors affecting attenuation are the frequency range of the signal, wire shielding, and cable type. Unshielded Twisted Pair (UTP) cable suffers from the most attenuation, while fiberoptic cable has very little attenuation. See also *attenuator, UTP cable*.

attenuator—A device that reduces the amplitude of a signal. See also *attenuation.*

attribute—A characteristic, similar to a parameter, in a RADIUS user profile or pseudo-user profile. RADIUS attributes can be assigned values to specify usernames and passwords and to configure routing, call management, and usage restrictions. See also *pseudo-user profile, RADIUS, RADIUS server, user profile*.

attribute set—In a transparent tunneling configuration, a set of RADIUS attributes that share the same tag number. A user's profile includes a primary attribute set, which specifies all of the values required to set up the tunnel, and additional attribute sets that can be used to establish a tunnel if the primary server is unavailable. See also *tag*.

attribute-value pair—See *AVP*.

ATU—ADSL Transceiver Unit. An ATU is a hardware device used with ADSL service. It connects to an Ethernet interface on one end and a telephone jack on the other. An ATU-C is the device for the Central Office (CO) side, and an ATU-R is the Customer Premises Equipment (CPE) device. See also *CO, CPE*.

audio codec—A device that encodes analog voice data into a digital signal for transmission over a digital medium. See also *codec, G.711 audio codec, G.728 codec, RT-24 codec*.

AUI—Auxiliary Unit Interface. An AUI is a 15-pin D-type connector for Ethernet connections. It typically links a cable to a Network Interface Card (NIC). An AUI is also known as a *Digital, Intel, Xerox (DIX) connector.* See also *Ethernet, NIC*.

authority zone—A portion of the domain-name hierarchy associated with a name server.

authentication—A method of identifying the users permitted to gain access to network resources. Authentication is the first line of defense against unauthorized access to your network. Each TAOS unit supports a variety of authentication methods. You can use:

- Calling-Line ID (CLID) to verify that the call is placed from a trusted telephone number.
- Called-number authentication to verify the number called.
- Callback security. After authentication is complete, the TAOS unit can hang up and call back, ensuring that the connection is made only with a trusted number.
- Expect-send scripts to authenticate logins to the terminal server.
- Name and password authentication of Point-to-Point Protocol (PPP) calls. TAOS units support Password Authentication Protocol (PAP), PAP with encryption (PAP-DES), Challenge Handshake Authentication Protocol (CHAP), and Microsoft's extension of CHAP (MS-CHAP).
- Token cards. Using a token-card server, you can accept or reject calls by means of PAP-Token, PAP-Token-CHAP, or Cache-Token authentication.

When a TAOS unit is shipped from the factory, it is set to not require any authentication.

See also *Cache-Token authentication, called-number authentication, CHAP, CLID authentication, expect-send script, PAP, PAP-Token authentication, PAP-Token-CHAP authentication, token card, token-card authentication, token-card server*.

Authentication Header—See *AH*.

authentication key—A shared secret passed between a TAOS unit and an authentication server. An authentication key can be one of the following types:

- If the TAOS unit is acting as a RADIUS, TACACS, or TACACS+ client, the authentication key is a password supplied by the TAOS unit to the server.
- If the TAOS unit is acting as a Defender client, the authentication key is a DES secret key shared between the TAOS unit and the Defender authentication server. This key is also used for authentication by the TAOS unit in its role as a Defender authentication agent.
- In Open Shortest Path First (OSPF) routing, the authentication key is a 64-bit clear password inserted into the OSPF packet header. The key is used by OSPF routers to allow or exclude packets from an area.

See also *authentication server*, *OSPF*, *RADIUS*, *TACACS*, *TACACS+*.

authentication request—A request that a TAOS unit sends to an authentication server on behalf of a client requesting access. See also *authentication response*, *authentication server*.

authentication response—A response from an authentication server, notifying the TAOS unit that a user's request for access has been either granted or denied. See also *authentication request*, *authentication server*.

authentication server—An external server, such as a RADIUS, TACACS, TACACS+, or token-card server, that verifies whether a user requesting access to the network has permission to use network resources. See also *RADIUS*, *RADIUS server*, *TACACS*, *TACACS+*, *token-card server*.

authentication timeout—The number of seconds between retries to an external authentication server. If the TAOS unit is acting as a RADIUS, TACACS, or TACACS+ client, the unit waits the specified number of seconds for a response to an authentication request. If it does not receive a response within that time, it times out and sends the authentication request to the next authentication server. If the TAOS unit is acting as a Defender or SecurID client (both of which support only one server address), it waits the specified number of seconds before assuming that the server is unavailable. See also *authentication server*, *RADIUS*, *RADIUS server*, *TACACS*, *TACACS+*.

authenticator field—In a RADIUS packet, a field that enables the system to authenticate transmissions between the TAOS unit and the authentication server. See also *authentication*, *authentication server*, *CHAP*, *DES*, *encryption*, *RADIUS*, *RC4*.

Authority and Format Identifier—See *AFI*.

authorization—Permission for a user to carry out tasks after he or she has access to the LAN. Authorization occurs *after* authentication is complete. See also *authentication*.

autobaud—A method of training up to a set modem data rate. If a DSL modem cannot train to this data rate, it will connect at the closest rate to which it can train (the modem's ceiling rate). See also *modem rate control*.

Auto-BERT—Automatic Bit Error Rate Test. During an Auto-BERT, a TAOS unit monitors the entire data stream between codecs. At the end of the time period, if any channels have failed, the TAOS unit clears them, redials, and repeats the test. The maximum number of errors that can accumulate per channel is 65,000. The TAOS unit reports the total number of errors for each channel during the current call, but not the error rate. The unit resets the error display for the current call to 0 (zero) when the call disconnects.

Automatic-at-Startup rate adaptation—A type of rate adaptation that specifies that the Customer Premises Equipment (CPE) initializes at a minimum specified bit rate and target noise margin. If the CPE fails to achieve the minimum bit rate in either direction, it cannot initialize, and it sends a message that the requested bit rate was too high. If the CPE can support a higher bit rate than the specified minimum, it can train up to a higher rate within the acceptable noise margin. Each direction can have a different minimum and maximum bit rate for the fast or interleaved ADSL channel. Compare with *Operator-Controlled rate adaptation*. See also *ADSL*, *CPE*.

Automatic Bit Error Rate Test—See *Auto-BERT*.

Automatic Call Distributor—See *ACD*.

automatic LIM port redundancy—Automatic Line Interface Module port redundancy. A feature that enables a Stinger™ unit to detect a Line Interface Module (LIM) port failure and automatically transfer the port connection to the same port on the spare LIM. When automatic LIM port redundancy is activated, the primary LIM port is monitored. If modem errors exceed the specified thresholds, the port connection to the primary LIM is transferred to the spare (secondary) LIM. Monitoring continues on the secondary LIM port. If modem errors again exceed thresholds, the connection is transferred back to the primary LIM port and the automatic redundancy process stops. See also *LIM*, *LIM port redundancy*.

automatic LIM redundancy—Automatic Line Interface Module redundancy. A feature that enables a Stinger unit to detect a Line Interface Module (LIM) failure and automatically set up all the Virtual Channels (VCs) of that LIM on the spare. When automatic LIM redundancy is activated, the primary LIM is monitored. If modem errors exceed the specified thresholds, all connections to the primary LIM are transferred to the spare (secondary) LIM. Monitoring continues on the secondary LIM. If modem errors exceed thresholds, the connections are transferred back to the primary LIM and the automatic redundancy process stops. See also *LIM*, *LIM redundancy*.

automatic Line Interface Module port redundancy—See *automatic LIM port redundancy*.

automatic Line Interface Module redundancy—See *automatic LIM redundancy*.

Automatic Number Identification—See *ANI*.

Autonomous System—See *AS*.

Autonomous System Border Router—See *ASBR*.

autoranging—The power supply's ability to detect the correct voltage received from the power source.

autosensing—A feature that enables you to change the device attached to an Ethernet port without reconfiguring the TAOS unit.

Auxiliary Unit Interface—See *AUI*.

Available Bit Rate—See *ABR*.

Available Cell Rate—See *AvCR*.

AvCR—Available Cell Rate. The available capacity for Constant Bit Rate (CBR), Variable Bit Rate-Real Time (VBR-RT), and Variable Bit Rate Non-Real Time (VBR-NRT) services. For Available Bit Rate (ABR) service, AvCR specifies the capacity available for Minimum Cell Rate (MCR) reservation. See also *ABR*, *CBR*, *MCR*, *PNNI*, *VBR-NRT*, *VBR-RT*.

Average Line Utilization—See *ALU*.

Average Queue Length—See *AQL*.

AVP—Attribute-value pair. (1) A RADIUS attribute and its specified value. Packets sent between a RADIUS server and a Network Access Server (NAS) consist of AVPs, such as `password="s64bigE&rt"`. See also *attribute*, *NAS*, *RADIUS*.

(2) In a Layer 2 Tunneling Protocol (L2TP) configuration, a variable-length string consisting of the name of a unique attribute and the attribute's value. AVPs make up the control messages used for establishing, maintaining, and disconnecting L2TP tunnels. See also *L2TP*.

B

B8ZS—Bipolar with 8-Zero Substitution. B8ZS is an encoding method in which an alternating positive and negative voltage represents a 1 (one), no voltage represents a 0 (zero), and at least one bit out of every eight bits must be a 1 (one).

backbone—The part of the communications network designed to carry the bulk of the traffic. The backbone provides connectivity between subnets in an enterprise-wide network. See also *enterprise-wide network, IP subnet*.

backbone area—An Open Shortest Path First (OSPF) area that connects routers for the purpose of hierarchical routing. The backbone area is special and always has the area number 0.0.0.0. To tie areas together, some routers belong to the backbone area and one other area. These routers are called *Area Border Routers (ABRs)*. See also *ABR, area, OSPF, router*.

backbone network—A network with a central cabling scheme linking it to other networks. Hosts on networks linked to the backbone can communicate with one another. See also *backbone router*.

backbone router—A router attached to a backbone network by dedicated lines. Usually, a backbone router does not have built-in digital dial-up WAN interfaces. Manufacturers of backbone routers include Cisco, Wellfleet, 3Com, and CrossCom. See also *backbone network, router*.

backoff queue—A file in which the RADIUS accounting server stores unacknowledged records. See also *accounting server, RADIUS*.

backplane—A circuit board assembly that provides a means of transferring signals between other circuit board assemblies connected to it.

back-to-back connection—A link in which the output of a sending device is connected directly to the input of a receiving device.

backup—The ability of the system to establish and use a temporary, alternative connection to a destination when the primary connection becomes unavailable. A backup connection replaces the primary connection, which must be a dedicated connection. The backup interface can be dedicated or switched.

When the system detects that the primary interface is unavailable, it puts the primary interface in a Backup Active state. *It does not remove the routes to the primary interface*. The system then diverts traffic from the primary to the backup interface. When the system detects that the primary interface is available again, it diverts traffic back to the primary interface. It also disconnects the backup interface if that interface has a switched connection. But if the backup interface is a dedicated link, the routes to the backup interface remain active.

Nested backups are not supported. The profile for a backup interface cannot specify another backup interface. The profile for a backup interface does not inherit attributes, such as filters or firewalls, from the profile for the primary dedicated connection.

See also *dedicated circuit, switched circuit*.

backup and overflow—See *FT1-B&O*.

Backup Designated Router—See *BDR*.

Backward Explicit Congestion Notification—See *BECN*.

BACP—Bandwidth Allocation Control Protocol. BACP provides dynamic bandwidth allocation for Multilink PPP (MP) connections. With criteria very similar to those for the bandwidth-on-demand feature in Multilink Protocol Plus (MP+), BACP can be used with digital or analog links. BACP is described in RFC 2125. See also *MP*, *MP+*.

balun—A small device that connects a balanced line (such as a twisted-pair cable) to an unbalanced line (such as a coaxial cable). See also *coaxial cable*, *twisted-pair cable*.

bandwidth—The amount of data a link can carry, measured in bits per second (bps) for digital signals and in hertz (Hz) for analog signals. See also *analog signal*, *digital signal*.

Bandwidth Allocation Control Protocol—See *BACP*.

Bandwidth Allocation Protocol—See *BAP*.

bandwidth-on-demand—A WAN feature that enables a user to add bandwidth as required. See also *bandwidth*.

Bandwidth ON Demand Interoperability Group—See *BONDING*.

banner—The text that first appears when a user logs in to the terminal server.

BAP—Bandwidth Allocation Protocol. BAP is a PPP protocol for managing bandwidth between two peers. Using BAP, the peers coordinate the process of adding and removing bandwidth. See also *BACP*, *PPP*.

base channel count—The initial number of channels to use for a Multilink PPP (MP) or Multilink Protocol Plus (MP+) connection. See also *MP*, *MP+*.

Basic Rate Interface line—See *ISDN BRI line*.

baud rate—The number of times a signal can switch from one state to another within 1 second. The more times a switch can occur, the higher the baud rate.

Bc—Committed Burst. Bc is the maximum number of data bits that the network agrees to transfer, under normal conditions, during the time interval specified by Tc. The Bc value is defined for each Permanent Virtual Circuit (PVC). See also *PVC*, *Tc*.

B channel—A 64Kbps channel that carries user data. A B channel is a bearer channel, one of the fundamental components of the ISDN interface. See also *E1 PRI line*, *ISDN*, *ISDN BRI line*, *T1 PRI line*.

B-channel bundling—A technique for putting multiple voice conversations on a single line. Speech is divided so that bits are transmitted only when someone is speaking. In T1 multiplexing, bundles consist of four bits, represent 11 channels carrying 32Kbps of compressed data, and have an associated signaling Delta channel. See also *B channel*.

BDR—Backup Designated Router. A BDR is the router that an Open Shortest Path First (OSPF) area uses in the event that the Designated Router (DR) goes out of service. To prevent the DR from becoming a serious liability to the network if it fails, OSPF elects a Backup Designated Router (BDR). Other routers maintain adjacencies with both the DR and BDR, but the backup router leaves as many processing tasks as possible to the DR. If the DR fails, the BDR immediately becomes the DR, and a new BDR is elected.

A TAOS unit can function as either a DR or a BDR. However, to dedicate the TAOS unit to WAN processing, many sites choose to assign both these functions to LAN-based routers. See also *adjacency*, *area*, *DR*, *OSPF*, *router*.

Be—Excess Burst. Be is the maximum number of bits of uncommitted data, in excess of the Committed Burst (Bc) size, that a Frame Relay network attempts to deliver during the time interval specified by Tc. In general, Be is delivered with a lower probability than Bc and is considered eligible for discard. See also *Bc*, *Tc*.

bearer channel—See *B channel*.

bearer service—An ISDN service for transmitting information from one device to another. Common bearer services are circuit-switched and Frame Relay services. See also *circuit switching*, *Frame Relay*.

BECN—Backward Explicit Congestion Notification. BECN is a bit used in a Frame Relay header to notify Data Terminal Equipment (DTE) that there is traffic congestion on the network and that the sending device should begin congestion-avoidance procedures. Compare with *FECN*. See also *congestion*, *congestion management*, *Frame Relay*.

Bell 103—A carrier standard created by Bell Labs in the 1960s and 1970s. Bell 103 accommodates modem-to-modem speeds of up to 300bps and is equivalent to the International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) V.21 standard. See also *ITU-T*, *V.21*.

Bell 212A—A carrier standard created by Bell Labs in the 1960s and 1970s. Bell 212A accommodates modem-to-modem speeds of up to 1200bps, and is equivalent to the International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) V.22 standard. See also *ITU-T*, *V.22*.

BER—Bit Error Rate. The BER is the number of received bits with errors as a percentage of the total number of bits received. It is commonly expressed as a number to the power of 10. See also *BERT*.

BERT—Bit Error Rate Test. The BERT calculates the number of received bits with errors as a percentage of the total number of bits received. See also *BER*.

Best Effort—A bit in an Asynchronous Transfer Mode (ATM) cell header, specifying that the network attempts to deliver traffic in excess of the limits of the Quality of Service (QoS) contract. However, there are no guarantees that traffic will be delivered. See also *ATM*, *QoS contract*.

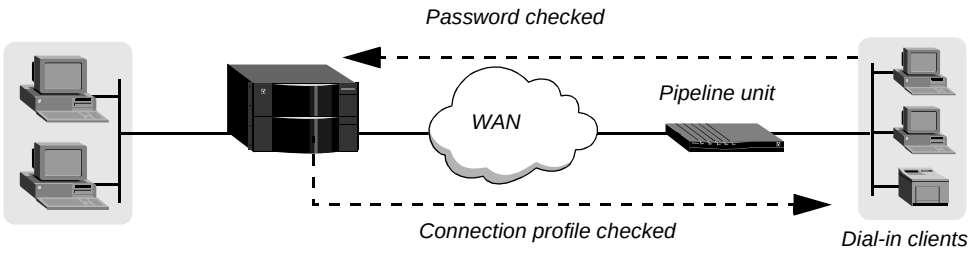
best-effort packets—Packets delivered to the best of the network's ability, after the requirements for delivering the guaranteed packets have been met. Compare with *guaranteed packets*.

bidirectional Challenge Handshake Authentication Protocol—See *bidirectional CHAP*.

bidirectional CHAP—An implementation of the Challenge Handshake Authentication Protocol (CHAP) that enables the called PPP device and the calling PPP device to authenticate each other. The called device determines whether the caller is permitted to access its resources, and the caller determines whether the remote site is the correct one. Bidirectional CHAP increases compliance with the RFC 1994 standard for PPP CHAP authentication. Note that the feature is not implemented for PAP-based authentication (PAP, PAP-TOKEN, or PAP-TOKEN-CHAP). Bidirectional CHAP is supported locally and through RADIUS.

Figure 11 shows a configuration in which a TAOS unit and its dial-in clients authenticate each other by means of bidirectional CHAP. One or more clients can dial in to the TAOS unit. The TAOS unit authenticates each calling device by means of a Connection profile, and each dial-in client authenticates the TAOS unit by means of a password value.

Figure 11. Bidirectional CHAP for all incoming calls to a TAOS unit



Note: As noted in RFC 1994, a security hole can occur when you use bidirectional authentication for an incoming call if the secrets used in each of the two directions are identical. Bidirectional authentication on a TAOS unit has been developed to avoid the security hole, even if the secrets are identical. For best results, however, Lucent Technologies recommends that you specify a different secret for each authentication direction.

See also *CHAP*.

binary data—Data in the form of zeroes and ones.

Binary mode—The Telnet eight-bit Binary option. You can run XModem and other eight-bit file transfer protocols with Binary mode. However, in Binary mode, the Telnet escape sequence does not operate. The Telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit. A user can override the Binary setting on the Telnet command line. Compare with *ASCII mode*, *Transparent mode*. See also *Telnet*, *Telnet mode*.

Binary Local mode—A data-transfer mode for X.25/T3POS calls. Binary Local mode specifies that there is no error recovery between the T3POS Packet Assembler/Disassembler (PAD) and the host, but that error recovery is in place between the PAD and the DTE. Like Blind mode, Binary Local mode passes data between the DTE and the host without reference to the protocol being used. Unlike Blind mode, Binary Local specifies that the system continues to use the T3POS protocol between the DTE and the PAD. Compare with *Blind mode*, *Local mode*, *Transparent mode*. See also *DTE*, *PAD*, *X.25/T3POS*.

BIP—Bit Interleaved Parity. BIP is an error-detection method that uses odd or even parity to verify the accuracy of a transmission.

Bipolar with 8-Zero Substitution—See *B8ZS*.

B-ISDN—Broadband-Integrated Services Digital Network. B-ISDN is a very high-speed data service, providing data transmission over fiberoptic media at a rate of 155Mbps and higher. See also *broadband*, *broadband network*, *E1 line*, *ISDN*, *T1 line*.

Bit—Binary digit, the smallest unit of information a computer can process, representing one of two states (indicated by 1 and 0).

Bit Interleaved Parity—See *BIP*.

bit inversion—A method of turning data 1s into 0s and data 0s into 1s. Bit inversion applies only to calls between codecs. In some connections, you need to invert the data to avoid transmitting a pattern that the connection cannot handle. If you apply bit inversion, you should do so on both sides of the connection. See also *codec*.

bit rate—The number of bits that travel over a connection per second. See also *bps*.

bits per second—See *bps*.

blackhole interface—An interface that enables a router to handle packets whose IP address matches an unused IP address in a summarized address pool. The blackhole interface has an IP address of 127.0.0.3. When you specify this address as the router to the destination pool network, the TAOS unit silently discards packets to an invalid host on that network. See also *pool summary*.

Blind mode—A data-transfer mode for X.25/T3POS calls. Blind mode provides a method of passing raw binary data between a Data Terminal Equipment (DTE) device and the host system without reference to the protocol being used. In addition, Blind mode specifies that the T3POS Packet Assembler/Disassembler (PAD) does not provide any error recovery. In this mode, the DTE device and the host system provide error recovery for the connection. Note that the T3POS PAD does not clear a call when it receives a clear-request command from the DTE device. The PAD or the host system must clear the call. Compare with *Binary Local mode*, *Local mode*, *Transparent mode*. See also *DTE*, *PAD*, *X.25/T3POS*.

Blue Alarm signal—An alarm signal indicating that the unit is receiving all 1s. Compare with *RAI*, *Red Alarm signal*.

BNC connector—A small connector with a half-turn locking shell. A BNC connector is commonly used with 10Base2 cabling.

BONDING—Bandwidth ON Demand Interoperability Group. BONDING is a consortium of over 40 data-communications-equipment vendors and service providers who joined together to create a standardized inverse-multiplexing protocol. The BONDING protocol enables inverse multiplexers from different vendors to interoperate. BONDING also refers to the resultant specification, sometimes known as the *BONDING specification*. See also *inverse multiplexer*, *inverse multiplexing*.

BOOTP—Boot Protocol. BOOTP starts up a network device by using information from a server. A TAOS unit can use BOOTP to get settings and check for a new software load. In addition, you can enable the terminal server to respond to BOOTP within a Serial Line Internet Protocol (SLIP) session. An interactive user who initiates a SLIP session can get an IP address from a designated IP address pool by means of BOOTP. See also *BOOTP relay*, *BOOTP request*, *BOOTP server*, *DHCP*, *IP address*, *IP address pool*, *SLIP*, *terminal server*.

BOOTP relay—A method of sending (*relaying*) Boot Protocol (BOOTP) requests to other networks. On a TAOS unit, you specify the IP address of a BOOTP server for handling BOOTP requests. If a server is on the same LAN as the TAOS unit, BOOTP requests from other networks are relayed to the server. If a server is on another network, BOOTP requests from clients on the same LAN as the TAOS unit are relayed to the remote server. If you specify two BOOTP servers, the TAOS unit that relays the BOOTP request determines when each server is used. See also *BOOTP*, *BOOTP request*, *BOOTP server*.

BOOTP request—A request a client makes to a BOOTP server in order to receive an IP address or start the operating system of a network workstation. See also *BOOTP*, *BOOTP relay*, *BOOTP server*.

Boot Programmable Read-Only Memory—See *Boot PROM*.

Boot PROM—Boot Programmable Read-Only Memory. A Boot PROM is a chip mounted on a printed circuit board. The chip provides executable boot instructions to a computing device. See also *PROM*.

Boot Protocol—See *BOOTP*.

BOOTP server—A server that handles BOOTP requests from network clients. See also *BOOTP*, *BOOTP relay*, *BOOTP request*.

bps—Bits per second. A measure of the capacity of a line.

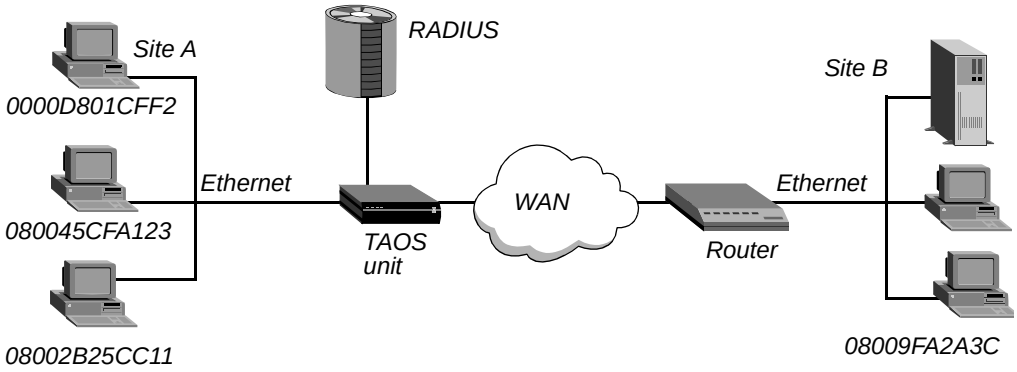
branding—A feature that enables you to select a set of voice announcements for playback from multiple sets of voice announcements stored on a MultiVoice gateway. This feature is useful when you enable multiple logical gateways. See also *logical gateway*, *MultiVoice™*.

bridge—A hardware device that transmits packets between networks. A bridge forwards packets from one network to another and ignores packets destined for hosts on the sending network. Operating at the Data Link layer, a bridge makes multiple networks look like a single network to higher-level protocols and software. See also *Data Link layer*.

bridge entry—An entry in a bridging table. See also *bridge*, *bridging table*.

bridging—A method of moving packets between networks by means of a device called a *bridge*, which operates at the Data Link layer. In Figure 12, the TAOS unit at Site A acts as a bridge between the Ethernet network and Site B.

Figure 12. Bridging configuration



The TAOS unit at Site A gradually learns addresses on both networks by examining each packet's source address, and it develops a bridging table that includes the following entries:

```
0000D801CFF2        SITEA
080045CFA123        SITEA
08002B25CC11        SITEA
08009FA2A3CA        SITEB
```

If the TAOS unit receives a packet whose destination MAC address is not on the local network, it first checks its internal bridging table. If it finds the packet's destination MAC address, the unit dials the connection and bridges the packet. If it does not find the address, the unit checks for active sessions that have bridging enabled. If one or more active bridging links are up, the unit forwards the packet across all active sessions that have bridging enabled.

See also *bridge*, *bridge entry*, *bridging table*, *Data Link layer*.

bridging table—A table that contains entries pairing up a host's Media Access Control (MAC) address with a particular Ethernet interface. If a TAOS unit receives a packet whose destination MAC address is not on the local network, it first checks its bridging table. If it finds the packet's destination MAC address, the unit dials the connection and bridges the packet. If it does not find the address, the unit checks for active sessions that have bridging enabled. If one or more active bridging links are up, the unit forwards the packet across all active sessions that have bridging enabled. See also *bridge*, *bridge entry*, *Ethernet*, *MAC*.

BRI line—See *ISDN BRI line*.

broadband—A data communications technology that transmits data in channels to simultaneously carry several services, such as voice, video, and data, at rates greater than the T1 PRI maximum. See also *B-ISDN*, *broadband network*.

Broadband Integrated Services Digital Network—See *B-ISDN*.

Broadband ISDN—See *B-ISDN*.

broadband network—A network that enables a device to transmit a large amount of voice, data, and video information on the same cable over long distances. See also *B-ISDN*, *broadband*.

Broadband Service Unit—See *BSU*.

broadband wireless LAN—Technology that provides higher data rates than either cellular or packet-radio communication. Broadband wireless LAN products operate at a much higher frequency (up to 2.4MHz) than cellular or packet radio products. However, the range of broadband systems is restricted to approximately 300 yards. Compare with *cellular communication, packet-radio communication*.

broadcast—To send a message to all users currently logged in to the network. Compare with *multicast*. See also *broadcast address, broadcast network, broadcast packet.*

broadcast address—A special address reserved for sending a message to all stations. Generally, a broadcast address is a Media Access Control (MAC) destination address of all 1s (ones). See also *broadcast*, *broadcast network*, *broadcast packet*, *MAC address*.

broadcast network—A network in which the router sends packets to all users, whether they appear on subscription lists or not. In an Open Shortest Path First (OSPF) topology, a broadcast network is any network that has more than two OSPF routers attached and can address a single physical message to all of them. Compare with *multicast network*, *unicast network.* See also *broadcast*, *broadcast address*, *broadcast packet*, *OSPF*, *router*.

broadcast packet—A packet containing a broadcast address, which indicates that all connected hosts receive the message. See also *broadcast*, *broadcast address*, *broadcast network.*

brouter—A networking device that combines the functionality of a bridge and a router.

browser—A software program for navigating and viewing the World Wide Web.

BRQ message—Bandwidth Request message. An H.323 Registration, Admission, and Status (RAS) message sent from a MultiVoice gateway to a MultiVoice Access Manager (MVAM) device, requesting a change in bandwidth. See also *H.323*, *MultiVoice™*, *MVAM*, *RAS.*

BSU—Broadband Service Unit. A BSU is a broadband WAN device that consolidates wide-area Asynchronous Transfer Mode (ATM) access for a combination of video, voice, and LAN-based data traffic. See also *ATM*, *broadband*.

build—The name of the software binary file you install on a TAOS unit. If possible, stay with the same build when upgrading. Loading a different build can cause your unit to lose all or part of its configuration. If this situation occurs, you must restore your configuration from a backup.

buildout—For a T1 line with an internal Channel Service Unit (CSU), the amount of attenuation the TAOS unit should apply to the line's network interface. The value depends on the cable length from the TAOS unit to the next repeater, because a repeater boosts the signal. If the TAOS unit is too close to a repeater, you need to add some attenuation. Obtain the value from your T1 provider. See also *attenuation*, *attenuator*, *CSU*, *repeater*, *T1 line*.

bundle—A group of physical links (such as multiple asynchronous lines) or multiplexed links (such as MP, MP+, X.25, or Frame Relay connections). The links in a bundle can be of different types (for example, dial-up asynchronous and dedicated synchronous connections). See also *bundle owner*.

bundle owner—In a stack of TAOS units, the unit that establishes the initial link. The bundle owner manages the connection's traffic across the stack. Stack peers forward incoming traffic from the WAN to the bundle owner, and the bundle owner receives outgoing traffic destined for the remote end and distributes it to bundled links. See also *bundle*, *MP*, *MP+*, *stack*.

burstiness—On a Frame Relay network, a characteristic of data that does not use the total bandwidth of a connection at all times. See also *Frame Relay network*.

burst mode—A method of transmitting data by collecting and sending it in a single high-speed transmission, rather than one character at a time.

bus—A path for signals transmitted between a computer's CPU and other hardware devices.

byte—Eight bits of data, also called an *octet*.

byte offset—See *offset*.

C

cable modem—A device that delivers high-speed data throughput over the coaxial cables used by the cable TV industry. Cable modems translate radio frequency signals to and from the cable plant into Internet Protocol (IP) signals. Compare with *digital modem*, *modem*.

CAC—Connection Admission Control. In an Asynchronous Transfer Mode (ATM) transmission, CAC consists of tasks performed by the network in order to determine whether to accept or reject a request for a connection or for reallocation of bandwidth. See also *ATM*.

cached token—A password dynamically generated on a token card, transmitted by Challenge Handshake Authentication Protocol (CHAP), and then cached for reuse. When a TAOS unit needs to add channels or make a new call, it uses the cached token to authenticate the additional bandwidth. You can specify a timeout value for the cached token, or configure the system to maintain the token throughout the session. See also *Cache-Token authentication*, *CHAP*, *token*, *token card*, *token-card authentication*, *token-card server*.

Cache-Token authentication—An authentication method that uses Challenge Handshake Authentication Protocol (CHAP) to transmit the initial token, and then caches the token for reuse. The system later uses the cached token when adding new channels or making a new call. See also *ACE authentication*, *cached token*, *SafeWord authentication*, *token*, *token card*, *token-card authentication*, *token-card server*.

call—A single session in which a calling device and an answering device connect over the WAN.

callback—A type of security in which you instruct a TAOS unit to hang up and call back when it receives an incoming call. You can require callback to ensure that the unit makes a connection with a known device. Hanging up and calling back adds a level of certainty that the connection is with a trusted user, especially because the TAOS unit calls back immediately after verifying the user's name and password. For a TAOS unit to use callback, it must be configured to both receive and initiate calls. Callback security applies only to switched lines. See also *Ascend callback*, *authentication*, *CBCP callback*, *CLID callback*, *DNIS callback*, *switched line*.

Callback Control Protocol callback—See *CBCP callback*.

call blocking—A feature that enables you to automatically stop the unit from attempting to place an outgoing call on a connection that repeatedly fails. Successive retries can cause excessive charges, congestion, and performance problems. Using call blocking, you can prohibit additional retries after a specified number of failed connection attempts. You can also control the length of time call blocking is in effect.

Call-Connected packet—A packet sent by a remote Data Terminal Equipment (DTE) device when it accepts a call from a unit on an X.25 network. See also *DTE*, *X.25*.

call-countdown timer—A value that specifies the maximum amount of time that a call can remain connected before the MultiVoice gateway disconnects the link. See also *call-disconnect warning timer*, *MultiVoice™*.

call detail reporting—See *CDR*.

call-disconnect warning timer—A value that specifies the amount of time that must elapse before the MultiVoice gateway plays a call-disconnect warning announcement for the caller. This warning announcement alerts the caller to the time remaining before the call is terminated. See also *call-countdown timer, MultiVoice™*.

called-number authentication—A form of authentication in which a TAOS unit uses the called-party number to authenticate the connection. The remote end uses this form of authentication to verify that the call goes to a known destination. When the profile requires called-number authentication, the number called must match a specified telephone number. The TAOS unit also uses the called number to direct incoming calls to a particular device. See also *called-party number*, *user profile*.

called-party number—An information element of the Q.931 ISDN signaling protocol. The called-party number is the telephone number the remote device calls to connect to the TAOS unit, but without a trunk group or dialing prefix specification. The called-party number is always available if specified in a profile. See also *called-number authentication, Q.931*.

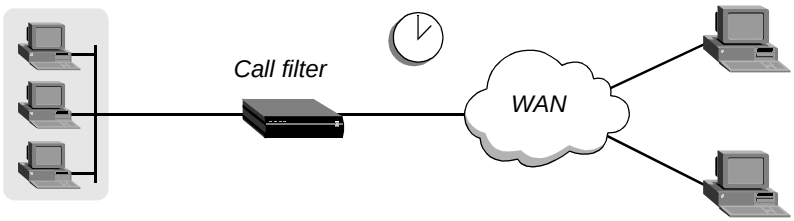
caller ID—See *CLID*.

Caller Identification—An ISDN telephone service that enables the called party's equipment to display the telephone number of the caller. See also *Caller Identification Restriction.*

Caller Identification Restriction—An ISDN telephone service that enables the caller to prevent his or her telephone number from being displayed to the called party. See also *Caller Identification*.

call filter—A packet filter that defines which packets can initiate a connection, or reset the idle timer for an established link (Figure 13). A call filter prevents unnecessary connections and helps a TAOS unit distinguish active traffic from "noise."

Figure 13. Call filters can prevent certain packets from resetting the timer.



By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection's idle timer. When a session's idle timer expires, the TAOS unit terminates the session.

When you apply a call filter, its forwarding action does not affect which packets are sent across an active connection. For a call filter to prevent an interface from remaining active unnecessarily, you must define rules for both incoming and outgoing packets. Otherwise, if only input rules are defined, outgoing packets keep a connection active. If only output rules are defined, incoming packets keep a connection active.

Compare with *data filter*. See also *input filter, output filter, packet filter*.

Calling-Line ID—See *CLID*.

Calling-Line ID authentication—See *CLID authentication*.

Calling-Line ID callback—See *CLID callback.*

Calling-Line ID substitution—See *CLID substitution*.

call logging—A method of logging call information from a TAOS unit. Call logging enables you to keep records for resource management or troubleshooting. When you set up call logging, you can create duplicate accounting information for sites that wish to keep accounting records separate from data about network operations. Call logging works only with NavisAccess™.

Call logging duplicates the RADIUS accounting stream. The call records are identical. The TAOS unit sends Start session, Stop session, and Failure-to-start session packets to a call-log host. When you turn on call logging and RADIUS accounting at the same time, the call-logging records are sent to NavisAccess, and the RADIUS accounting records are sent to a RADIUS server. The information is sent in parallel. You can use call logging with all versions of NavisAccess later than 4.0.

The call-logging feature permits NavisAccess to maintain information about the real-time state of the TAOS unit without having to perform an SNMP query for retrieving the information. In general, SNMP is not an optimal means for tracking the state of a Network Access Server (NAS) in real time. Because call-logging data is acknowledged, it is also much more reliable than SNMP.

Do not use call logging instead of RADIUS accounting. You can, however, use call logging as a backup to RADIUS accounting. See also *accounting*, *call-log host, Failure-to-start session, NAS, RADIUS, SNMP, Start session, Stop session*.

call-log host—A local host that supports the RADIUS accounting protocol and is configured to communicate with the TAOS unit. See also *accounting*, *call logging*.

call proceeding timer—In an Asynchronous Transfer Mode (ATM) configuration, a timer that starts when a Setup message is received. The call proceeding timer is also called the *T310 timer.* See also *ATM*.

call-progress tones—Dual-Tone Multifrequency (DTMF) tones that report call states. Ringback and busy signals are common call-progress tones.

call request—On an X.25 network, a request made by the calling party, asking the Data Terminal Equipment (DTE) to accept the call. See also *Call-Request packet, Call-Request timer, DTE, X.25*.

Call-Request packet—A packet sent by a device when it makes an outgoing call on an X.25 network. See also *call request, Call-Request timer, X.25*.

Call-Request timer—A value that specifies the number of 10-second ticks that a TAOS unit waits before clearing an outgoing call that the remote Data Terminal Equipment (DTE) has not accepted. When a device makes an outgoing call, it sends a Call-Request packet. If the remote DTE accepts the call, it sends back a Call-Connected Packet. If the DTE refuses the call, it sends back a Clear-Request packet. See also *Call-Connected packet, call request, Call-Request packet, Clear-Request packet, DTE, X.25*.

call routing—The process of routing incoming and outgoing calls to the proper modules on a TAOS unit.

When a TAOS unit receives a call on a WAN line, it performs Calling-Line ID (CLID) or called-number authentication (if appropriate), answers the call, and determines which slot should receive the call. It then finds the caller's profile, authenticates the call, builds a session, and passes the data stream to the appropriate module or host.

When a TAOS unit dials an outgoing call, it routes the call from the originating slot to a WAN channel. It first looks for channels associated with the trunk group specified by the dialed number (if any) and the port that originated the call. If no trunks have available channels, the TAOS unit does not place the call.

See also *called-number authentication*, *CLID authentication.*

Call Setup message—See *ISDN Call Setup message*.

call spanning—A method of enabling a Multilink PPP (MP) or Multilink Protocol Plus (MP+) call to span the TAOS units in the stack. Call spanning using a stack configuration can be effective when:

- A TAOS unit running MP+ is asked for another telephone number and has no available lines.
- A rotary hunt group uses the same telephone number to access multiple TAOS units, making it impossible to assume that a subsequent call is answered by the same TAOS unit.

Call spanning is protocol independent. See also *hunt group*, *MP*, *MP+*, *stack*.

Call User Data—See *CUD*.

CAP—Carrierless Amplitude Phase. CAP is a modulation method used with some DSL technologies. It uses both amplitude and phase to create signals for data transmission over twisted-pair lines. CAP stores different parts of a message in memory and then reassembles those parts in the modulated wave. CAP uses the frequency range from 4kHz to 1.1MHz. See also *DSL*, *RADSL*.

CAP—Competitive Access Provider. A CAP is a business that competes with the local telephone company in providing clients with access to services. For example, a cable company that offers high-speed data communications services is a CAP.

Carrier Detect—See *CD*.

Carrierless Amplitude Phase—See *CAP*.

Carrier Sense Multiple Access/Collision Detect—See *CSMA/CD*.

carrier services—Telecommunications services provided to the public for a fee (for example, ISDN lines and Frame Relay services).

CAS—(1) A carrier switch type in New Zealand. (2) Channel Associated Signaling. When you use CAS, the circuit state is indicated by one or more signaling bits sent in a repetitive manner.

cause code—A numerical diagnostic code sent from an ISDN switch to Data Terminal Equipment (DTE). A cause code indicates why call establishment failed, or why a call was terminated. The cause codes are part of ISDN D-channel signaling communications supported by the Signaling System 7 (SS7) supervisory network. When you dial a call from a TAOS unit with ISDN access, the TAOS unit reports the cause codes. When the TAOS unit clears the call, it reports a cause code, even when inband signaling is in use. A cause code is also called a *cause element.* See also *DTE*, *ISDN*, *SS7*.

cause element—See *cause code*.

Cause field—A field that indicates an event that triggered an X.25 Clear-Request, Reset-Request, or Restart-Request packet. Values for the Cause field can vary, depending on the packet type. See also *Clear-Request packet*, *Diagnostic field*, *Reset-Request packet*, *Restart-Request packet*, *X.25*.

CBCP callback—Callback Control Protocol callback. Microsoft's CBCP callback is a Link Control Protocol (LCP) option negotiated at the beginning of Point-to-Point Protocol (PPP) sessions. CBCP authenticates a caller by means of a username and password.

Microsoft developed CBCP callback to address a need for greater security when establishing PPP connections. The standard callback option defined in RFC 1570 has a potential security risk because the authentication is performed after the callback. CBCP callback, like Ascend callback, occurs after authentication, leaving no potential security hole. CBCP also offers features not available with standard callback. The client side supports a configurable time delay, enabling users to initialize modems or startup software before the TAOS unit calls the client. You can configure the TAOS unit with a telephone number to use for the callback, or you can allow the client to specify the telephone number.

Compare with *Ascend callback*, *CLID callback*, *DNIS callback.* See also *callback*, *LCP*, *PPP*.

C-bit Parity Errors—See *CPERR*.

CBR—Constant Bit Rate. CBR is a Quality of Service (QoS) class defined by the Asynchronous Transfer Mode (ATM) forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery of bits. Compare with *ABR*, *UBR*, *VBR-NRT*, *VBR-RT*. See also *ATM*, *QoS*.

CCITT—Consultative Committee on International Telegraphy and Telephony. The CCITT is a disbanded organization whose standards were moved to the UN-sanctioned International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) on March 1, 1993.

CCP—Compression Control Protocol. CCP enables both ends of a Point-to-Point Protocol (PPP) connection to negotiate whether to use data compression, and if so, which algorithm to use.

CD—Carrier Detect. CD is a signal sent from a modem to a host, indicating that the modem is online.

CDDI—Copper Distributed Data Interface. CDDI is the copper equivalent of FDDI. It is a network architecture that supports transmission rates of up to 100Mbps over Unshielded Twisted Pair (UTP) cable, with a maximum length of 100 meters. See also *FDDI*, *UTP cable*.

CDMA—Code Division Multiple Access. CDMA is a digital wireless transmission technique that uses mathematical codes, instead of frequencies or time slots, to transmit information. CDMA is a leading digital standard. See also *AMPS*, *CDPD*, *cellular communication*, *cellular modem*, *cellular network*, *wireless technology*.

CDPD—Cellular Digital Packet Data. CDPD is a digital wireless transmission technique that uses idle voice channels on the existing Advanced Mobile Phone Service (AMPS) cellular telephone network. CDPD transmits data packets at a raw data rate of 19.2Kbps, using channel hopping to move data packets through unused spaces across different frequencies. Because data is not as time-sensitive a service as voice, data can be fragmented and then reassembled at the receiving end. CDPD is particularly suited to sending small messages and transactions. It is not appropriate for transmitting multimegabit files. See also *AMPS*, *CDMA*, *cellular communication*, *cellular modem*, *cellular network*, *wireless technology*.

CDR—Call detail reporting. CDR is a feature that provides a database record of information about each call, including date, time, duration, called number, calling number, call direction, service type, and associated inverse-multiplexing session and port. Because the network carrier charges for bandwidth on an as-used basis, and bills each connection in an inverse-multiplexed call as a separate charge, you can use CDR to understand and manage bandwidth usage and the cost of each inverse-multiplexed session.

CDV—Cell Delay Variation. In an Asynchronous Transfer Mode (ATM) configuration, CDV is a routing metric that measures the average variation in delay between one cell and the next, expressed in fractions of a second. CDV measurements enable the network to determine whether cells are arriving too quickly or too slowly. See also *Admin Cost*, *ATM*, *End-to-End Delay*.

cell—In Asynchronous Transfer Mode (ATM), a 53-byte fixed-length data packet consisting of a 5-byte header and a 48-byte payload; in cellular communication, a portion of a city or county. In cellular communication, each cell contains the transmitters and receivers that provide the telephone service. The frequencies assigned to one cell are limited to the boundaries of that cell. When a cellular telephone moves from one cell toward another, a computer at the switch monitors the motion and hands off the telephone call to the new cell, which uses another radio frequency. The transfer is not noticeable to the user. See also *ATM*, *ATM cell*, *cellular modem*, *cellular network*.

Cell Delay Variation—See *CDV*.

Cell Loss Priority—See *CLP*.

cell relay—See *ATM*.

cell switching—In a cellular network, a feature that enables a caller to move from one location to another without losing the connection. The cellular system is designed to switch calls to a new cell without a noticeable drop in the connection. Although not noticeable in voice communications, the 300 milliseconds (ms) required for cell switching can cause problems in data transmission. Cell switching is sometimes referred to as *handing off*. See also *cellular communication*, *cellular network*.

Cell Transfer Delay—See *CTD*.

cellular communication—A type of wireless communication first available in 1981. To implement this technology, a carrier divides a city or county into units called *cells*. Each cell contains the transmitters and receivers that provide the telephone service. The frequencies assigned to one cell are limited to the boundaries of that cell. When a cellular telephone moves from one cell toward another, a computer at the switch monitors the motion and hands off the telephone call to the new cell, which uses another radio frequency. The transfer is not noticeable to the user. Compare with *landline telephone communication*. See also *CDMA*, *CDPD*, *cellular modem*, *cellular network*, *wireless technology*.

Cellular Digital Packet Data—See *CDPD*.

cellular modem—A modem that uses cellular technology to transmit data between remote locations. See also *CDMA*, *CDPD*, *cellular communication*, *cellular network*.

cellular network—A network that enables cellular subscribers to travel anywhere in the country and remain connected to the Public Switched Telephone Network (PSTN) by means of their mobile telephones. See also *CDMA*, *CDPD*, *cellular communication*, *cellular modem*.

Central Office—See *CO*.

Central Processing Unit—See *CPU*.

central site—A data-location point for telecommuters, branch offices, and remote users.

Centrex—Business telephone service that a Local Exchange Carrier (LEC) offers from a central office. Centrex services include call forwarding, call transfer, call restrictions, and call hold. Centrex service is an alternative to buying or leasing a Private Branch Exchange (PBX). See also *LEC*, *PBX*.

Challenge Handshake Authentication Protocol—See *CHAP*.

Change-Filter-Request packet—A request to change the packet filters for a routing session. See also *Change-Filter-Request-ACKed packet*, *Change-Filter-Request-NAKed packet*.

Change-Filter-Request-ACKed packet—A message a TAOS unit sends if it finds at least one routing session for which it could change packet filters. Compare with *Change-Filter-Request-NAKed packet*. See also *Change-Filter-Request packet*.

Change-Filter-Request-NAKed packet—A message a TAOS unit sends if it could not find a routing session for which it could change packet filters. Compare with *Change-Filter-Request-ACKed packet*. See also *Change-Filter-Request packet*.

channel—A portion of a line's bandwidth. A line contains a fixed number of channels. Each line can contain switched channels only, dedicated channels only, or a combination of switched and dedicated channels. See also *bandwidth*, *dedicated channel*, *line*, *switched channel*.

Channel Associated Signaling—See *CAS*.

channel bank—Equipment that converts multiple voice signals to Time Division Multiplexing (TDM) signals for transmission on a T1 or E1 line. A channel bank connects a T1 or E1 line to a PBX or a Central Office (CO) switch. The channel bank takes in the analog signals from the PBX and uses Pulse-Code Modulation (PCM) to convert the signals to digital. At the receiving end of the connection, the channel bank converts the digital signals back to analog. Using a channel bank enables an organization to use the T1/E1 circuit for voice, video, fax, and data.

Any digital PBX that terminates T1/E1 lines at a customer site is capable of terminating them directly without use of a channel bank. The CO portion of the T1/E1 circuit, however, still requires a channel bank, because telephone lines are primarily analog. See also *CO*, *D4-framed T1 line*, *ESF*, *G.703*, *PBX*, *TDM*.

channelized T1 PRI/E1 PRI—A T1 PRI or E1 PRI line divided into individual 64Kbps channels, or into channels whose data rate is a multiple of 64Kbps (for example, a 256Kbps channel made of four 64Kbps channels). Channelized T1 PRI or E1 PRI lines can be switched or dedicated. For example, a dedicated line can run from the Central Office (CO) to the corporate headquarters as a single, unchannelized T1 PRI line, and can then be divided into channels when it runs to remote sites from the corporate headquarters. Compare with *unchannelized T1 PRI/E1 PRI.* See also *dedicated line*, *E1 line*, *E1 PRI line*, *inband signaling*, *switched line*, *T1 line*, *T1 PRI line*.

Channel Service Unit—See *CSU*.

CHAP—Challenge Handshake Authentication Protocol. CHAP authentication verifies the caller's identity by using a three-way handshake upon initial link establishment, and then by repeating the handshake any number of times. In CHAP authentication, the authentication server sends a challenge to the caller. The caller responds with an MD5 digest calculated from the password. The authentication server then checks the digest against its own calculation of the expected hash value to authenticate the call. The server can send a new challenge at random intervals.

CHAP is a stronger authentication method than Password Authentication Protocol (PAP), because the password does not travel across the line as plain text. In addition, the use of repeated challenges limits the time of exposure to any single attempt to break the encryption code. The server is in control of how often it sends challenges.

Using bidirectional CHAP, you can enable the calling device and the called device to authenticate each other. See also *bidirectional CHAP*, *encryption*, *hash value*, *PAP*.

Char-to-Char timer—For an X.25/T3POS connection, a value that specifies the maximum amount of time permitted between characters sent from the Data Terminal Equipment (DTE) to the Packet Assembler/Disassembler (PAD). The Char-to-Char timer is also called the *T1 timer.* See also *DTE*, *PAD*, *X.25/T3POS*.

CHCS errors—Correctable Header Check Sequence errors. CHCS errors are Header Check sequence (HCS) errors that the unit can correct. Compare with *UCHCS errors*. See also *HCS*.

check item—A component of a RADIUS user profile that must be matched in an Access-Request packet for the access to succeed. See also *Access-Reject packet*, *RADIUS*, *reply item*.

Checkpoint packet—A RADIUS accounting (session-in-progress) packet that is identical to a Stop packet, except that Acct-Status-Type=3 (instead of 2) and the packet does not include the Ascend-Disconnect-Cause (195) attribute. See also *accounting*, *accounting checkpoint*, *Checkpoint record*.

Checkpoint record—A RADIUS accounting record that enables you to retrieve information about each user session in the event of network disruption. By default, RADIUS accounting logs a Start and Stop record for each user session. If a disruption in service causes a connection to fail before the TAOS unit receives a RADIUS Stop record, you can use the Checkpoint records to reconstruct usage.

In the RADIUS detail file, a Checkpoint record contains the same group of attributes as a RADIUS Stop record. However, the value for the Acct-Status-Type attribute in a Checkpoint record is the number 3. When queuing RADIUS accounting records, the TAOS unit prioritizes Start and Stop records ahead of Checkpoint records. See also *accounting*, *accounting checkpoint*, *Start record*, *Stop record*.

checksum—A count of the number of bits in a transmission unit. A checksum enables the receiving device to determine whether the same number of bits arrived as were sent. If the counts match, the receiver can assume that the transmission arrived intact. See also *CRC*.

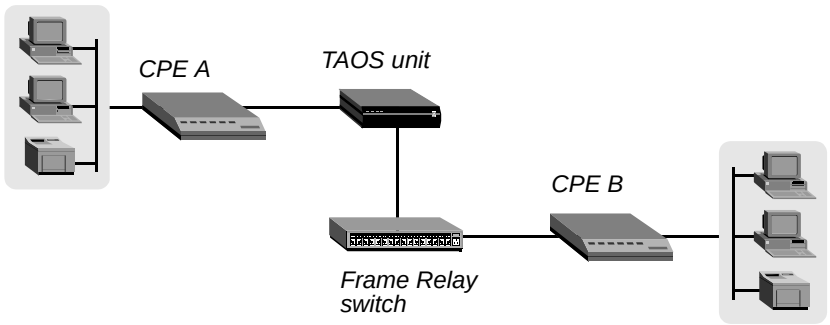
CIC—Circuit Identification Code. In a Signaling System 7 (SS7) network, the CIC specifies a port or time slot on a T1 or E1 interface. See also *SS7 network*.

CIR—Committed Information Rate. The rate (in bits per second) at which the network agrees to transfer information under normal conditions. The rate is averaged over the minimum increment of time specified by Tc. See also *Tc*.

circuit—A connection between end points over a physical medium.

circuit connection—A connection that follows a specified path through the Frame Relay switch. By linking two Data Link Connection Identifier (DLCI) end points, a TAOS unit creates a Permanent Virtual Circuit (PVC). The two DLCI end points act as a tunnel. Figure 14 illustrates a circuit connection.

Figure 14. Circuit connection



Data that the TAOS unit receives on one DLCI bypasses the router and goes out on the other DLCI. If any one of the DLCIs in a PVC becomes inactive because of a disconnect or failure, the PVC using that DLCI becomes inactive. A physical line can carry multiple DLCIs, and the failure of the line causes the failure of all the DLCIs it carries. Compare with *Frame Relay direct*. See also *DLCI*, *Frame Relay switch*, *PVC*, *router*.

Circuit Identification Code—See *CIC*.

circuit-level inverse multiplexing—A method of inverse multiplexing in which the inverse multiplexer slices the data stream into equal portions and transmits each portion over an available circuit. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. The AIM and BONDING protocols define how circuit-level inverse multiplexing works. Applications that require transparent digital circuits (for example, videoconferencing, dedicated backup and overflow, and bulk file transfer) use circuit-level multiplexing. Compare with *packet-level inverse multiplexing*. See also *AIM*, *BONDING*, *inverse multiplexer*, *inverse multiplexing*.

Circuit-Switched Cellular Data—See *CSCD*.

circuit-switched line—A temporary connection, like a telephone call. A temporary connection can be made to a variety of sites to handle occasional data-transfer needs or to provide additional bandwidth.

circuit-switched network—A type of network that uses a continuous link between a sender and a receiver. Voice and video applications use circuit switching to ensure that all the parts of a signal arrive in the proper order. Compare with *packet-switched network*.

Circuit-Switched Public Data Network—See CSPDN.

circuit switching—A mode of data transfer in which a dedicated connection is busy for the duration of the call. Compare with *packet switching*.

CIR Guaranteed Bandwidth TOS Routing—Committed Information Rate Guaranteed Bandwidth Type of Service Routing, an Open Shortest Path First (OSPF) feature. This type of routing guarantees that if multiple paths have sufficient bandwidth to meet CIR requirements to the destination, the system chooses the path with the lowest administrative cost. If multiple paths exist with sufficient available bandwidth and the same administrative cost, the system chooses the path with the largest available bandwidth. If no path to the destination has sufficient available bandwidth, the system reestablishes the circuit, using the path with the lowest administrative cost. See also *CIR*, *OSPF*.

Clear-Confirmation packet—On an X.25 network, a packet that the Data Terminal Equipment (DTE) or Data Circuit-terminating Equipment (DCE) device receives in response to its request to clear a call. When the device receives a Clear-Confirmation packet from the remote end, the call is cleared and the logical channel is available for other calls. See also *Clear-Indication packet*, *Clear-Request packet*, *DCE*, *DTE*, *X.25*.

Clear-Indication packet—On an X.25 network, a packet that the Data Circuit-terminating Equipment (DCE) sends when it refuses an incoming call or when it clears a call upon completion of the data exchange. See also *Clear-Confirmation packet*, *Clear-Request packet*, *DCE*, *X.25*.

Clear-Request packet—On an X.25 network, a packet that the Data Terminal Equipment (DTE) device sends when it refuses an incoming call or when it clears a call upon completion of the data exchange. See also *Clear-Confirmation packet*, *Clear-Indication packet*, *DTE*, *X.25*.

Clear-Request retries—The number of times a TAOS unit sends a Clear-Request packet on an X.25 network before waiting indefinitely for a response. See also *Clear-Request packet, X.25*.

Clear-Request timer—A value that specifies the number of 10-second ticks that a TAOS unit waits before retransmitting a Clear-Request packet. See also *Clear-Request packet*, *X.25*.

Clear To Send—See *CTS*.

CLEC—Competitive Local Exchange Carrier. A CLEC is a company that competes with the established local telephone company by providing its own network and switching services. See also *LEC*.

CLID—Calling-Line ID. The CLID is the telephone number of a calling device that attempts to connect to a TAOS unit. The telephone company provides the telephone number. A CLID is also known as a *caller ID*. See also *CLID authentication*.

CLID authentication—Calling-Line ID authentication. CLID authentication is a method a TAOS unit uses to authenticate incoming calls by checking the calling party's telephone number (as received from the telephone company). The CLID is the telephone number of the calling device. A TAOS unit performs CLID authentication before enabling itself to answer an incoming call. When a profile requires CLID authentication, the caller's telephone number must match a specified telephone number. You can thereby ensure that the call comes from a known source.

You can use CLID authentication only when the call information is available end-to-end and Automatic Number Identification (ANI) applies to the call. In some areas, the WAN provider might not be able to deliver CLIDs, or a caller might keep a CLID private. Typically, a site uses CLID authentication to protect against a situation in which an unauthorized user obtains the name, password, and IP address of an authorized user and then calls the TAOS unit from another location.

See also *CLID*, *RADIUS*, *user profile.*

CLID callback—Calling-Line ID callback. CLID callback is the method by which a TAOS unit uses the CLID information element to detect callback during the ringing state of an incoming call. The TAOS unit does not answer the call (go off hook), and the originating caller is not charged for the call. Compare with *Ascend callback*, *CBCP callback*, *DNIS callback*. See also *callback*.

CLID substitution—Calling-Line ID substitution. CLID substitution occurs when a MultiVoice gateway connects a Voice over IP (VoIP) call and transmits a CLID generated by the MultiVoice Access Manager (MVAM) software on the gatekeeper instead of the PSTN-generated CLID collected on the trunk line. When MVAM receives the CLID from a gateway, it translates the CLID to the appropriate dial string, adding or removing country codes and area codes as appropriate. The gatekeeper then reports the revised CLID to both gateways as part of the Admission Confirmation (ACF) message.

CLID substitution enables the MultiVoice network to provide the appropriate E.164 addresses for the called and calling telephone numbers to the appropriate Public Switched Telephone Networks (PSTNs). When the gateways connecting the call reside in different area codes or countries, the CLID received from the PSTN must be changed to provide the appropriate calling number information to the local carrier, to call management applications, and to billing software. See also *CLID, MultiVoice™, MVAM, PSTN, VoIP*.

client—A user or device that requires services from another unit or program. For example, a user requesting access is a client of the TAOS unit, and a TAOS unit making a RADIUS authentication request is a client of the RADIUS server. See also *RADIUS server*.

client DNS—A configuration that enables a TAOS unit to direct incoming connections to a Domain Name System (DNS) server belonging to a particular client or location, thereby preventing WAN users access to a local DNS server. Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration. The addresses configured for client DNS servers are presented to WAN connections during IPCP negotiation. You can also choose to present your local DNS servers in the event that no client servers are defined or available. See also *DNS*, *IPCP*.

CLNP—Connectionless Network Protocol. CLNP is the Open Systems Interconnection (OSI) protocol for datagram service. It is the OSI equivalent of the Internet Protocol (IP). See also *IP*, *SDTN*.

clock—A timing mechanism for synchronizing data communication and processing tasks. A clock divides time into very short intervals. See also *clock speed*.

clock speed—The number of intervals per second that a clock uses for synchronizing data communication and processing. See also *clock*.

Closed User Group—See *CUG*.

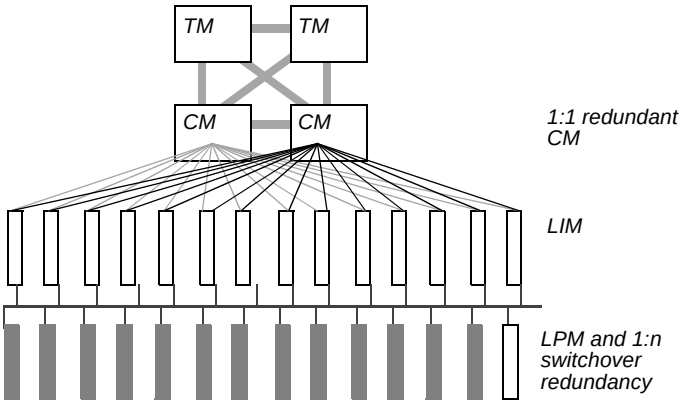
CLP—Cell Loss Priority. A field in an Asynchronous Transfer Mode (ATM) cell header, CLP indicates the eligibility of the cell for discard under congested conditions. See also *ATM, congestion, GFC, HEC, Payload, PT, VCI, See also ATM, VPI, VPL.*.

CLT module—Copper Loop Test module. A Stinger module that consists of an integrated test head installed on a Path Selector Module (PSM). The test head is used to perform a full suite of technical tests on copper loops associated with Digital Subscriber Line (DSL) connections. A CLT module can also be used as a PSM to support Line Interface Module (LIM) and LIM port redundancy. See also *DSL*, *LIM*, *PSM*.

CM—Control Module. Each CM is a Stinger controller designed for functional redundancy. Although the unit can operate with a single CM, redundant operation is recommended. When two CMs are installed and the system is powered on, the unit elects one of the modules as the *primary CM*. The other becomes the *secondary CM*. As soon as the election process is complete, the status lights (LEDs) on the CM front panel indicate which of the modules is primary.

The primary and secondary CMs monitor each other, using a heartbeat protocol, and maintain synchronized repositories of the system configuration stored in the primary CM's flash memory. If the primary CM resets, the system switches over to the secondary CM. The mechanism for switchover is built into the CM hardware, and allows switchover to occur instantaneously. To maintain full functional redundancy, the primary and secondary CMs have separate paths to each Line Interface Module (LIM) and Trunk Module (TM), as shown in Figure 15.

Figure 15. Redundant paths from each CM



The primary CM manages the LIMs, and assumes all the normal controller responsibilities of managing the unit, including the call-control and circuit-management functions. In the event of a switchover, the LIMs are not hardware reset (avoiding the need to retrain the DSL modems). However, all connections are dropped. Connections are subsequently rebuilt after the new primary CM completes its initialization. Log messages notify the user of the following significant events related to CM redundancy:

- The CM has become primary.
- The CM has become primary and no secondary CM is present.
- The primary CM has lost heartbeat communication with the secondary CM.
- The primary CM has established heartbeat communication with the secondary CM.
- The CM has experienced a software crash.

All configuration must take place on the primary CM. The primary CM configuration repository regularly overwrites that of the secondary CM. In addition, the primary CM always overwrites the secondary CM's repository immediately following a configuration change. See also *LIM*, *Stinger™*, *TM*.

CMF-R2—Compelled Multiple Frequency R2. A type of signaling in which an R2 tone is sent until a reply tone is received, however long that process takes.

CO—Central Office. The CO is the telephone switching office to which a customer directly connects. It links the customer to other portions of the telephone network.

coaxial cable—A data-transmission cable consisting of a braided outer shield surrounding an insulated core.

codec—COder/DECoder. A codec is a device that encodes analog video or voice data into a digital signal for transmission over a digital medium. Codecs are often used for videoconferencing. See also *analog data*, *audio codec*, *digital signal*.

Code Division Multiple Access—See *CDMA*.

coldboot—A reboot that enables the user to restart the switch as if it were powered off and then on again. Compare with *warmboot*.

coldstart—The process by which a TAOS unit reinitializes itself in a way that might alter the configuration of the SNMP manager or the system. Compare with *warmstart*.

coldstart notification—In a RADIUS accounting Stop record, a value that informs the accounting server that the TAOS unit has started up. See also *accounting*, *accounting server*, *Stop record*.

collision detection—See *CSMA/CD*.

command mode—A terminal-server mode in which you can enter commands at the terminal-server prompt. Compare with *immediate mode*, *menu mode*.

comment line—A line, in a RADIUS user profile or pseudo-user profile, that describes the purpose of one or more lines of the profile. Beginning with the # character at column one, the comment line consists of text that extends to the end of the line. You can embed a comment line anywhere in a profile. See also *pseudo-user profile*, *user profile*.

Committed Burst Size—See *Bc*.

Committed Information Rate—See *CIR*.

Committed Rate Measurement Interval—See *Tc*.

Common Part—See *CP*.

community name—A password that a TAOS unit sends to the Simple Network Management Protocol (SNMP) manager when an SNMP trap event occurs, and that the manager sends to the TAOS unit with each polling request. The password authenticates the sender. The default is `public`. See also *agent*, *manager*, *SNMP*.

Compelled Multiple Frequency R2—See *CMF-R2*.

Competitive Access Provider—See *CAP*.

Competitive Local Exchange Carrier—See *CLEC*.

Compressed Serial Line Internet Protocol—See *CSLIP*.

compression—A process that reduces the quantity of bandwidth or storage space required to encode a block of information. See also *VJ compression*.

communications protocol—A standard method of communicating between networked devices. A hardware interface standard (for example, RS-232C). See also *protocol*.

concentrator—A repeater or hub that joins communications channels from several network nodes and provides bridging, routing, and management functions. See also *hub*, *repeater*.

congestion—The point at which a network device is operating at its highest degree of utilization. See also *absolute congestion*, *congestion avoidance*, *congestion management*, *mild congestion*, *severe congestion*.

congestion avoidance—A method of notifying the edge nodes of congestion in a Frame Relay network. The header of each frame includes a field for the Forward Explicit Congestion Notification (FECN) bit and the Backward Explicit Congestion Notification (BECN) bit. FECN informs the destination device of congestion for destination-controlled protocol suites. BECN informs the source device of congestion for source-controlled protocol suites.

FECN and BECN bits indicate the existence of network congestion to the higher-layer protocols. The system can then reduce the rate of information flow into the network until the congestion clears. However, many Frame Relay CPE devices cannot use this information. Both the FECN and BECN bits are set by the network, not by the user. Therefore, end-point nodes are not required to do anything about them. The FECN and BECN bits are often ignored, or are simply counted by internetworking devices, such as routers, to provide an indication of congestion in the network.

See also *congestion*, *congestion management.*

congestion management—A method for monitoring congestion on a Frame Relay network. As data travels through the Frame Relay network and is queued for transmission, the state of each queue is checked for pending congestion. Each switch executes a time-average algorithm, Average Queue Length (AQL), each time it queues a frame for transmission. It then compares the AQL value to a precalculated threshold. When the AQL is less than or equal to the lowest threshold, maximum throughput and minimum delay occur.

The switch uses three thresholds to determine congestion:

- Mild congestion
- Severe congestion
- Absolute congestion

If the AQL exceeds the threshold for mild congestion but is less than the threshold for severe congestion, the link is considered *mildly congested*. If the AQL exceeds the threshold for severe congestion but is less than the threshold for absolute congestion, the link is considered *severely congested*. If the AQL exceeds the threshold for absolute congestion, the link is considered *absolutely congested*. When the link is in this state, there is no room in the queue for any packets. See also *absolute congestion*, *congestion*, *congestion avoidance*, *mild congestion*, *severe congestion*.

Connection Admission Control—See *CAC*.

connectivity—The degree to which a given computer or application can interoperate with other network components.

connect request timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum number of seconds that can elapse between the transmission of a Connect message and the receipt of a Connect Acknowledge message. The connect request timer is also known as the *T313* timer. Compare with *restart request timer*. See also *ATM*.

Constant Bit Rate—See *CBR*.

Consultative Committee on International Telegraphy and Telephony—See *CCITT*.

continuity test—In a Signaling System 7 (SS7) network, a test to verify that the physical link between the Central Office (CO) switch and the TAOS unit is available. The CO switch informs the signaling gateway, which then informs the TAOS unit that it will conduct a continuity test on the circuit. During a call continuity test, the CO switch sends a tone through the physical path to the TAOS unit and receives back from the TAOS unit a tone indicating the continuity of the path. The TAOS unit supports a 4-wire-only continuity test (as defined in Q.724 Sections 7 and 8, ANSI T1.113.4 Annex B, GR-246-CORE Annex B), a 2-wire continuity test (as defined in GR-246-CORE Section B.2), and 4-wire-to-2-wire emulation (as defined in GR-246-CORE Section B.3). See also *2-wire continuity test*, *4-wire continuity test*, *4-wire-to-2-wire continuity test*, *CO*, *signaling gateway*, *SS7 network*.

Control frame—In an X.25/T3POS network, a supervisory frame of the following format:

`SOH MSS CUD STX [`*`data`*`] ETX XRC`

where:

- `SOH` is the ASCII character \001.
- `MSS` is the Mode Selection Signal, which can be used to indicate the call mode.
- `CUD` is the Call User Data, which can contain an X.121 address in addition to user facilities, or can contain call-user data in an X.28 format.
- *`data`* is optional in the control frame. In Transparent and Blind modes, the T3POS PAD is restricted to passing data frames between the T3POS Data Terminal Equipment (DTE) and the T3POS host.
- `ETX` is the ASCII character \003.
- `XRC` is the checksum. For all modes except Binary Local, the checksum is a one-character Longitudinal Redundancy Check (LRC) checksum. For Binary Local mode, the checksum is a two-character Cyclic Redundancy Check (CRC) checksum.

Control frames are in use only when a call is being established, not during data transfer. See also *Binary Local mode*, *Blind mode*, *CRC*, *DTE*, *Local mode*, *LRC*, *Transparent mode*, *X.25/T3POS*.

control-lead signaling—A method of toggling one or more leads within a cable in order to initiate a dialed call.

control-line state—A state that results when a device sends a signal through a pin and over the line to another device. The signal being sent determines the control-line state. For example, a device can send a signal to inform another party that it is ready to receive data. In this case, the control-line state is Data Transmit Ready (DTR). The process of sending control signals is called *handshaking*. See also *DTR*, *handshaking*.

Control Module—See *CM*.

convergence—The time it takes all routers to receive information about a change to the network topology. Slow convergence can result in routing loops and errors. A Routing Information Protocol (RIP) router broadcasts its entire routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In contrast, Open Shortest Path First (OSPF) uses a link-state database of the network, and propagates only changes to the database, resulting in faster convergence. See also *link-state database*, *OSPF*, *RIP*.

Convergence Sublayer—See *CS*.

Coordinated Universal Time—See *UTC*.

Copper Distributed Data Interface—See *CDDI*.

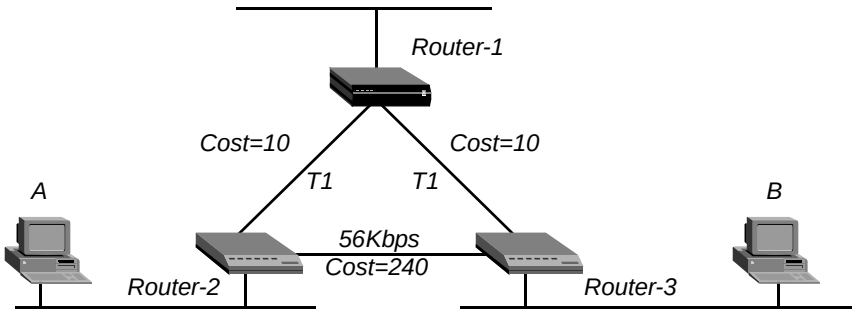
Copper Loop Test module—See *CLT module*.

Correctable Header Check Sequence errors—See *CHCS errors*.

cost—An Open Shortest Path First (OSPF) value you assign to the output side of each router interface. The cost indicates the likelihood that the TAOS unit will use the interface to transmit data. The lower the cost, the more likely is the TAOS unit to use the interface.

Figure 16 shows how costs are used to direct traffic over high-speed links. For example, if Router-2 in Figure 16 receives packets destined for Host B, it will route them through Router-1 across two T1 links (Cost=20), rather than across one 56Kbps B channel to Router-3 (Cost=240).

Figure 16. OSPF costs for different types of links



You can use the cost value to perform preferred path selection. If two paths to a destination have equal costs, you can assign a higher cost to one of the paths, making it a backup when the primary path is not available. In addition, you might want to reflect the bandwidth of a connection when assigning costs. As in Figure 16, the cost of a single B-channel connection could be 24 times greater than the cost of a T1 link.

A TAOS unit has a default cost of 1 for a connected route (Ethernet) and 10 for a WAN link. Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network. See also *OSPF*, *route*, *router*.

coverage area—A group of telephone numbers that the system can use to dial and receive calls through a particular MultiVoice gateway. You define coverage areas for each MultiVoice gateway by assigning dial strings to a database on the gatekeeper. A dial string can be a country code, an area code, a country code/area code combination, an area code/exchange combination, or a complete telephone number. See also *gatekeeper*, *gateway*, *inclusion area*, *MultiVoice™*.

CP—Common Part. The CP is the portion of the Signaling ATM Adaptation Layer (SAAL) that represents the functionality common to all users requiring a connection-oriented, variable bit-rate information transfer. It provides unguaranteed information transfer but includes a mechanism for detecting corruption of information carried in the SAAL frames. Compare with *SSP*. See also *SAAL*.

CPE—Customer Premises Equipment. CPE is equipment connected to the telephone network and located at the customer's site. The equipment can be owned or leased.

CPERR—C-bit Parity Errors. CPERR indicates the number of times that the C-bit parity check failed on the DS3 line. Compare with *FERR*, *PERR*. See also *DS3 line*.

CPU—Central Processing Unit. The CPU is the computer's main processor.

crankback—In a Private Network-to-Network Interface (PNNI) configuration, the ability to reroute a call on an alternative path in case of failure. See also *PNNI*.

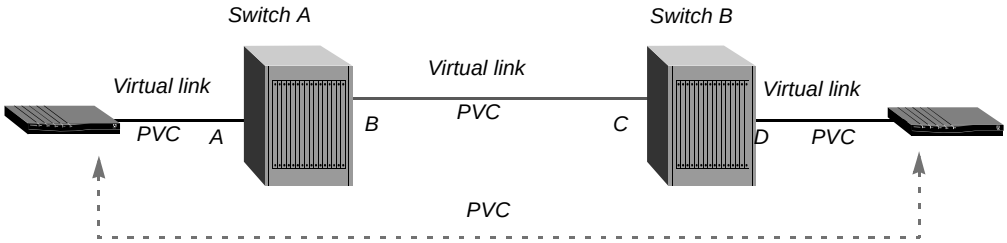
CRC—Cyclic Redundancy Check. CRC is an error-detection method that uses a mathematical divisor to check the integrity of the data in a transmitted packet. See also *checksum*, *CRC error*.

CRC-4—Cyclic Redundancy Check 4. A four-bit error-checking technique that calculates a numeric value to check the integrity of transmitted data and to detect errors in the data stream.

CRC error—Cyclic Redundancy Check error. A CRC error is a condition that occurs when the CRC in a frame does not match the CRC received from the network. See also *CRC*.

cross-connect—An Asynchronous Transfer Mode (ATM) function that enables each switch along the path of an end-to-end Permanent Virtual Circuit (PVC) to receive the cell stream on one interface and transmit it on another. Figure 17 shows an end-to-end PVC connection across two switches. Switch A has an ATM circuit configuration between its interfaces, labeled A and B, cross-connecting two virtual links. Switch B has a similar ATM circuit configuration between its interfaces, labeled C and D.

Figure 17. End-to-end PVC cross-connected in each switch



See also *ATM*, *ATM circuit*, *PVC*.

crossover cable—A cable with wires that cross over so that the terminating ends of the cable have opposite wire assignments. A crossover cable is sometimes referred to as a *null modem*. Compare with *straight-through cable*.

CS—Convergence Sublayer. CS is a sublayer of ATM Adaptation Layer (AAL). Its primary purpose is to convert data and protocols between Asynchronous Transfer Mode (ATM) formats and non-ATM formats. See also *AAL*, *ATM*.

CSCD—Circuit-Switched Cellular Data. CSCD is a wireless transmission technology that supports sending large files and faxes. CSCD uses switches to set up connections in analog cellular networks, and is also used in conjunction with such digital packet technologies as Cellular Digital Packet Data (CDPD). See also *CDPD*, *cellular communication*, *wireless technology*.

CSLIP—Compressed Serial Line Internet Protocol. CSLIP is a form of the Serial Line Internet Protocol (SLIP). Both SLIP and CSLIP enable you to transmit IP packets over serial connections, but CSLIP uses a compressed packet header and involves less overhead than SLIP. See also *SLIP*.

CSMA/CD—Carrier Sense Multiple Access/Collision Detect. CSMA/CD is a media-access mechanism in which a device ready to transmit data checks the channel for the presence of a carrier. If it does not sense a carrier for a specific period of time, the device can transmit its data. If two devices transmit at the same time, a collision occurs and all transmitting devices detect it. The collision delays retransmissions from the devices for random lengths of time. Ethernet and IEEE 802.3 use CSMA/CD. See also *802.3*, *Ethernet*.

CSPDN—Circuit-Switched Public Data Network. A CSPDN is a communications network that uses circuit-switched digital data circuits and is available to the public. See also *circuit switching*, *digital signal*.

CSU—Channel Service Unit. Along with a Data Service Unit (DSU), a CSU is a component of Data Circuit-terminating Equipment (DCE). A CSU connects a digital telephone line to a customer's network-access equipment. It can be built into the network interface of the network-access equipment, or it can be a separate device. The CSU terminates the connection at the user's end and processes digital signals. It also prevents a faulty DSU from interfering with data transmissions on the digital line.

On a Frame Relay circuit, the CSU converts the signals between the V.35 interface on Data Terminal Equipment (DTE) and the T1 or E1 interfaces on a Frame Relay switch.

See also *DCE*, *digital signal*, *DSU*.

CTD—Cell Transfer Delay. The elapsed time between a cell exit event at the source and the corresponding cell entry event at the destination for a particular Asynchronous Transfer Mode (ATM) connection. See also *ATM*.

CTS—Clear To Send. CTS is a signal sent from a receiving device to a transmitting device, indicating that the transmitter can begin sending data. A CTS signal is generally a response to a transmitter's Request To Send (RTS) signal. See also *RTS*.

CUD—Call User Data. The CUD field in a Control frame identifies the encapsulation in use over an X.25 Virtual Circuit (VC). See also *encapsulation*, *VC*, *X.25*.

CUG—Closed User Group. A CUG is a calling group to which access is restricted. A user can be a member of more than one CUG. In general, members of a specific CUG can communicate among themselves, but not with users outside the group. In some cases, however, specific CUG members can originate calls to destinations outside the group, or receive calls from outside the group. The Network Service Provider (NSP) can determine the maximum number of CUGs a user can belong to. See also *CUG index*, *NSP*.

CUG index—Closed User Group index. On an X.25/PAD call, the CUG index indicates to the called switch the CUG selected for a virtual call. See also *CUG*, *X.25/PAD*.

Custom AESA format—Custom ATM End System Address format. The Custom AESA format uses the Custom Authority and Format Identifier (AFI) and byte order. Compare with *DCC AESA format*, *E.164 AESA format*, *ICD AESA format*. See also *AESA format*, *AFI*.

Customer Premises Equipment—See *CPE*.

Cyclic Redundancy Check—See *CRC*.

Cyclic Redundancy Check 4—See *CRC-4*.

D

D4-framed T1 line—A T1 line that uses the D4 format, also known as the *Superframe format*, to frame data at the physical layer. The D4 format consists of 12 consecutive frames, each one delimited by framing bits. T1 lines that do not use ISDN D-channel signaling use the D4 format. See also *T1 line*.

DAC—Digital Access Cross-Connect. A DAC is a device used to split and switch channels between incoming and outgoing circuits. This capability, referred to as *fanout*, provides for distribution of these channels to accommodate changes in traffic patterns and site relocations. In some cases, a DAC reallocates channels to support peak traffic overflow and provide redundancy in fault-tolerant configurations. See also *drop-and-insert multiplexer*.

D-A conversion—Digital-to-Analog conversion. D-A conversion is a process in which a digital signal is modified into an analog signal. D-A conversion takes place, for example, when digital data reaches an analog modem. Compare with *A-D conversion*. See also *analog signal*, *digital signal*, *modem.*

daemon—A type of program that, once activated, carries out a specific task without user intervention. A daemon typically handles a task that runs repeatedly (for example, a printing, mail, or communications service). See also *RADIPAD*, *RADIUS*.

DARPANet—A network created in 1969 by the Defense Advanced Research Projects Agency (DARPA). The DARPANet provided an efficient way to exchange military information between scientists in various locations. Originally consisting of a 4-computer network, the DARPANet expanded into a network of 37 computers and was later renamed ARPANet. ARPANet was the precursor of the present-day Internet. See also *Internet.*

DASS-2—A signaling protocol used by British Telecom on ISDN links. DASS-2 specifies the signaling that occurs on the D channel. Although DASS-2 is widely available, many new installations use Q.931. See also *Q.931*.

Database-Description packet—A Type-2 Open Shortest Path First (OSPF) packet. OSPF routers exchange Database-Description packets when an adjacency is being initialized. Each packet describes the contents of the link-state database. The routers use a poll-response procedure. One of the routers is the master, and the other a slave. The master sends Database-Description poll packets, and the slave sends Database-Description response packets. OSPF links the responses to the polls by means of a sequence number in each packet. See also *adjacency*, *link-state database*, *OSPF*.

data bits—In asynchronous transmission, the bits that contain the data being sent. Data bits are sometimes referred to as a *payload*. See also *asynchronous transmission*.

Data Carrier Detect—See *DCD.*

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

data compression—A method for current modem standards and protocols to attain higher rates of speed. Compression algorithms, such as those in the V.42bis standard, take advantage of redundancies in data files by substituting a few characters for many. Compression is especially effective with text files and certain graphic-file formats, and has become an important topic as multimedia, video, document imaging, and other technologies emerge.

Data Country Code—See *DCC*.

Data Country Code ATM End System Address format—See *DCC AESA format*.

Data Delivery Layer—See *DDL*.

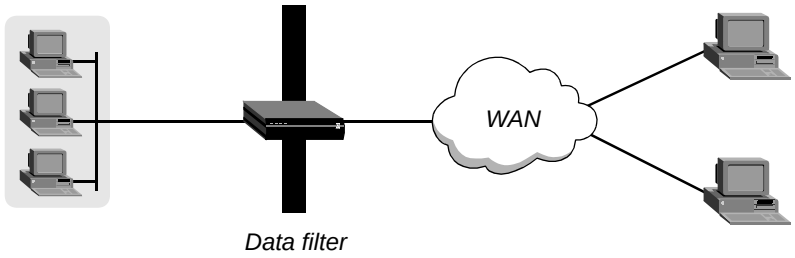
Data Encryption Standard—See *DES*.

Data Encryption Standard-Cypher Block Chaining—See *DES-CBC*.

Data Exchange Interface—See *DXI*.

data filter—A packet filter that defines which packets a TAOS unit can transmit on a connection. When you apply a data filter, its forward or drop action affects the actual data stream by preventing certain packets from reaching the Ethernet network from the WAN, or vice versa (Figure 18).

Figure 18. Data filters can drop or forward certain packets.



Many sites apply data filters for security purposes, but you can apply them for any purpose that requires the TAOS unit to drop or forward only specific packets. For example, you can use data filters to drop packets addressed to particular hosts, to prevent broadcasts from going across the WAN, or to allow users to access only specific devices across the WAN. Compare with *call filter*. See also *packet filter*.

data frame—See *general frame*.

datagram—A message unit that contains a source address, destination address, and data. A datagram is routed through a packet-switched network. See also *packet-switched network.*

Datagram Delivery Protocol—See *DDP*.

data link—The link interface to a Frame Relay device. The data link refers to specific dedicated bandwidth on the TAOS unit and defines the operations and link-management functions that the TAOS unit performs on the interface. See also *Frame Relay*, *Frame Relay network.*

Data Link Connection Identifier—See *DLCI*.

Data Link layer—The second layer of the OSI Reference Model. The Data Link layer creates, sends, and receives data packets appropriate for the type of network in use. Data-Link-layer protocols include High-Level Data Link Control (HDLC), Link Access Procedure, Balanced (LAPB), Link Access Procedure, D channel (LAPD), Point-to-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP). See also *HDLC*, *LAPD*, *OSI Reference Model*, *PPP*, *SLIP*.

Data Over Subscriber Bearer Service—See *3.1kHz audio-bearer service*.

data-over-voice—A method of sending digital data over telephone trunks by means of either voice-bearer service or 3.1kHz audio-bearer service. See also *3.1kHz audio-bearer service*.

Data Over Voice Bearer Service—See *3.1kHz audio-bearer service*.

data packet—See *packet*.

data rate—The transmission speed of data over a line, generally expressed as thousands of bits per second (Kbps).

data service—A service provided over a WAN line and characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice. The following types of data services are available:

- Switched-56
- Switched-64
- Switched-384 (also known as *H0*)
- Switched-1536 (also known as *H11*)
- MultiRate
- GloBanD

See also *GloBanD*, *MultiRate*, *Switched-56*, *Switched-64*, *Switched-384*, *Switched-1536*.

Data Service Unit—See *DSU*.

Data Set Ready—See *DSR*.

Data Terminal Equipment—See *DTE*.

data-transfer mode—For an X.25/T3POS connection, the method used for error recovery and data transmission. A TAOS unit enables you to specify Local, Transparent, Blind, or Binary Local. See also *Binary Local mode*, *Blind mode*, *Local mode*, *Transparent mode*.

data transfer rate—The speed at which data is transferred, usually measured in megabits per second (Mbps).

Data Transmit Ready—See *DTR*.

DB-9—A 9-pin serial port. See also *DB connector*.

DB-25 pin connector—A 25-pin connector on which the RS-232C standard is based. Ten connections are commonly used. On a standard DB-25 pin connector, the pin designations and names of the signals are:

Pin	Signal
1	Protective (frame) ground
2	Transmit Data (TD)
3	Receive Data (RD)
4	Request To Send (RTS)
5	Clear To Send (CTS)
6	Data Set Ready (DSR)
7	Signal Ground (SG)
8	Carrier Detect (CD)
20	Data Terminal Ready (DTR)
22	Ring Indicator (RI)

See also *CD*, *CTS*, *DSR*, *DTR*, *protective ground*, *RD*, *RI*, *RS-232C*, *RTS*, *SG*, *TD*.

DBA—Dynamic Bandwidth Allocation. DBA denotes the process of adding or subtracting bandwidth from a switched connection in real time without terminating the link. Multilink Protocol Plus (MP+) supports DBA governed by a set of parameters you specify. To add bandwidth, the TAOS unit dials additional connections.

The TAOS unit can reject a request to add bandwidth if no more channels are available or if the network is congested. Under either of these conditions, the two ends enter bandwidth-addition-lockout mode, in which neither side can request bandwidth. The lockout prevents both ends from continually trying to add new channels unsuccessfully. Both ends automatically remove the lockout restriction when the conditions that caused the lockout change. When the lockout ends, each end is free to add bandwidth.

If you use a circuit between two locations to capacity 24 hours per day, using a dedicated line is more cost-effective than using a switched line. However, if you need the circuit only sporadically, or if the circuit is sometimes underutilized, it often makes more sense to lease a smaller amount of dedicated bandwidth and then supplement it with additional switched bandwidth as traffic requirements dictate.

For example, you might establish some connections only when you need to transfer data, and a single circuit can accommodate low traffic levels. However, if traffic levels grow beyond the capacity of the circuit (such as during a large file transfer), DBA automatically adds additional switched channels. When traffic levels subside, DBA automatically removes the channels from the connection. The bandwidth and connection costs are thereby reduced. You pay for bandwidth only when you need it. See also *bandwidth*, *circuit*, *dedicated line*, *MP+*, *switched line*.

DB connector—Data bus connector. A DB connector is a cable connector for parallel or serial ports. The number following *DB* indicates the number of pins on the connector. For example, a DB-25 connector has 25 pins. See also *DB-9*, *DB-25 pin connector*.

DCA—Defense Communication Agency. The DCA is an agency responsible for installing the Defense Data Network.

DCC—Data Country Code. The DCC is a 2-byte portion of an ATM End System Address (AESA) and identifies the country in which the address is registered. Country codes are standardized and defined in ISO Reference 3166. See also *AESA format*.

DCC AESA format—Data Country Code ATM End System Address format. In DCC AESA format, the DCC is specified in the address, identifying the country in which the address is registered. Compare with *Custom AESA format*, *E.164 AESA format*, *ICD AESA format*. See also *AESA format*.

DCD—Data Carrier Detect. DCD is a hardware signal defined by the RS-232C standard. It indicates that the device is online and ready to receive a transmission.

DCE—Data Circuit-terminating Equipment (also known as *Data Communications Equipment*). A DCE device connects Data Terminal Equipment (DTE) to a communications channel, such as a telephone line. *DTE* refers to a device that an operator uses (for example, a computer or a terminal). A DCE device converts the format of the data coming from the DTE into a signal suitable to the communications channel. An example of a DCE device is a modem, which converts digital data from a computer to analog signals suitable for sending over a telephone line. See also *analog signal*, *digital data*, *DTE*, *modem.*

DCE interface—An interface that provides AIM/BONDING inverse multiplexing services to a device connected to it.

DCF message—Disengage Confirmation message. An H.323 Registration, Admission, and Status (RAS) message sent by the MultiVoice Access Manager (MVAM) device to a MultiVoice gateway in response to a Disengage Request (DRQ) message. Compare with *ACF message*. See also *DRQ message*, *H.323*, *MultiVoice™*, *MVAM*, *RAS*.

D channel—A channel that carries WAN synchronization and signaling information on a T1 PRI or E1 PRI line. See also *E1 PRI line*, *T1 PRI line*.

DCS 1800—Digital Cellular System working at 1800 MHz. DCS 1800 is a European mobile-telephone service based on European Telecommunications Standards Institute (ETSI) standards. See also *ETSI*.

DCS 1900—See *GSM 1900*.

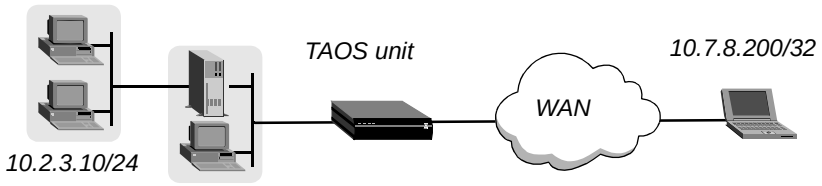
DDL—Data Delivery Layer. In a Signaling System 7 (SS7) configuration, the DDL uses a TCP/IP socket on both the signaling gateway and the TAOS unit. On the signaling gateway side, the DDL is the server that listens for the socket connection and keeps track of the mapping between a TAOS unit and its socket. On the TAOS unit side, the DDL is the client that initiates a socket connection and handles connection establishment, connection recovery, and link selection. See also *SS7*.

DDP—Datagram Delivery Protocol. DDP is an AppleTalk Network-layer protocol. It provides connectionless service between sockets and handles both addressing and routing. See also *routing*, *socket*.

DDP-IP gateway—A gateway that adds Datagram Delivery Protocol (DDP) encapsulation to Internet Protocol (IP) packets it transmits, and removes DDP from IP packets it receives. This type of gateway enables the use of AppleTalk Remote Access (ARA) client software for an IP connection.

In Figure 19, the dial-in client is running ARA (which includes DDP-IP tunneling capabilities) and Telnet to communicate with an IP host on the TAOS unit's local interface. The client has its own host route.

Figure 19. DDP-IP connection using ARA



The TAOS unit is configured as an IP router and an AppleTalk router. See also *ARA, AppleTalk routing, DDP, IP, IP router*.

DE—Discard Eligibility. On a Frame Relay network, DE is a bit that you set in a frame to indicate that the network can discard the frame in favor of others in order to maintain Quality of Service (QoS). Frames that have the DE bit set are Be excess data. See also *Be*, *Frame Relay network*.

dedicated channel—A channel on a line rented from the telephone company for exclusive use, 24 hours per day, 7 days per week. A dedicated channel is also called a *leased channel*, a *nailed channel*, or a *nailed-up channel*. See also *dedicated circuit, dedicated line.*

dedicated circuit—A permanent connection between end points, over which two parties exchange data. The number of dedicated channels must be the same at both ends of the connection. For example, if there are five dedicated channels at the local end, there must be five dedicated channels at the remote end. However, channel assignments do not have to match. For example, channel 1 can be switched at the local end and dedicated at the remote end. A dedicated circuit is also known as a *leased circuit*, a *nailed circuit*, a *nailed-up circuit,* or a *private circuit.* See also *dedicated channel, dedicated line*.

dedicated line—A line rented from the telephone company for exclusive use, 24 hours per day, 7 days per week. The connection exists between two predetermined points and cannot be switched to other locations. A dedicated line is also called a *leased line*, a *nailed line,* or a *nailed-up line*. See also *dedicated channel, dedicated circuit*.

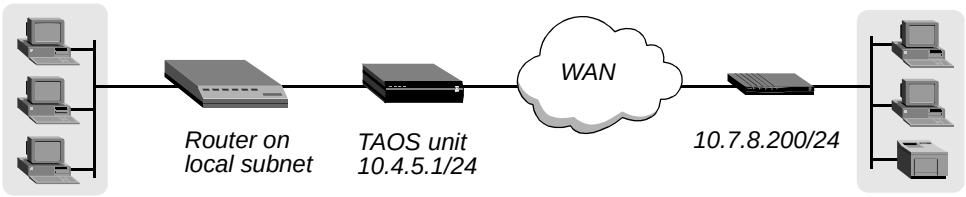
dedicated server—A network device that functions only as a server, performing specific network tasks. See also *server*.

default gateway—The default router that a TAOS unit uses for traffic from a specific connection if it finds no explicit route in the IP routing table. See also *IP router, IP routing table*.

default route—The route that a TAOS unit uses if it does not find a match for a packet's destination address. The default route has the destination address 0.0.0.0. If the TAOS unit finds a default route, it establishes the required connection (if necessary) and forwards the packet.

Figure 20 shows a router, on a local subnet, configured as the default route in a TAOS unit. This type of configuration enables the TAOS unit to turn off RIP on its local interfaces and forward all local packets to the default route.

Figure 20. Default route to a local IP router



If the routing table has no default route and no route that matches a packet's destination address, the TAOS unit drops the packet. See also *IP route*, *IP router*, *IP routing table*.

default zone—The zone assigned to an AppleTalk service on an interface if the service does not have a specified zone in which to reside. See also *zone*, *zone list*.

Defense Communication Agency—See *DCA*.

Defender authentication—A form of token-card authentication that makes use of the AssureNet Pathways Defender authentication server. When you configure Defender authentication, the TAOS unit forwards any call not authenticated by a local Connection profile to the Defender server. Defender authentication proceeds in three stages:

Stage	Description
1	Begins a short time after the caller connects to the TAOS unit, and before the TAOS unit receives the first prompt from the authentication host. The Defender server provides the text of the prompts or challenges, and the TAOS unit passes them to the caller. Calls in Stage 1 are preserved if an authentication host is unavailable or loses its connection. This situation might occur when the very first caller is authenticating with Defender after the router boots up, and the first authentication host is unavailable. The router attempts to authenticate the user through the second and third hosts.
2	Occurs during the time the caller is interacting with the authentication host, but before the authentication sequence is complete. The Defender server uses a challenge-response protocol, expecting a token card to provide the responses. Calls in Stage 2 are never preserved if an authentication host loses its connection. Defender has no mechanism for having one authentication server take over for another if the first loses a connection in the middle of a state.

Stage	Description
3	Occurs when the caller has completed authentication and is interacting with the TAOS unit. Callers in Stage 3 are not dropped by the router, because their calls are already authenticated. However, if the host on which they were authenticated is no longer available, their logout time is not sent. (It would be sent if the host had remained connected.) Defender provides no mechanism to notify one authentication host when a user call authenticated by another host is terminated.

You can use a Defender server with or without RADIUS authentication. The Defender server does not provide per-user control, such as enforcing a maximum number of channels. It provides only per-user authentication. If you need both per-user control and authentication, use RADIUS. See also *authentication server*, *RADIUS*, *token-card server*.

define path—A function that enables you to define a manual path for the Permanent Virtual Circuit (PVC), bypassing the Open Shortest Path First (OSPF) algorithm for PVC routing decisions. See also *OSPF*, *PVC*.

Denial of Service attack—See *DoS attack*.

density enforcement—For AMI-encoded T1 lines, requirements that restrict the system from transmitting 16 consecutive zeroes. See also *AMI*, *T1 line*.

DES—Data Encryption Standard. DES is the U.S. encryption standard for nonclassified documents. This standard uses a 64-bit key and private-key encryption. In private-key encryption, only the sender and receiver know the key for encrypting the data. DES cannot ensure that the sender and receiver are legitimate. A sender who has learned the key can fraudulently use it. See also *DES-CBC*, *encryption*, *private-key encryption.*

DES-CBC—Data Encryption Standard-Cypher Block Chaining. DES-CBC is an Internet Protocol Security (IPSec) encryption algorithm. When you use DES-CBC, message text and signatures are encrypted by means of the DES algorithm in CBC mode. See also *3DES-CBC*, *40DES-CBC*, *DES*, *IPSec*.

Designated Router—See *DR.*

Designated Transit List—See *DTL*.

DeskDial client—Lucent Technologies client software for network modem-pool access.

destination address—In a frame, packet, or message sent over a bridged or routed connection, the IP, IPX, AppleTalk, or hardware address of the intended recipient of the transmission. Compare with *source address*.

Destination Point Code—See *DPC.*

destination port—The port to use to communicate with the destination machine. The port might be, for example, a User Datagram Protocol (UDP) port on an authentication server or a Simple Mail Transfer Protocol (SMTP) port on a mail server. Compare with *source port*. See also *SMTP*, *UDP*, *UDP port.*

Destination Service Access Point—See *DSAP*.

device integration—In ISDN technology, the ability to carry digital signals from various devices over a single network interface. Communication that once required numerous wire pairs can now take place over a single wire pair. The system passes digital signals through local B channels. You can connect a variety of devices to an ISDN line by means of an ISDN network termination type 1 (NT1) device or an ISDN Integrated Access Device (IAD). See also *IAD*, *ISDN*, *ISDN line*, *NT1*.

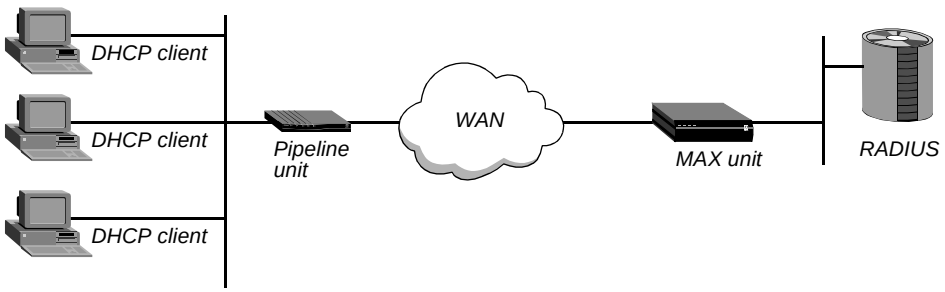
DHCP—Dynamic Host Configuration Protocol. DHCP is a TCP/IP protocol that enables a client to obtain a temporary IP address from a central server (known as a *DHCP server*). See also *DHCP server*.

DHCP server—Dynamic Host Configuration Protocol server. A DHCP server assigns a temporary IP address to a client that requests it. See also *DHCP*, *DHCP spoofing*, *IP address*.

DHCP spoofing—Dynamic Host Configuration Protocol spoofing. A process that enables a local device to receive an IP address from a DHCP server across a slow WAN link. When you set up a DHCP connection, the TAOS unit can assign a dynamic IP address to a remote DHCP client over a bridged connection. The TAOS unit becomes a DHCP server.

For example, suppose a group of DHCP clients resides on a LAN connected to a Pipeline unit, and the Pipeline unit connects to a MAX™ unit over a bridged PPP connection (Figure 21). The MAX unit can assign dynamic IP addresses to any of the DHCP clients on the remote LAN.

Figure 21. Pipeline unit connected to DHCP clients



The RADIUS server holds the configuration information the TAOS unit uses to identify and authenticate each DHCP client. When a PC sends a broadcast DHCP request, the following events take place:

1. Acting as a DHCP server, the Pipeline unit receives the DHCP request and sends the PC a temporary IP address. The address can be static or dynamic. It has a very short Time To Live (TTL) value.
2. The Pipeline unit dials the remote side, passing along the original DHCP request.
3. The DHCP server sends back a server-assigned IP address.
4. When the Pipeline unit receives the address from the remote side, it passes the address to the PC.
5. The PC changes its IP address to the server-assigned address.

Typically, a device requesting an IP address from a DHCP server waits a limited amount of time before timing out the request. For complex WAN links with authentication processes, there might not be enough time to complete the process.

The DHCP server allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment before the 30-minute period expires. The DHCP server uses its local memory to keep track of all IP addresses it has assigned. Therefore, if you reset it, the server loses the entries for current unexpired IP address assignments.

A client can keep an unexpired IP address assignment if you reset the DHCP server. But after the reset, the server might assign that address to a new client. The duplicate IP addresses cause network problems until the first assignment expires or one of the two clients reboots.

See also *DHCP, DHCP server, IP address*.

Diagnostic field—On an X.25 network, an optional field in a Clear-Request, Reset-Request, or Restart-Request packet. Each packet has a required Cause field and an optional Diagnostic field. If the Cause field indicates that the remote Data Terminal Equipment (DTE) did not request the clear, reset, or restart, the Diagnostic field has standard values. If the Cause field indicates that the remote DTE requested the clear, reset, or restart, the Diagnostic field contains information specified in the Cause field by the remote DTE. See also *Cause field, Clear-Request packet, DTE, Reset-Request packet, Restart-Request packet, X.25*.

Dialed Number Information Service—See *DNIS*.

Dialed Number Information Service callback—See *DNIS callback*.

dial-in/dial-out server— See *asynchronous communications server*.

dial-in modem access—The ability of a remote worker using a modem with a PC or other computer device to dial in to a Remote Access Server (RAS) at the corporate office, a central-site location, or a service provider's Point-of-Presence (POP). Compare with *dial-out modem access, LAN-to-LAN modem access*.

dial-in user—A remote user or device that calls a TAOS unit over a switched circuit and requests a connection.

dial-out modem access—The ability of a user at a workstation on a corporate LAN to dial out through a shared modem to a service provider's Point-of-Presence (POP) or branch-office location. Compare with *dial-in modem access, LAN-to-LAN modem access*.

dial-out timer—A value that specifies the maximum number of seconds the system waits for a Call Setup Complete message from the remote side when dialing out.

dial query—A feature designed for sites that support many clients and connections to only a few remote IPX networks. When a TAOS unit receives a Service Advertising Protocol (SAP) query for a file server (service type 0x04) and its SAP table has no entry for that service type, the unit establishes all connections that enable dial query. See also *SAP*.

dial-up line—A connection or circuit between two sites through a switched telephone network. A dial-up is most commonly associated with a voice telephone call between two locations. For modem access, a dial-up line forms a link between two distant pieces of equipment, such as computers or LANs. Not restricted to landline connections, a dial-up circuit can also be established through a circuit-switched cellular network, or through a combination of landline and cellular media. See also *cellular communication, circuit-switched line, landline telephone communication, wireless technology*.

DID—Direct Inward Dialing. A feature that enables a caller outside a company to dial an internal extension without having to go through an operator or attendant.

Digital Access Cross-Connect—See *DAC*.

digital cellular—See *PCS*.

digital data—Data that can have only a limited number of separate values. The time of day represented by a digital clock and the temperature represented by a digital thermometer are examples of digital data. The digital values do not change continuously, but remain at one discrete value and then change to another discrete value. Compare with *analog data*. See also *digital signal*.

Digital Identification Signal—See *DIS*.

digital line—A line that transmits data by means of a digital signal. See also *digital signal*.

digital loopback—A procedure that tests the digital processing for a communications device. Compare with *analog loopback*. See also *local loopback*, *loopback*, *remote loopback*.

Digital Loop Carrier—See *DLC*.

Digital MilliWatt tone—See *DMW tone*.

digital modem—A device in a TAOS unit that enables the unit to communicate over a digital line with a station connected to an analog line. Incoming modem calls and incoming digital calls come over the same digital line. The TAOS unit can accept an incoming call from the network either as a pure digital stream or as a digital stream encoded by Pulse Coded Modulation (PCM). A PCM-encoded digital stream contains a digitized version of the analog waveform sent by a device attached to a modem.

A TAOS unit can also convert outgoing data into analog waveforms, convert these waveforms to a PCM-encoded digital stream, and send them to the network over a digital line. The network presents the data to the receiving modem in analog form over an analog line. The data is in exactly the same form as it would be if sent by an analog-based modem. See also *analog line*, *digital line*, *modem*.

digital multimeter—See *DMM*.

Digital Private Network Signaling System—See *DPNSS*.

digital signal—A type of signal that uses a limited number of discrete values to encode data transmitted over a wire.

The value of the data encoded in a digital signal depends on the state of the signal during a particular time period. Therefore, the sender and the receiver must synchronize their clocks. Each clock runs at a baud rate, the number of times per second the state of the signal is read or set. Several clocking schemes are available, and digital signals often include clock-timing cues.

A digital signal can transmit analog or digital data. For example, a Compact Disc (CD) encodes analog music data into digital signals, while the wires between computers transmit digital data in digital signals. Compare with *analog signal*. See also *analog data*, *clock*, *digital data*.

Digital Signal Cross-Connect—See *DSX*.

Digital Signal level—See *DSx*.

Digital Signal Processor—See *DSP*.

Digital Subscriber Line—See *DSL*.

digital-to-analog conversion—See *D-A conversion*.

DIP switch—Dual Inline Package switch. A DIP switch is a small switch that you use to select the operating mode of a device.

direct-access dial-out—A feature that enables terminal-server users to have direct access to a particular Telnet port for modem dial-out. See also *modem dial-out*.

direct FRAD—See *FRAD*.

direct Frame Relay Access Device—See *FRAD*.

Direct Inward Dialing—See *DID*.

direct route—A route that can reach a destination without going through any intervening routers. See also *route*, *router*.

DIS—Digital Identification Signal. A signal sent at 300 baud by a fax device when it answers a call. A fax device uses the DIS to specify the features that it supports.

Discard Eligibility—See *DE*.

Disconnect message—See *ISDN Disconnect message*.

Disconnect-Request packet—A message from a client of a TAOS unit, asking the unit to disconnect the session. See also *Disconnect-Request-ACKed packet*, *Disconnect-Request-NAKed packet*.

Disconnect-Request-ACKed packet—A message that a TAOS unit sends to a client if it finds at least one session to disconnect. Compare with *Disconnect-Request-NAKed packet*. See also *Disconnect-Request packet*.

Disconnect-Request-NAKed packet—A message that a TAOS unit sends to a client if it could not find a session to disconnect. Compare with *Disconnect-Request-ACKed packet*. See also *Disconnect-Request packet*.

Disengage Confirmation message—See *DCF message*.

Disengage Request message—*DRQ message*.

disk capture feature—A feature that enables your terminal emulator to capture to disk the ASCII characters it receives at its serial port. See also *serial port*, *terminal emulator*.

distance-vector metric—A metric that uses a hop count to select the shortest route to a destination network. Routing Information Protocol (RIP) always uses the lowest hop count, regardless of the speed or reliability of a link. Compare with *link-state metric*. See also *RIP*.

distinct secret—In a Layer 2 Forwarding (L2F) configuration, a feature that enables you to specify one password to authenticate the Network Access Server (NAS) to the home gateway, and another password to authenticate the home gateway to the NAS. The following sequence of events describes how a TAOS unit uses distinct secrets to authenticate L2F tunnels:

1. A client requests access and the TAOS unit looks up the username and password in the associated Connection profile or RADIUS profile.
2. If an L2F tunnel is specified in the Connection profile or RADIUS profile, the TAOS unit either adds the client connection to an existing tunnel or creates a new tunnel to the specified server end point.
3. If a password is present in the Connection profile or RADIUS profile, the TAOS unit uses this password to authenticate the NAS to the home gateway.
4. The TAOS unit authenticates the home gateway by locating a profile that matches the name provided by the home gateway.
5. The TAOS unit establishes the tunnel between itself and the home gateway.

Compare with *shared secret*. See also *L2F*, *NAS*.

Distributed Queue Dual Bus—See *802.6*.

DIX connector—See *AUI*.

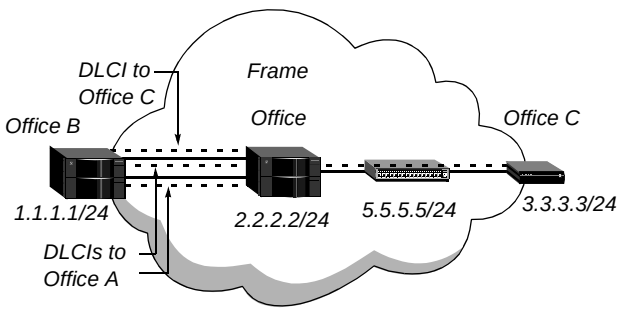
DLC—Digital Loop Carrier. DLC is equipment that concentrates analog local loop lines by digitizing and multiplexing calls for transmission to the Central Office (CO). See also *CO*, *local loop*, *multiplexing*.

DLCI—Data Link Connection Identifier. A unique number that the administrator assigns to a Permanent Virtual Circuit (PVC) in a Frame Relay network. See also *Frame Relay network*.

DLCI bundling—A multilink Frame Relay (MFR) feature that creates DLC bundles to enable a more flexible use of physical lines. When you use DLCI bundling, a single line can support both bundled and nonbundled connections. In each of the MFR peers, the bandwidth used by the bundled connections must reside on the same card.

In the following example, a company has three offices connected by means of Frame Relay. Office A receives heavy traffic from Office B, and Office C receives very little traffic from Office B. Office B has two T1 lines to Office A. As shown in Figure 22, instead of installing a third fractional T1 line from Office B to Office C, you can include traffic destined for Office C on one of the existing T1 lines and define a bundle of two DLCIs to Office A.

Figure 22. Example of MFR on per-DLCI basis



Because very little traffic is sent to Office C, most of the bandwidth of the second T1 line is available for traffic to Office A.

See also *DLCI, Frame Relay network, MFR, MFR bundle.*

DLE, EOT command—A clear-request signal from the Data Terminal Equipment (DTE) on a T3POS PAD connection. The X.25/T3POS PAD clears the call when it receives a DLE, EOT command. See also *DTE, X.25/T3POS.*

DLE, EOT timer—A value that specifies the maximum idle time the PAD allows for a T3POS call. The DLE, EOT timer applies only to Transparent and Blind mode. It is disabled in both Local and Binary Local mode. The DLE, EOT timer is also called the *T5 timer.* See also *Binary Local mode, Blind mode, Local mode, Transparent mode, X.25/T3POS*.

DMM—Digital multimeter. An instrument used for measuring voltage, current, and resistance. Values are displayed digitally rather than by an analog dial.

DMT—Discrete MultiTone. A method of sending data over copper telephone wires by dividing the frequency range into 256 subfrequencies, from 64kHz to 1.1MHz. Each subfrequency is an independent channel with its own signals.

DMW tone—Digital MilliWatt tone. A 1000Hz tone that a Signaling System 7 (SS7) switch sends to a TAOS unit over an Internet Protocol Device Control (IPDC) link. The DMW tone requests that the unit generate special test calls that measure the line distortion and attenuation in the telephone network. See also *IPDC, SS7 network*.

DNIS—Dialed Number Information Service. DNIS is a telephone company service that provides information about the called number (for example, the name and location of the target user or device).

DNIS callback—Dialed Number Information Service callback. DNIS callback is the method by which a TAOS unit uses the DNIS information element to detect callback during the ringing state of an incoming call. The unit does not answer the call (go off hook), and the originating caller is not charged for the call. Compare with *Ascend callback, CBCP callback, CLID callback*. See also *callback.*

DNS—Domain Name System. DNS is a TCP/IP service for centralized management of address resolution. Using DNS, you can specify a symbolic name instead of an IP address. DNS maintains a database of network numbers and corresponding domain names. When you use a symbolic name, DNS translates the domain name into an IP address and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the symbolic name corresponding to the IP address. See also *address resolution, host number, IP address, IP network number, local DNS table, symbolic name*.

DNS list attempt—A feature that enables a TAOS unit to avoid disconnecting physical links when a host is unavailable. Domain Name System (DNS) can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of the hosts. A user typically attempts to connect to the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is broken when the initial connection attempt fails. When you enable the DNS list attempt feature, the TAOS unit tries one entry in the DNS list of hosts, and if that connection fails, tries the next entry, and so on, without closing the WAN session. See also *DNS, L2TP list attempt*.

domain identifier—The portion of a domain name that appears last and specifies the type of organization to which the host belongs. The Internet Network Information Center (InterNIC) provides the following domain identifiers:

Domain identifier	Description
.arpa	ARPANET
.com	Commercial enterprise
.edu	Educational institution
.gov	Governmental organization
.mil	Military organization
.org	An organization not covered by the other categories

domain name—The portion of a symbolic name that corresponds to the network number in the IP address. In the symbolic name `steve@abc.com`, the domain name is `abc.com`. See also *IP address*, *IP network number*.

Domain Name System—See *DNS*.

Domain-Specific Part—See *DSP*.

DoS attack—Denial of Service attack. A DoS attack is a deliberate attempt to interfere with network performance by directing forged Internet Control Message Protocol (ICMP) Echo Request packets to IP broadcast addresses.

Under ordinary circumstances, to determine whether a machine on the Internet is connected and responding, a host sends an ICMP Echo Request packet. If a machine receives the packet, it returns an ICMP Echo Reply packet. In a DoS attack, however, an attacker directs ICMP Echo Request packets to IP broadcast addresses from one or more remote locations. An intermediary receives an ICMP Echo Request packet directed to the IP broadcast address of its network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, the machines on the network receive the ICMP Echo Request packet, and each sends an ICMP Echo Reply packet in return.

The packets from the attacker do not use the IP address of the source machine as the source address. Instead, they contain the spoofed source address of the intended victim. When all the machines at the intermediary's site respond to the ICMP Echo Requests, they send replies to the victim's device. An attacker can send DoS attacks to multiple intermediaries at the same time, causing all of the intermediaries to direct responses to the same victim. Both the intermediary and victim of a DoS attack can suffer severely degraded network performance.

To protect against DoS attacks, you should disable IP-directed broadcasts on the TAOS unit. By disabling these broadcasts, you deny an attacker the ability to direct IP broadcast traffic onto your network. In addition, you should prevent the TAOS unit from responding to ICMP packets sent to IP broadcast addresses. If someone compromises a machine on your network, he or she might try to launch an attack using the TAOS unit as an intermediary, sending the ICMP Echo Request packet to the IP broadcast address of the local network. Because this traffic does not travel through a router to reach the machines on the local network, disabling IP-directed broadcasts on the TAOS unit is not sufficient to prevent a DoS attack. You must also prevent the TAOS unit from responding to ICMP packets sent to the local broadcast address. See also *Echo*, *ICMP*.

dotted decimal notation—A system for specifying an IP address or subnet mask. In dotted decimal notation, each of the four portions of the IP address or mask is separated from the others by a decimal point, as in the address 200.10.5.1. See also *IP address*, *subnet mask.*

DOVBS—See *3.1kHz audio-bearer service.*

downstream path—The path a call takes from a carrier's Central Office (CO) to the end user's home.

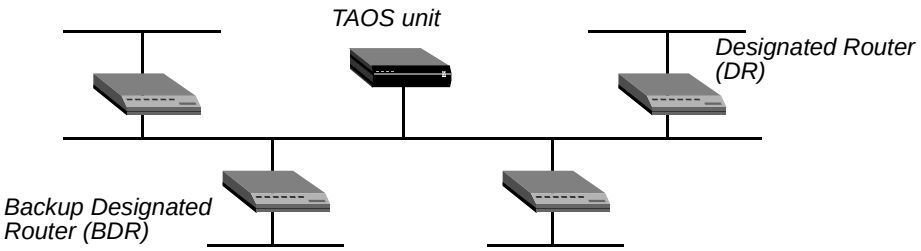
DPC—Destination Point Code. In a Signaling System 7 (SS7) network, the DPC identifies the destination of the signaling message. See also *SS7 network*.

DPNSS—Digital Private Network Signaling System. DPNSS is a standard that defines how different Private Branch Exchange (PBX) systems can interoperate to produce a single virtual PBX. See also *PBX*.

DQDB—See *802.6.*

DR—Designated Router. The DR is the router with which all other Open Shortest Path First (OSPF) routers in a broadcast network establish adjacencies. Figure 23 illustrates a configuration with both a DR and a Backup Designated Router (BDR).

Figure 23. Designated and Backup Designated Routers



To reduce the number of adjacencies each router must form, OSPF designates one of the routers as the DR. Doing so simplifies the routing table update procedure and reduces the number of link-state records in the database. The DR plays other important roles in reducing the overhead of OSPF link-state procedures. For example, other routers send Link State Advertisements (LSAs) to the DR by using the "all-designated-routers" multicast address of 224.0.0.6.

The administrator chooses the DR on the basis of the processing power, speed, and memory of the system, and then assigns priorities to other routers in case the BDR is down at the same time. A TAOS unit can function as a DR or BDR. However, many sites choose to assign a LAN-based router as the DR or BDR in order to dedicate the TAOS unit to WAN processing.

See also *adjacency*, *BDR*, *LSA*, *OSPF*, *router*.

DRAM—Dynamic Random Access Memory. DRAM is a kind of memory whose information resides in capacitors. The charge of each capacitor must be periodically refreshed. Compare with *EEPROM*, *NVRAM*, *RAM*.

drop-and-insert—A feature that enables a single T1 line to carry both data and voice traffic. The TAOS unit specifies a preallocated portion of the T1 line to use both dedicated and switched circuits for LAN internetworking. The remaining portion of the line can go to a PBX with a T1 interface. The PBX can access both dedicated and switched circuits for voice purposes. You can also use drop-and-insert to share access-line bandwidth between the TAOS unit and equipment other than a PBX (for example, a channel bank or T1 multiplexer). See also *channel bank, dedicated circuit, multiplexer, PCM, switched circuit, T1 line*.

drop-and-insert multiplexer—A T1/E1 multiplexer that enables organizations to bypass the PBX for data communications. The Drop-and Insert-configuration is used to allocate channels to different equipment, such as channel banks and Digital Access Cross-Connects (DACs). The drop-and-insert multiplexer drops off some of the channels to the data devices. It then stuffs bits into the channels it drops off, so that a full T1/E1 transmission is sent to the PBX's T1/E1 multiplexing equipment. See also *channel bank, DAC, multiplexer, PBX*.

DRQ message—Disengage Request message. An H.323 Registration, Admission, and Status (RAS) message sent from a MultiVoice gateway to a MultiVoice Access Manager (MVAM) device when a call ends. Compare with *ARQ message*. See also *DCF message, H.323, MultiVoice™, MVAM, RAS*.

DS0 channel—A 64Kbps D channel on a digital line. See also *DS1 channel*.

DS0 minute—The online usage of a single 56Kbps or 64Kbps switched channel for one minute. For example, a 5-minute, six-channel call uses 30 DS0 minutes.

DS1 channel—For a T1 line, a 1.544Mbps channel that consists of 24 DS0 channels and an extra framing bit; for an E1 line, a 2.048Mbps channel that consists of 32 DS0 channels. On a T1 line, a DS1 channel uses either the D4 or ESF method of framing. See also *D4-framed T1 line, DS0 channel, DS3 line, E1 line, ESF, T1 line*.

DS2 channel—For a T1 line, a 6.312Mbps channel that consists of four DS1 channels; for an E1 line, an 8.45Mbps channel that consists of four DS1 channels. See also *DS1 channel*.

DS3 line—A 44.736Mbps line consisting of seven DS2 channels. A DS3 line is also called a *T3 line*. See also *DS2 channel, T3 line*.

DSAP—Destination Service Access Point. A DSAP is the Service Access Point (SAP) address at which the Logical Link Control (LLC) layer passes information to a Network-layer process. Compare with *SSAP*. See also *SAP*.

DSL—Digital Subscriber Line. DSL is a technology that provides high bandwidth over the conventional copper wiring that makes up the local loop of the Public Switched Telephone Network (PSTN). DSL links bypass the network's circuit-switched lines and provide much faster data-transmission rates than analog modem connections. See also *ADSL, HDSL, IDSL, PSTN, RADSL, SDSL, VDSL*.

DSL Access Multiplexer—See *DSLAM*.

DSLAM—DSL Access Multiplexer. Located at the telephone company's Central Office (CO), a DSLAM concentrates the data traffic from multiple loops onto a single Asynchronous Transfer Mode (ATM) line. Some DSLAMs provide added features such as extensive call routing and comprehensive network management. See also *ATM*, *CO*, *DSL*, *MultiDSL™*, *NSP*, *T1 line*, *T3 line*.

DSLMAX™—A comprehensive Digital Subscriber Line Access Multiplexer (DSLAM) providing Digital Subscriber Line (DSL) access concentration and circuit termination. Designed for high-speed low-density WAN access, the DSLMAX unit is an integrated Layer-2 (multiplexing) and Layer-3 (routing) device that uses TAOS. See also *DSL*, *DSLAM*, *TAOS*.

DSL modem—See *DSL remote transceiver unit*.

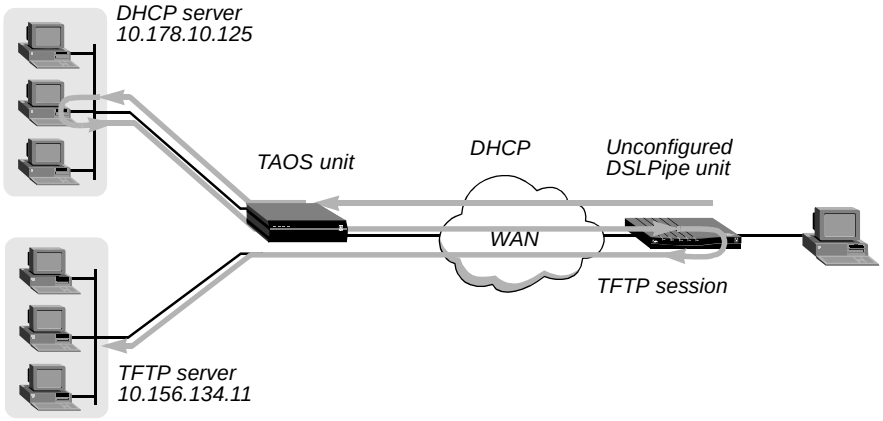
DSLPipe™—A Lucent Technologies product that enables you to take advantage of high-speed SDSL services. This powerful router lets you access multiple destinations simultaneously to download high-resolution graphics, gain access to multimedia applications, or transmit large files from a corporate intranet. See also *DSL*, *DSLPipe plug-and-play*.

DSLPipe plug-and-play—A feature that enables a DSLPipe to obtain its configuration through a TAOS unit by using the Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP). DSLPipe units ship with the plug-and-play feature enabled, so they require absolutely no configuration (provided that the TAOS unit and servers have been configured properly).

When a DSLPipe unit starts up, it uses factory default settings that enable it to forward a DHCP request to a TAOS unit. The TAOS unit sends the request to a DHCP server. The DHCP server returns an IP address, subnet mask, the path to a more detailed configuration file, and a TFTP server hostname. The TAOS unit forwards the DHCP response to the requesting DHCP client.

Figure 24 illustrates how plug-and-play works.

Figure 24. DSLPipe unit obtaining its configuration (plug-and-play)



To gain access to the specified TFTP server and its configuration file, the DSLPipe unit uses the minimal configuration obtained by means of DHCP. After downloading the file, the unit begins using the configuration. See also *DHCP*, *DHCP server*, *DSL*, *DSLPipe™*, *TFTP*.

DSL remote transceiver unit—A device that bridges or routes data between two LANs across a DSL connection. With router-based support for IP traffic, a DSL remote transceiver unit can create and maintain subnets to allow segmentation of the LAN. Multicast and unicast traffic recognition is also supported. In addition, router support can provide privacy, security, and protection against such LAN problems as broadcast storms.

Typically, a DSL remote transceiver unit consists of one DSL port, one Ethernet port, and a console port used for management. Units operate in pairs across the local loop. The type of unit used by the subscriber must match the one used at the Central Office (CO).

A DSL remote transceiver unit is also called a *DSL modem*. See also *CO*, *DSL*, *local loop*.

DSL Terminator™—A unit that receives and routes the data on the Virtual Circuits (VCs) provided by the Digital Subscriber Line Access Multiplexers (DSLAMs) that physically terminate Digital Subscriber Line (DSL) copper wiring. As a Layer-3 (routing) device, a DSL Terminator can be placed in remote locations or in central data centers. See also *DSL*, *DSLAM*, *VC*.

DSP—Digital Signal Processor. Also, Domain-Specific Part. A Digital Signal Processor analyzes and processes analog signals, converting them to digital format. (See also *analog signal*, *digital signal*.) The Domain-Specific Part is a portion of an Asynchronous Transfer Mode (ATM) address in ATM End System Address (AESA) format. The DSP specifies the High-Order Domain-Specific Part (HO-DSP), End System Identifier (ESI), and Selector (SEL) subfields. Compare with *IDP*. See also *AESA format*, *ESI*, *HO-DSP*, *SEL subfield*.

DSR—Data Set Ready. DSR is a signal that a modem transmits when it is ready to send and receive data. See also *modem*.

DSU—Data Service Unit. Along with a Channel Service Unit (CSU), a DSU is a component of Data Circuit-terminating Equipment (DCE). The DSU connects to Data Terminal Equipment (DTE) by means of a synchronous serial interface, such as a V.35, RS-422, or RS-423 connection. The DSU formats and controls the flow of digital data between the network and the CSU. See also *CSU*, *DCE*, *digital data*, *DTE*, *RS-422*, *RS-423*, *V.35*.

DSX—Digital Signal Cross-Connect. DSX is a method of connecting DS1 and DS3 signals by linking T1 and T3 lines. See also *DS1 channel*, *DS3 line*, *T1 line*, *T3 line*.

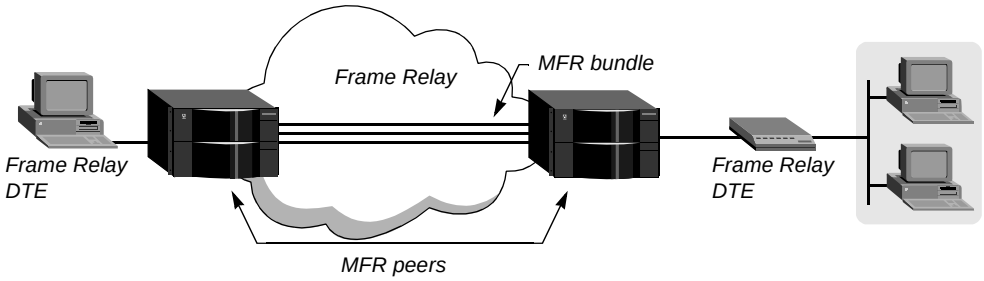
DSx—Digital Signal level. DSx is a physical-layer designation associated with T-carrier and E-carrier circuits. Many people use the T1/E1 and physical-layer designations interchangeably. However, DSx is a service designation that refers to the actual speed of the connection, while the T or E designation refers to the carrier type. See also *DS0 channel*, *DS1 channel*, *DS2 channel*, *DS3 line*, *E-carrier circuit*, *T-carrier circuit*.

DTE—Data Terminal Equipment. DTE refers to a device that an operator uses (for example, a computer or a terminal). Compare with *DCE*.

DTE–DTE aggregation—A Frame Relay configuration that enables two Data Terminal Equipment (DTE) devices to use the aggregate bandwidth of a Frame Relay Multilink (MFR) bundle across a regular Frame Relay (non-MFR) network. The fact that aggregate bandwidth of multiple links is in use is transparent to the Frame Relay switching equipment that resides between MFR peers.

Figure 25 shows two DTE devices using an MFR bundle of three data links through a Frame Relay network.

Figure 25. MFR DTE-DTE aggregation



To aggregate the bandwidth, a TAOS unit uses a segmentation-sequencing-reassembly protocol described in the Frame Relay Fragmentation Implementation Agreement FRF.12, which is based on the Multilink PPP (MP) described in RFC 1990. See also *DTE*, *Frame Relay*, *MFR*, *MFR bundle*, *MP*.

DTL—Designated Transit List. A list of nodes and link IDs that indicate a path across a Private Network-to-Network Interface (PNNI) peer group. See also *PNNI*, *PNNI peer group*.

DTMF—Dual-Tone Multifrequency. DTMF is a technology that enables a touch-tone telephone to create 16 tones that use only eight frequencies.

DTMF-R2 signaling—Dual-Tone Multifrequency R2 signaling. The dual-tone signaling standard used for European digital trunk signaling. Compare with *MFC-R2 signaling*.

DTR—Data Transmit Ready. DTR is a signal indicating that a device is ready to transmit and receive data.

dual-capacity card—A slot card that performs the functions of both a host card and a network card. See also *host card*, *network card*, *slot card*.

Dual Inline Position switch—See *DIP switch*.

dual IP—A method of assigning a second IP address to the Ethernet interface in order to give the TAOS unit a logical interface on two networks (or subnets) on the same backbone. See also *IP*, *IP address*.

dual-port call—A call in which a codec performs inverse multiplexing on two channels in order to achieve twice the bandwidth of a single channel. The codec provides two ports, one for each channel. Two AIM ports on the TAOS unit connect a dual-port call to the codec. These ports are the *primary port* and the *secondary port*. Because the TAOS unit places the two calls in tandem and clears the calls in tandem, it considers them a single call. See also *AIM port*, *codec*, *inverse multiplexing*.

Dual-Tone Multifrequency—See *DTMF*.

Dual-Tone Multifrequency R2 signaling—See *DTMF-R2 signaling*.

DXI—Data Exchange Interface. Described in RFC 1483, DXI defines how a network device can convert data for transmission between different network services. For Asynchronous Transfer Mode (ATM) configurations, DXI is an interface between Data Terminal Equipment (DTE) and an ATM Channel Service Unit/Data Service Unit (CSU/DSU). The ATM CSU/DSU carries out the process of conversion between variable-length DXI frames and fixed-length ATM cells. See also *ATM*, *ATM cell*, *CSU*, *DSU*, *DTE*.

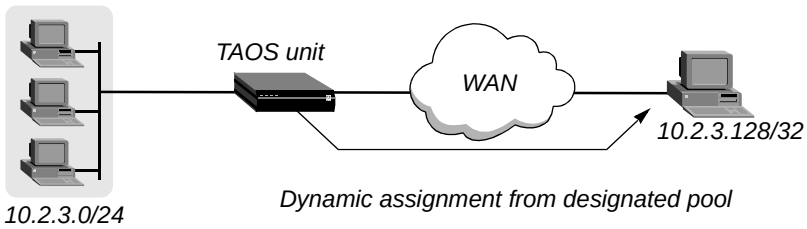
Dynamic Bandwidth Allocation—See *DBA*.

dynamic bandwidth overflow—A method of supplementing bandwidth during periods of peak demand. Through the mechanism of inverse multiplexing, a TAOS unit adds bandwidth when traffic reaches a specified level. See also *DBA*, *inverse multiplexing*.

Dynamic Host Configuration Protocol—See *DHCP*.

dynamic IP—The process of assigning an IP address to a dial-in caller from an IP address pool. Figure 26 shows a TAOS unit assigning an address from one of its defined pools.

Figure 26. Dial-in host requiring assigned IP address



See also *IP address*, *IP address pool*.

Dynamic Random Access Memory—See *DRAM*.

dynamic rate adaptation—A process in which a line adjusts its bit rate dynamically on the basis of specified noise margins and noise-level intervals. The line upshifts to increase its bit rate or downshifts to reduce it.

dynamic route—A path that a router learns by means of dynamic updates from other routers, rather than by means of a static specification in a configured profile. Routers that use Routing Information Protocol (RIP) broadcast their entire routing tables every 30 seconds, updating other routers about which routes are usable. Hosts that run Internet Control Message Protocol (ICMP) can also send ICMP Redirect packets to offer a better path to a destination network. To update their routing tables, Open Shortest Path First (OSPF) routers propagate link-state changes as they occur. Compare with *multipath route*, *static IP route*. See also *IP route*, *IPX route*, *route*.

dynamic routing—A routing technique that enables a message's route to change as the message proceeds along the network.

E

E1 line—A 2.048Mbps line that supports 32 64Kbps channels, each of which can transmit and receive data or digitized voice. The line uses framing and signaling to achieve synchronous and reliable transmission. The most common configurations for E1 lines are E1 PRI and unchannelized E1. See also *channelized T1 PRI/E1 PRI*, *E1 PRI line*, *unchannelized T1 PRI/E1 PRI*.

E1 PRI line—E1 Primary Rate Interface line. An E1 PRI line consists of 32 64Kbps channels. It uses 30 B channels for user data, 1 64Kbps D channel for ISDN D-channel signaling, and 1 framing channel. The B channels can be all switched, all dedicated, or a combination of switched and dedicated. The E1 PRI line is a standard in Europe and Asia, but is called CEPT G.703 on those continents. Compare with *ISDN BRI line*, *T1 PRI line*. See also *B channel*, *channelized T1 PRI/E1 PRI*, *D channel*, *dedicated channel*, *E1 line*, *ISDN D-channel signaling*, *switched channel*, *unchannelized T1 PRI/E1 PRI*.

E1 Primary Rate Interface line—See *E1 PRI line*.

E1-R2 Israeli signaling—See *R2 signaling*.

E.164—A standard for public-network addressing, using up to 15 digits. See also *E.164 AESA format*.

E.164 AESA format—E.164 ATM End System Address format. In E.164 AESA format, the E.164 address is specified in international format. Compare with *Custom AESA format*, *DCC AESA format*, *E.164*, *ICD AESA format*. See also *AESA format*.

E.164 address—See *native E.164 address.*

E2 line—An 8.45Mbps line that supports four 2.048Mbps E1 channels.

E3 line—A 34Mbps line that supports 16 2.048Mbps E1 channels.

Early Packet Discard—See *EPD*.

early ringback—In a MultiVoice environment, a ringback tone that the local gateway sends to the caller as soon as a call is started on the remote gateway. Early ringback is intended only for networks with long call setup times, such as satellite IP networks, wireless networks, and networks using Channel Associated Signaling (CAS). See also *CAS*, *MultiVoice™*, *ringback tone*.

EAS—External Authentication Server. See *authentication server*.

EAZ—Endgeraete Auswahl Ziffer. For calls over German 1TR6 lines, EAZ is a one-digit string appended to the telephone number.

E-carrier circuit—An E1 or E3 circuit. In Europe, the Pacific Rim, the Middle East, and Latin America, E-carrier circuits are the most widely used digital communications circuits. An E1 circuit has a total capacity of 2.048Mbps. Each E1 circuit can be divided into 32 channels of 64Kbps each. An E3 circuit is equivalent to 16 E1 circuits and has a total capacity of 34.368Mbps. E1 and E3 circuits are commonly used in central sites to support network services and applications similar to those handled by T1 and T3 circuits. Compare with *T-carrier circuit*. See also *E1 line*, *E3 line*.

Echo—A signal that determines whether a node can receive and acknowledge data transmissions. A host sends an Echo Request packet. If the destination is properly connected and receives the Echo Request packet, it sends back an Echo Reply packet.

echo cancellation—A method that the telephone company uses to remove echoes from an analog line. See also *analog line*, *echo tail*.

echo tail—The amount of hybrid-line echo that the G.165 echo canceller can eliminate in Voice over IP (VoIP) calls. The echo canceller is designed to eliminate the echo generated when a voice call is transmitted across a two-wire/four-wire boundary. The echo canceller is applied to the speech on the trunk side of a TAOS unit. It does not suppress the acoustic echo that is normally generated at the calling end point (receiver/transmitter echo). When the length of the hybrid-line echo exceeds 32 milliseconds, the echo will be detected at the distant end point. See also *echo cancellation*.

echo test—A diagnostic test, used to verify network reachability, in which an Internet Control Message Protocol (ICMP) Echo Request packet or Simple Network Management Protocol (SNMP) test packet is sent to elicit a standard response. See also *ICMP*, *SNMP*.

ECM—Error Correction Mode. In the event that a frame is not received correctly during a real-time fax call, ECM enables fax frames to be retransmitted. ECM frames are relayed end to end between terminals. See also *real-time fax over IP*.

ECN—Explicit Congestion Notification. ECN is a method of informing Frame Relay nodes that there is traffic congestion on the network. The Frame Relay header can use a Backward Explicit Congestion Notification (BECN) bit or a Forward Explicit Congestion Notification (FECN) bit to notify nodes of traffic congestion. See also *BECN*, *congestion*, *congestion management*, *FECN*, *Frame Relay*.

EDAC—Error Detection and Correction. EDAC is a method of determining whether transmission errors have occurred. In the event of an error, EDAC makes the necessary corrections. See also *error correction*.

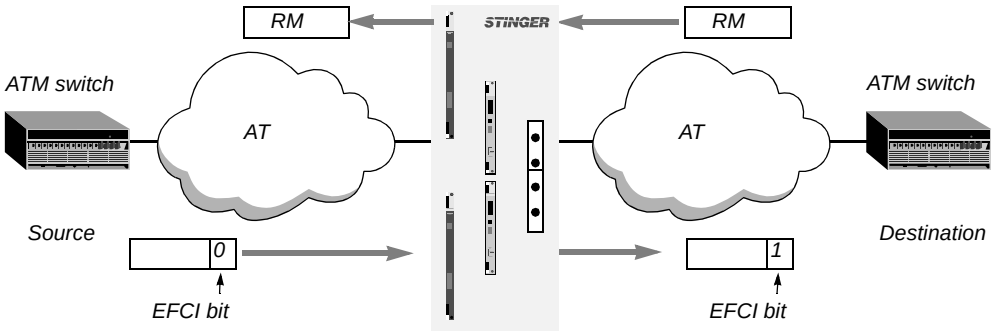
EEPROM—Electronically Erasable Programmable Read-Only Memory. EEPROM is a type of Programmable Read-Only Memory (PROM) that can be erased by exposing it to an electrical charge. EEPROM retains its contents across resets and power cycles. Data is written or erased one byte at a time. See also *PROM*.

EFCI—Explicit Forward Congestion Indication. In Asynchronous Transfer Mode (ATM), EFCI is a field in a cell header. The EFCI field is set to notify the destination device of a nearly congested or fully congested network condition. See also *ATM*, *congestion*.

EFCI marking—Explicit Forward Congestion Indication marking. EFCI is a type of marking that signals to the next Asynchronous Transfer Mode (ATM) switch that the TAOS unit's buffer thresholds are exceeded. The unit sets the EFCI bit in the header of transmitted data cells. The destination system stores the EFCI state and includes it in the congestion-indication bit of its Resource Management (RM) cells. The source system then uses the information it obtains from the RM cells to adjust its cell transmission rate.

Figure 27 shows a TAOS unit setting the EFCI bit to 1 in its transmitted data cells. The destination system returns RM cells that will cause the source system to slow down its transmissions.

Figure 27. Congestion management with EFCI



See also *RM cell*.

EGP—Exterior Gateway Protocol. EGP is a type of protocol used to exchange routing information between one Open Shortest Path First (OSPF) Autonomous System (AS) and another. The AS number can be used by Area Border Routers (ABRs) to filter out certain EGP routing information. OSPF can make use of EGP data generated by other border routers and added to the OSPF system as Autonomous System Externals (ASEs). See also *ABR*, *AS*, *ASE*, *OSPF*.

EIA—Electronic Industries Association. The EIA is a group that determines standards for electrical transmission.

EIA/TIA-232—A Physical-layer standard nearly identical to V.24. EIA/TIA-232 is also known as *RS-232*. See also *RS-232*.

EIA-449—A Physical-layer standard also known as *RS-449*. See also *RS-449*.

EIA-530—A way of referring to RS-422 and RS-423. See also *RS-422*, *RS-423*.

eight-bit Binary mode—See *Binary mode*.

Electronically Erasable Programmable Read-Only Memory—See *EEPROM*.

Electronic Industries Association—See *EIA*.

Embedded Operations Channel—See *EOC*.

en-bloc dialing—The process of sending all dialed digits to a TAOS unit in one block. When a TAOS unit uses Q.931 en-bloc dialing, the Setup message sent by the dialing unit to the network switch contains all information required to process the call. Therefore, the TAOS unit can obtain the dial number from a called-number Information Element, instead of from the keypad-facility Information Element used by overlap-dialing devices. Q.931 en-bloc dialing is also known as *senderized digit transmission*. See also *en-bloc receiving*, *Q.931*.

en-bloc receiving—A feature that affects the procedure of establishing an incoming call received on a T1 PRI or E1 PRI line on a TAOS unit. When a TAOS unit uses en-bloc receiving, the Setup message received from the network switch must contain all information required to process the call. See also *en-bloc dialing*. Compare with *overlap receiving*.

Encapsulating Security Payload—See *ESP*.

encapsulation—A technique used by layered protocols. A low-level protocol accepts a message from a higher-level protocol and places the message in the data portion of the lower-level frame. The logistics of encapsulation require that packets traveling over a physical network contain a sequence of headers. Encapsulation enables the transmission of data over networks that use differing protocols. See also *protocol*.

encryption—A process that takes ordinary data and converts it into a format unreadable to anyone without a decryption key. Authorized personnel with access to this key can unscramble the information. Data encryption is a useful tool against network snoopers. See also *private-key encryption*, *public-key encryption*.

end-of-pulse signaling—See *EOP signaling*.

end point—When a tunneling protocol is in use, the system that encapsulates the packets (the Foreign Agent) or the system that decapsulates the packets (the tunnel server). Examples of tunneling protocols are Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP). See also *ATMP*, *L2TP*, *PPTP*.

end point discriminator option—On a Multilink PPP (MP) or Multilink Protocol Plus (MP+) link, a method of identifying the system transmitting the packet. The end point discriminator option indicates to a system whether the peer on the link could be the same as the peer on another connection. If the option distinguishes the peer from all others, the system must establish a new bundle for the link. See also *bundle*, *MP*, *MP+*.

End System Identifier—See *ESI*.

End-to-End Delay— An Asynchronous Transfer Mode (ATM) routing metric that measures the time it takes a cell to get from one end of a connection to the other. See also *Admin Cost*, *ATM*, *CDV*.

Enhanced Through Cellular—See *ETC*.

Enigma—An important provider of network security applications. Enigma's SafeWord AS (also known as the *Enigma Logic SafeWord server*) is a UNIX-based software authentication server that identifies users by means of dynamic passwords (called *tokens*). The server identifies users at the point of connection to a TCP/IP network, and uses standard network authentication protocols and token cards. See also *SafeWord authentication*, *SafeWord token*, *token*, *token card*, *token-card authentication*, *token-card server*.

ENQ—A control character that signifies a request for identification or status on an X.25/T3POS connection. See also *ENQ handling timer*, *X.25/T3POS.*

ENQ handling timer—A value that specifies the amount of time the Packet Assembler/Disassembler (PAD) waits for an ENQ from the host on an X.25/T3POS connection. See also *ENQ*, *PAD*, *X.25/T3POS*.

enterprise-wide network—A network that contains all or most of a company's hardware and software resources. Typically, an enterprise-wide network includes computers that run different operating systems and reside on different types of networks. Therefore, achieving interoperability is the biggest challenge facing the administrator of an enterprise-wide network.

environment variable—A system-defined or user-defined variable that provides information to the UNIX shell about the operating environment.

EOC—Embedded Operations Channel. In a BRI-U interface, an EOC is the out-of-band mechanism for implementing maintenance functions. Instead of using the D or B channels, EOC uses the maintenance bits of the U-interface superframe. Maintenance functions include test loopback, statistics gathering, and requests to generate errors (to verify that the block-error counters work). See also *B channel*, *D channel*.

EOP signaling—End-of-pulse signaling. A method for determining when transmission of a dial string is complete. Collection of the dialed digits is considered complete when the listening device detects an interval of silence exceeding the interval between dialed digits.

EPD—Early Packet Discard. EPD is an Asynchronous Transfer Mode (ATM) flow-control mechanism. The ATM Flow-Control Processor performs EPD for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate-Non Real Time (VBR-NRT) Virtual Channels (VCs). If a cell causes the queue for a VC to exceed the discard thresholds, the VC enters the EPD state. The cells in the current packet of the VC are admitted to the queue. However, when the end of the current packet is detected, subsequent cells are discarded. Compare with *Selective Discard*, *PPD*. See also *ABR*, *ATM*, *ATM Flow-Control Processor*, *UBR*, *VBR-NRT*, *VC*.

epoch date—A starting date from which a system measures time. The Internet uses January 1, 1900 as its epoch date. See also *Internet*.

Equal Access—See *FGD*.

error correction—A process that determines whether line noise has caused data to be garbled or dropped in transit, and then attempts to correct the problem. The two most common error-correction protocols and standards used by analog modems are MNP and V.42. See also *MNP*, *V.42*.

Error Correction Mode—See *ECM*.

Error Detection and Correction—See *EDAC*.

Errored Second—On a SONET network, a second in which one or more coding violations or incoming errors have occurred in a line, path, or section. Compare with *Severely Errored Frame*, *Severely Errored Framing Second*, *Severely Errored Second*. See also *line*, *path*, *section*, *SONET*.

error rate—The ratio of the number of bits received incorrectly and the total number of bits in the transmission.

ESF—Extended SuperFrame. ESF is a framing format that consists of 24 consecutive frames, separated by framing bits. Each frame consists of a DS0 time slot and a coded framing bit. The frame is repeated 24 times to create a superframe. The ISDN specification advises that you use ESF with ISDN D-channel signaling. See also *ISDN D-channel signaling*.

ESI—End System Identifier. The ESI is a subfield of the Domain-Specific Part (DSP) of an ATM End System Address (AESA). It uniquely identifies the end system within the specified subnet, and is typically an IEEE Media Access Control (MAC) address. Compare with *HO-DSP*, *SEL subfield*. See also *AESA format*, *DSP*, *MAC address*.

ESP—Encapsulating Security Payload. ESP is an Internet Protocol Security (IPSec) protocol that performs full encryption of the data portion of every packet. The receiving system decrypts the packets before routing them. The encryption/decryption provides the added assurance that packet contents have not been viewed while the packet was in transit. ESP works with the Data Encryption Standard-Cipher Block Chaining (DES-CBC), Triple DES-CBC (3DES-CBC), and 40DES-CBC encryption algorithms. ESP version 2 also works with the Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA1), Message Digest 5–Keyed-Hashing for Message Authentication (MD5-HMAC), and SHA1-HMAC authentication algorithms. Compare with *AH*. See also *3DES-CBC*, *40DES-CBC*, *DES-CBC*, *IPSec*, *MD5*, *MD5-HMAC*, *SHA1*, *SHA1-HMAC*.

ETC—Enhanced Throughput Cellular. An error-correction protocol developed by AT&T Paradyne, Inc. ETC is based on V.32bis, providing a maximum rate of 14,400bps. See also *V.32bis*.

Ethernet—The most commonly used architecture for Local Area Networks (LANs) connecting devices such as computers, printers, and terminals. An Ethernet network uses the Physical and Data Link layers for data transmission. It incorporates a bus topology and can operate at a rate of up to 10Mbps. See also *Data Link layer*, *Physical layer*.

Ethernet II—A protocol specification for the Media Access Control (MAC) header of an IPX frame. Compare with *802.2*, *802.3*, *SNAP*. See also *IPX frame*, *MAC*.

Ethernet address—See *MAC address*.

Ethernet packet—A variable-length unit of data transmitted on an Ethernet LAN. See also *packet*.

Ethernet transceiver—A device that connects workstations to standard 10Base2 or 10Base5 cable. An Ethernet transceiver sends information, receives information, and offers data-packet collision detection. An Ethernet transceiver is also known as a *Medium Access Unit (MAU)*. See also *10Base2, 10Base5*.

ETSI—European Telecommunications Standards Institute. ETSI is a European organization established in 1988 to provide telecommunications standards.

EU-RAW—A WAN encapsulation protocol used primarily in Europe. When you use EU-RAW encapsulation, IP packets are HDLC-encapsulated and include a Cyclic Redundancy Check (CRC). See also *CRC*.

European Telecommunications Standards Institute—See *ETSI*.

EU-UI—A WAN encapsulation protocol used primarily in Europe. When you use EU-UI encapsulation, IP packets are HDLC-encapsulated and include a special header and a Cyclic Redundancy Check (CRC). See also *CRC*.

even parity—See *parity*.

exclusive port routing—A feature that causes a TAOS unit to drop calls for which it has no explicit call-routing information (such as answer numbers and ISDN subaddresses). When exclusive port routing is disabled (the default) and the bearer service is voice, the TAOS unit routes the call to a digital modem. If the bearer service is V.110, the unit routes the call to the first available V.110 module. If the bearer service is data, the unit routes the call to the first available AIM port. If no AIM port is available, the unit routes the call to the bridge/router. See also *answer number*, *call routing*, *subaddress*.

expansion card—See *slot card*.

expansion module—See *slot card*.

expansion slot—See *slot*.

expect-send script—A script whose lines begin with either the `send` or the `expect` command. A line that begins with `send` causes all the other characters on the line to go through the WAN port running the script. A line that begins with `expect` causes the router to wait for matching characters from the WAN port. You can use an expect-send script to authenticate logins to the terminal server, or to start a Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) session from within a terminal-server connection. See also *authentication*, *PPP*, *SLIP*, *terminal mode*.

Explicit Congestion Notification—See *ECN*.

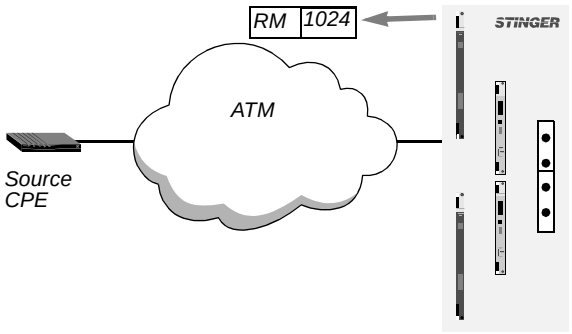
Explicit Forward Congestion Indication—See *EFCI*.

Explicit Forward Congestion Indication marking—See *EFCI marking*.

Explicit Rate marking—A type of flow control employed for Asynchronous Transfer Mode (ATM) Available Bit Rate (ABR) traffic. A source system initially sets the Explicit Rate field to the Peak Cell Rate (PCR) value specified for the connection, or to a lower rate negotiated when the Permanent Virtual Circuit (PVC) is established. If bandwidth is scarce, a TAOS unit sends a lower value in the Explicit Rate field of its forward or reverse Resource Management (RM) cells. When the source system receives an RM cell with a lower Explicit Rate value, it reduces its transmission rate to that value.

Figure 28 shows a TAOS unit setting the Explicit Rate field in reverse RM cells to a lower cell transmission rate for a Virtual Channel Identifier (VCI). The destination system receives the RM cell and slows down its transmission rate to the specified Explicit Rate value.

Figure 28. Flow control for ABR traffic with Explicit Rate marking



See also *RM cell*.

extended AppleTalk network—An AppleTalk Phase 2 network that uses an extended addressing scheme. With extended addressing, AppleTalk uses an 8-bit node number and a 16-bit network number for each host, allowing up to 16 million hosts on one network. See also *AppleTalk*, *AppleTalk routing*.

extended profiling—A feature that enables you to extend the amount of memory used for profiles. When this feature is enabled, twice as many configured profiles can be stored in Nonvolatile Random Access Memory (NVRAM).

Warning: Before enabling extended profiling, you must complete the entire software upgrade process so that both the boot-loader and shelf-controller images support extended profiling. If you enable the feature while one of these images is at a version level that does not support extended profiling, *all profile information will be lost.*

See also *NVRAM*.

Extended SuperFrame—See *ESF*.

Exterior Gateway Protocol—See *EGP*.

external authentication—A remote method of identifying the users permitted to access network resources. The remote server can be a RADIUS, TACACS, TACACS+, or token-card server. See also *RADIUS*, *RADIUS server*, *TACACS*, *TACACS+*, *token-card server*.

External Authentication Server—See *authentication server*.

external LSA—External Link State Advertisement. In an Open Shortest Path First (OSPF) configuration, an external LSA is exchanged between Autonomous Systems (ASs) by Autonomous System Border Routers (ASBRs). Compare with *internal LSA*. See also *AS, ASBR, LSA, OSPF*.

external route—A route imported into the Open Shortest Path First (OSPF) database from outside the router's Autonomous System (AS). Compare with *intra-area route*. See also *AS, OSPF, route*.

external testing—A loopback test that diagnoses the ability of a port to send and receive data. See also *loopback*.

F

Facilities Data Link—See *FDL*.

facility—An optional service offered by an X.25 packet-switching network. The user can request a facility when subscribing to a network service or when establishing a call. See also *X.25*.

fail count—A statistic that displays the number of tests that produced an error condition.

Failure-to-start record—A RADIUS-accounting or call-logging record that contains information about a failed login attempt. See also *Failure-to-start session*.

Failure-to-start session—An event denoting that a login attempt has failed. Information about this event appears in a RADIUS-accounting or call-logging Failure-to-start record.

fallback/fall-forward line sensing—A feature that enables a high-speed analog modem to monitor the quality of the telephone line and to step down to the next-lower speed if the line quality deteriorates. The modem falls forward to the next higher speed as line quality improves. See also *modem*.

fanout—The ability of a Digital Access Cross-Connect (DAC) to split and switch channels between incoming and outgoing circuits. See also *DAC*.

Far-End Block Error—See *FEBE*.

far end cut-through—See *network tone cut-through*.

Fast Ethernet—A LAN transmission standard with a data rate of 100Mbps. A workstation with a 10Mbps (10BaseT) Ethernet card can also be connected to a Fast Ethernet network. See also *10BaseT*.

fatal error—An error that causes the abrupt termination of a program.

Fax Connection Response Packet—See *FCRP*.

fax server—A server that receives fax data over the Internet and transfers the data onto regular telephone lines. See also *IP fax*.

FCRP—Fax Connection Response Packet. A packet that a fax server sends to a TAOS unit in response to an Incoming Fax Authentication Packet (IFAP). An FCRP-NAK indicates that the security code in the IFAP failed authentication. An FCRP-NR indicates that the fax server has a resource problem. An FCRP-ACK indicates that the fax server is ready to receive the fax transmission. See also *fax server*, *IFAP*.

FCS—Frame Check Sequence. In a data frame, a field that contains the standard 16-bit Cyclic Redundancy Check (CRC) for detecting errors in High-Level Data Link Control (HDLC) Frame Relay frames. See also *CRC*, *HDLC*, *LAPD*.

FDDI—Fiber Distributed Data Interface. FDDI is a proposed ANSI standard for a network architecture that uses high-speed fiberoptic lines and supports transmission rates of up to 100Mbps. Compare with *CDDI*. See also *fiberoptic line*.

FDL—Facilities Data Link. An FDL is a 4Kbps digital link between a sender and the telephone company's monitors. The link uses Extended Superframe (ESF) framing. The telephone company uses an FDL to check on the quality and performance of T1 lines. You cannot use FDL reporting on a line configured for D4 framing. See also *ESF*, *T1 line*.

FDM—Frequency Division Multiplexing. FDM is a method of dividing a transmission channel into several parallel paths. All signals are carried simultaneously. Compare with *TDM*.

Feature Group C—See *FGC*.

Feature Group D—See *FGD*.

FEBE—Far-End Block Error. FEBE is a signal the remote end sends to indicate that it has received DS3 or E1 frames with either Framing Errors (FERR) or C-bit Parity Errors (CPERR). A block error is detected each time the calculated checksum of the received data does not correspond to the control checksum transmitted in each successive superframe. One block error indicates that one superframe has not been transmitted correctly. No conclusion with respect to the number of bit errors can be drawn from the block-error counter. Compare with *NEBE*. See also *CPERR*, *DS3 line*, *FERR*.

FECN—Forward Explicit Congestion Notification. FECN is a bit set in a Frame Relay header to notify Data Terminal Equipment (DTE) that there is traffic congestion on the network and that the receiving device should begin congestion-avoidance procedures. Compare with *BECN*. See also *congestion*, *congestion management*, *Frame Relay*.

FERR—Framing Errors. FERR indicates the number of errors in the bits used to frame the DS3 signal. Compare with *CPERR*. See also *DS3 line*.

FGC—Feature Group C. Trunk-side Local Access and Transport Area (LATA) access for AT&T customers, usually between each end office and an AT&T switching system. Compare with *FGD*. See also *LATA*.

FGD—Feature Group D. Trunk-side Local Access and Transport Area (LATA) access that provides call supervision to an interLATA carrier, a uniform access code, optional calling-party identification, access-charge billing details, and subscription to a specified interLATA carrier. FGD is also known as *Equal Access*. Compare with *FGC*. See also *LATA*.

Fiber Distributed Data Interface—See *FDDI*.

fiberoptic line—A transmission medium consisting of thin glass filaments. Light beams travel through the fiberoptic line, carrying large amounts of data over long distances. See also *FDDI*.

FIFO—First-In, First-Out. An algorithm that specifies that the first data that enters a buffer is the first data to be removed from the buffer.

File Transfer Protocol—See *FTP*.

filter—A set of rules describing what action a TAOS unit should take when it encounters certain types of packets. A filter can apply to incoming packets, outgoing packets, or both. A packet filter applies to packets on an interface. A route filter applies to routes in Routing Information Protocol (RIP) update packets. See also *packet filter*, *route filter*.

filter persistence—A method of enabling a firewall to persist across connection-state changes. With filter persistence, the firewall rules stay in force even when a connection goes offline. See also *firewall*.

Finger—A simple protocol that provides access to a Remote User Information Program (RUIP). Using the Finger protocol, the Finger utility can determine whether a particular user is logged in to a certain device, and can gather other information about the user.

firewall—A set of instructions that protects the devices and resources of a private network from intrusion by users outside the network.

First-In, First-Out—See *FIFO*.

flag pattern—A pattern of 1s and 0s (01111110) that a TAOS unit can use as the idle indicator on a call. Compare with *mark pattern*.

flash memory—Nonvolatile memory that does not require batteries to preserve its contents. Flash memory can only be erased and written in blocks, and is less expensive than Nonvolatile Random Access Memory (NVRAM). On a MAX TNT unit or an APX 8000 unit, flash memory is used to store code loads. On a MAX unit, flash memory is used to store the current (compressed) executable and a copy of the current configuration. Compare with *NVRAM*. See also *APX 8000™*, *MAX™*, *MAX TNT®*.

flow control—A method of compensating for differences in the flow of incoming and outgoing data for a modem or other device. If one system receives more data than it can process and its buffers are full, it signals the sender to delay further transmission. Flow control can take place by means of hardware or software. See also *hardware flow control*, *software flow control*.

Foreign Agent—The system at the client end of an Ascend Tunnel Management Protocol (ATMP) tunnel. The mobile client dials in to the Foreign Agent. After authenticating the mobile client, the Foreign Agent establishes an IP connection to the Home Agent, which is on the home network. The Foreign Agent and the Home Agent build a tunnel by encapsulating the IP packets in ATMP. Compare with *Home Agent*. See also *ATMP, L2TP, mobile client, PPTP*.

Forward Explicit Congestion Notification—See *FECN*.

Fractional T1—See *FT1*.

fractional T1 line—A T1 or ISDN BRI line that contains both switched and dedicated channels. See also *dedicated channel*, *ISDN BRI line*, *switched channel, T1 line*.

Fractional T1–Multilink Protocol Plus—See *FT1-MP+*.

FRAD—Frame Relay Access Device. A FRAD provides Frame Relay encapsulation for any HDLC-based protocol. The system can then transport the encapsulated packets over a Frame Relay network. See also *Frame Relay*, *Frame Relay network*, *HDLC*.

frame—In Token Ring and Systems Network Architecture (SNA), a packet at the Data Link layer of the OSI Reference Model. In Frame Relay, a variable-length data unit transmitted as pure data across a Frame Relay network. In Time Division Multiplexing (TDM), a sequence of time slots, each containing a portion of a multiplexed channel. A frame contains source and destination information, flags that designate the start and end of the frame, and information about the integrity of the frame. All other data, such as network protocol information and the actual payload of data, is first encapsulated in a packet. The system then encapsulates the packet in a frame. See also *Data Link layer*, *Frame Relay*, *OSI Reference Model*, *packet*, *TDM*.

Frame Check Sequence—See *FCS*.

framed protocol—A synchronous protocol that encapsulates data into frames. See also *framing*, *protocol*, *synchronous transmission*.

Frame Relay—A WAN architecture originally developed for ISDN lines. A Frame Relay network provides high throughput by handing monitoring functions to higher-level protocols. Frame Relay is a very efficient standard, with a bandwidth of up to 2Mbps. It is ideal for situations in which periods of very high traffic are interspersed with idle periods. Frame Relay is protocol independent. It performs routing over Virtual Circuits (VCs) built with Data Link Connection Identifiers (DLCIs). See also *DLCI*, *FRAD*, *Frame Relay concentrator*, *Frame Relay direct*, *Frame Relay network*, *Frame Relay switch*, *IEC*, *ISDN*, *PVC*.

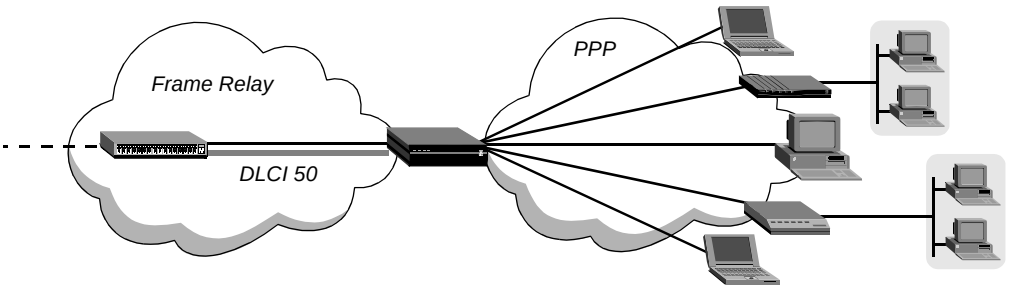
Frame Relay Annex A—The International Telecommunication Union (ITU) standard defining Frame Relay maintenance procedures for Permanent Virtual Circuits (PVCs). ITU Annex A is analogous to the ANSI standard Annex D. See also *Frame Relay Annex D*.

Frame Relay Annex D—Part of the ANSI T1.617 standard. Annex D defines maintenance procedures that apply to Permanent Virtual Circuits (PVCs). Before ANSI standard T1.617 Annex D, a group of companies defined the Link Management Interface (LMI) mechanism for PVC management. The LMI specifies functionality similar to that defined by the ANSI standard, and is still widely supported. ANSI Annex D is analogous to the International Telecommunication Union (ITU) standard Annex A. See also *Frame Relay*, *Frame Relay Annex A*, *LMI*, *PVC*.

Frame Relay Access Device—See *FRAD*.

Frame Relay concentrator—A device that concentrates many low-speed, dial-in connections into one high-speed, dedicated connection to a Frame Relay switch. As a Frame Relay concentrator, a TAOS unit forwards many lower-speed PPP connections onto one or more high-speed Frame Relay interfaces, as shown in Figure 29.

Figure 29. Frame Relay concentrator

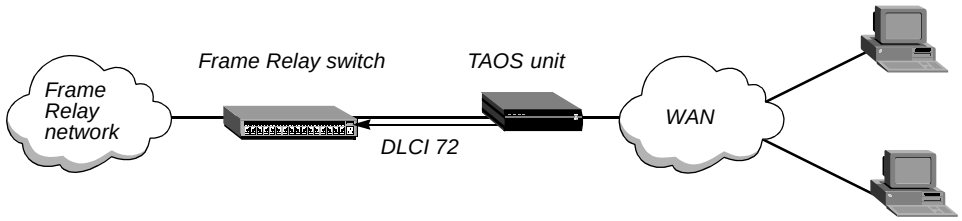


In this kind of configuration, the decision to forward frames onto the Frame Relay interface can be made at OSI Layer 3 (using IP routing), or by Frame Relay direct. Compare with *Frame Relay switch*. See also *Frame Relay, Frame Relay direct, Frame Relay network, IP routing.*

Frame Relay direct—A Frame Relay connection in which a TAOS unit ignores the destination IP address in a packet from a dial-in PPP client and instead uses the Data Link Connection Identifier (DLCI) to route the packet instead. The TAOS unit does not route packets from the client in the usual sense. It simply passes them on to the Frame Relay network and assumes that another device will route the packets on the basis of the destination IP address.

Figure 30 shows two incoming PPP connections redirected out to the Frame Relay network. Both direct connections (shown at the right of Figure 30) use the same DLCI number (72).

Figure 30. Frame Relay direct connections using the same DLCI



A Frame Relay direct connection is not a full-duplex tunnel between the PPP dial-in device and the switch. The TAOS unit's router handles the IP packets coming back from the Frame Relay switch, so the packets must contain the PPP caller's IP address for proper routing back across the WAN. See also *DLCI, Frame Relay, Frame Relay network, Frame Relay switch, IP address, PPP.*

Frame Relay link management—A feature that enables you to retrieve information about the status of the Frame Relay interface by means of special management frames with a unique Data Link Connection Identifier (DLCI) address. (DLCI 0 is the default for link-management frames.) On a User-to-Network Interface (UNI) to Frame Relay, link-management procedures occur in one direction. The UNI-DTE device requests information, and the UNI-DCE device provides it. On a Network-to-Network Interface (NNI), link-management procedures are bidirectional. Switches perform both the DTE and DCE link-management functions, because both sides of the connection request information from their peer switches. See also *DLCI, Frame Relay network, NNI, UNI, UNI-DCE interface, UNI-DTE interface*.

Frame Relay multicasting—A feature that enables a device to forward a frame on a particular Data Link Connection Identifier (DLCI) into the Frame Relay network. The Frame Relay network sends the frame to a list of destinations defined by the network manager.

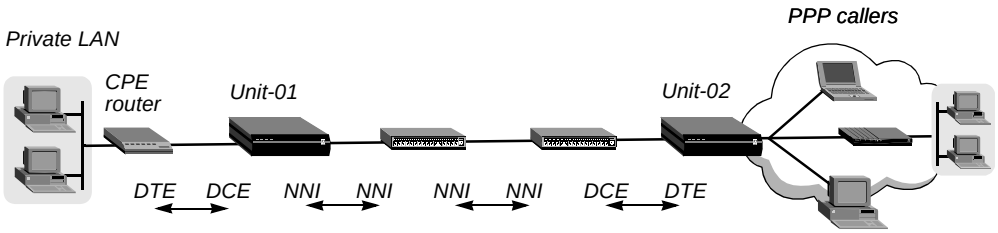
Frame Relay multicasting provides a point-to-multipoint frame delivery service. This service is connection oriented. To send multicast data, the network manager must first create individual Permanent Virtual Circuits (PVCs) to the destination sites from the site that sends the broadcasts. After defining the PVCs, the network manager must establish a multicast group. A multicast group consists of a multicast DLCI with a list of the member PVC DLCIs participating in a multicast communication. The multicast group is a logical entity providing multicast service to all members. Compare with *IP multicast forwarding*. See also *DLCI, Frame Relay, Frame Relay network, PVC.*

Frame Relay network—A network in which every access point connects directly to a Frame Relay switch for the transmission of multiplexed data. Depending on how a device such as a TAOS unit is integrated into the Frame Relay network, the device can operate as a Frame Relay terminating unit (Customer Premises Equipment, or CPE) or as a Frame Relay switch.

A CPE device is the source or destination of data traversing the Frame Relay service. For example, the TAOS unit labeled Unit-02 in Figure 31 is the source and destination of the data stream from its PPP callers. When it is configured with a User-to-Network Interface (UNI) to Frame Relay, the TAOS unit acts as the user side (UNI-DTE) communicating with the network side (UNI-DCE) of a switch.

A network-side device connects the CPE device to a Frame Relay network. For example, the unit labeled Unit-01 in Figure 31 receives Frame Relay encapsulated frames from a CPE device and forwards them on to another Frame Relay switch. When it is configured with a UNI-DCE interface, the TAOS unit acts as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device.

Figure 31. Frame Relay network



A Frame Relay switch is another kind of network-side device. It switches frames from one interface to another and exchanges status information with its peer switch. For example, the unit labeled Unit-01 in Figure 31 receives frames from its peer switch and switches them to its other Frame Relay interface. When it is configured with a Network-to-Network Interface (NNI) to Frame Relay, the TAOS unit acts as a Frame Relay switch. Switch-to-switch communication includes both user-side (NNI-DTE) and network-side (NNI-DCE) functions.

See also *CPE, FRAD, Frame Relay, Frame Relay concentrator, Frame Relay direct, Frame Relay switch, NNI, UNI, UNI-DCE interface, UNI-DTE interface.*

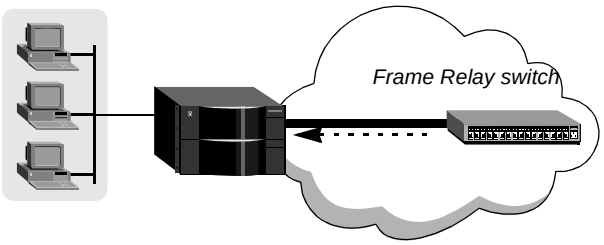
Frame Relay Permanent Virtual Circuit—See *Frame Relay PVC.*

Frame Relay PVC—Frame Relay Permanent Virtual Circuit. A Frame Relay PVC is a logical link on a Frame Relay network. It consists of the Frame Relay address and Data Link Connection Identifier (DCLI) of both the interface that initiates the PVC and the interface that terminates it. Compare with *Frame Relay SVC.* See also *Frame Relay, VC.*

Frame Relay SVC—Frame Relay Switched Virtual Circuit. A Frame Relay SVC is a point-to-point switched connection, which provides a lower cost, usage-based alternative to Permanent Virtual Circuits (PVCs). In addition, a Frame Relay SVC provides an easier configuration for Virtual Circuits (VCs) throughout a Frame Relay network, and allows flexibility in rerouting VCs when equipment becomes unavailable. Like other types of switched connections, SVCs can be initiated by a dial-in or dial-out call.

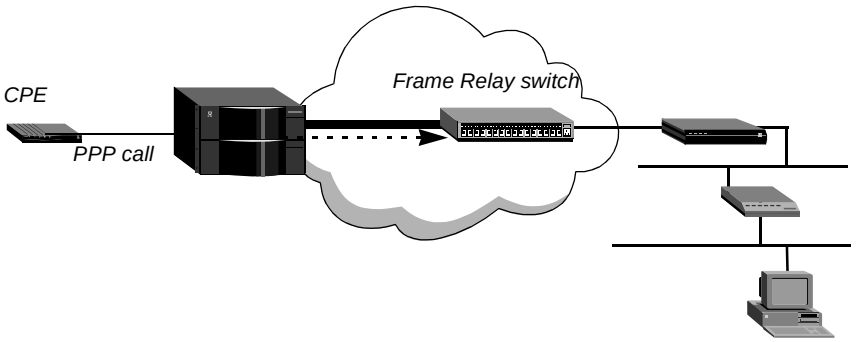
A dial-in Frame Relay SVC terminates locally. The TAOS unit receives the call on a Frame Relay interface (a data link). Figure 32 shows an example of a terminating SVC.

Figure 32. Terminating SVC on a Frame Relay interface



A dial-out SVC is initiated as an outgoing call on a Frame Relay interface, on the basis of either an explicit dial-out or IP routing. Figure 33 shows a Pipeline unit, using PPP or some other type of encapsulation, dialing in to a MAX TNT unit. The MAX TNT unit establishes the incoming call and then dials out on a Frame Relay interface on the basis of IP routing, just as it would for another type of switched dial-out call.

Figure 33. Dial-out SVC on a Frame Relay interface



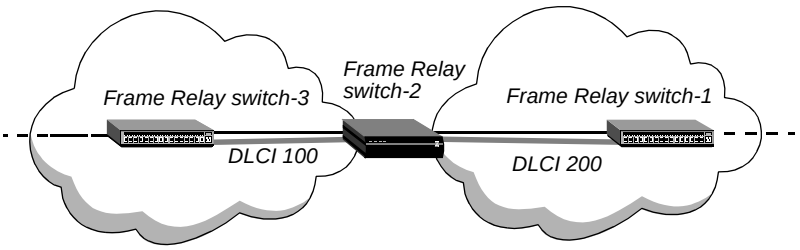
Unlike PVCs, which are dedicated connections, SVCs are on-demand connections and must use E.164 addresses (ISDN numbers) to identify and route to the SVC interface. Compare with *Frame Relay PVC*. See also *Frame Relay, VC*.

Frame Relay switch—A device that sends Frame Relay data out to the Frame Relay network. As a Frame Relay switch, a TAOS unit receives frames on one interface and transmits them on another interface. The decision to forward frames onto the Frame Relay interface is made at OSI Layer 2. The TAOS unit's router software is not involved.

To use a TAOS unit as a switch, you must configure a circuit that pairs two Frame Relay interfaces. Instead of using Layer 3 routing logic to select the interface on which to forward the frames, the unit relies on the circuit configuration to relay the frames received on one interface to its paired interface.

Figure 34 shows a TAOS unit operating as a Frame Relay switch.

Figure 34. Frame Relay switch



Compare with *Frame Relay concentrator*. See also *Frame Relay*, *Frame Relay network.*

Frame Relay Switched Virtual Circuit—See *Frame Relay SVC.*

Frame Relay–to–ATM switching—A procedure that converts Frame Relay encapsulation (defined in RFC 1490) to ATM Adaptation Layer 5 (AAL 5) encapsulation (defined in RFC 1483). The conversion is described in the Frame Relay Forum FRF-5 implementation agreement. A TAOS unit can receive frames on a Frame Relay Data Link Connection Identifier (DLCI) interface and transmit them on an ATM Permanent Virtual Circuit (PVC), and vice versa. The decision to forward frames is based on circuit-name assignments. When the TAOS unit receives a frame on an ATM-Frame Relay circuit end point, it removes the frame's encapsulation and adds the encapsulation required by the other end point. See also *AAL*, *ATM*, *DLCI*, *Frame Relay*, *Frame Relay network*, *PVC.*

Frame window size—See *Level 2 Window Size*.

framing—At the Physical and Data Link layers of the OSI model, a method of fitting bits into a unit called a *frame.* A frame contains source and destination information, flags that designate the start and end of the frame, and information about the integrity of the frame. All other data, such as network protocol information and the actual payload of data, is first encapsulated in a packet. The system then encapsulates the packet in a frame. See also *Data Link layer*, *encapsulation*, *OSI Reference Model*, *packet*, *Physical layer*.

Framing Errors—See *FERR.*

Frequency Division Multiplexing—See *FDM.*

FT1—Fractional T1. FT1 is a type of call that consists entirely of dedicated channels. The call connects to a Terminal Adapter (TA), Channel Service Unit (CSU), or Data Service Unit (DSU) over fractional T1 or other dedicated circuits. See also *CSU*, *dedicated line*, *DSU*, *fractional T1 line*, *FT1-AIM*, *FT1-B&O*, *FT1-MP+*, *TA.*

FT1-AIM—Fractional T1-Ascend Inverse Multiplexing. FT1-AIM is a type of call in which a TAOS unit combines dedicated channels with switched channels to achieve the required bandwidth. An FT1-AIM call uses the AIM protocol, and is available only on host ports equipped with AIM functionality. Both ends of the call must have AIM-compatible equipment. When the quality of a dedicated channel in an FT1-AIM call falls to Marginal or Poor, the TAOS unit drops the channel and does not replace it. The unit cannot monitor these channels or restore them to an online call. See also *FT1*, *FT1-B&O*, *FT1-MP+*.

FT1-B&O—Fractional T1-Backup and Overflow. FT1-B&O is a type of call that provides automatic protection of dedicated circuits.

In providing backup bandwidth, the TAOS unit drops all the dedicated channels when the quality of any one dedicated channel falls to Marginal or Poor. The unit then attempts to replace the dropped dedicated channels with switched channels. The unit also monitors dropped dedicated channels. When the quality of all dropped channels changes to Fair or Good, the TAOS unit reinstates them.

In providing overflow protection, a TAOS unit supplies supplemental dial-up bandwidth during times of peak demand in order to prevent saturation of a dedicated line. The circuit remains in place until the traffic subsides, and then it is removed.

The backup and overflow feature uses the Ascend Inverse Multiplexing (AIM) protocol, and is available only on host ports equipped with AIM functionality. Both ends of the call must have AIM-compatible equipment. You must limit calls of this type to 28 channels. See also *FT1*, *FT1-AIM*, *FT1-MP+*.

FT1-MP+—Fractional T1–Multilink Protocol Plus. An FT1-MP+ connection begins as a dedicated connection, but can later use switched channels, either to increase bandwidth or to provide a backup if the dedicated channels go offline. When a dedicated connection is temporarily down, the TAOS unit polls continuously while trying to reestablish the link. If an outgoing packet arrives while the dedicated connection is still down, the unit replaces the dedicated channel with a switched channel. See also *fractional T1 line*, *MP+*.

FTP—File Transfer Protocol. FTP is an Application-layer protocol that enables you to transfer files from one device to another over a network. See also *Application layer*, *FTP server*.

FTP server—A server that a user can contact in order to transfer files by means of the File Transfer Protocol (FTP) over a TCP/IP network.

full duplex—A type of communications configuration in which data can be transmitted in both directions at the same time. Compare with *half duplex.*

Full Rate Global System for Mobile Communication Voice Encoder/Decoder—See *Full Rate GSM VoCoder*.

Full Rate GSM VoCoder—Full Rate Global System for Mobile Communication Voice Encoder/Decoder. A voice encoder/decoder standard for cellular communications. The Full Rate GSM VoCoder compresses speech samples from 64Kbps to 13.2Kbps. It is the standard used by European, Japanese, and Australian cellular communications systems. Full Rate GSM uses a speech-frame size of 160 samples (20ms). The encoder produces 33 bytes per frame, while the decoder produces 160 samples (20ms) of speech from the 33-byte encoder output. See also *GSM*.

full status reporting—In Frame Relay, a link-management message function that provides the user device with the complete status of all Permanent Virtual Circuits (PVCs) configured on the link. See also *Frame Relay*, *PVC*.

G

G.703—A standard specifying the physical and electrical characteristics of digital devices, including those operating at 64Mbps and 2.048Mbps.

G.711 A-Law—See *A-Law*.

G.711 audio codec—An audio codec that transmits 3.4kHz voice at 56Kbps and 64Kbps. A G.711 audio codec is suitable for high-bandwidth environments. See also *audio codec*, *codec*.

G.711 U-Law—See *U-Law*.

G.723—An International Telecommunication Union (ITU) standard for compressing voice data at 5.3Kbps and 6.3Kbps.

G.728 codec—A Low-Delay Code Excited Linear Prediction (LD-CELP) based audio codec that provides toll-quality audio at a bit rate of 16Kbps. With a frame size of only 2.5 milliseconds, G.728 has a very low delay. Although the MultiVoice implementation of G.728 uses a frame size of 5 milliseconds, the bit stream from the audio codec is the same as described in the ITU-T standard and can thus be decoded by any G.728 decoder. See also *audio codec*, *codec*, *MultiVoice™*.

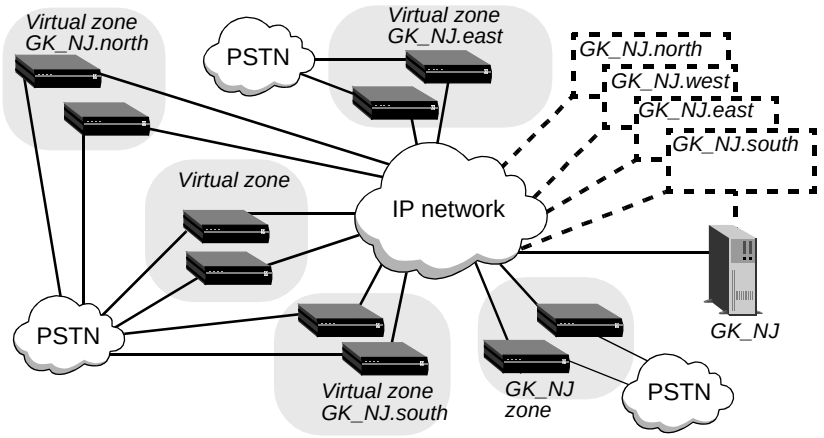
G.729—An International Telecommunication Union (ITU) 8Kbps Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP) speech compression algorithm.

gatekeeper—A device that manages an IP network, supporting all gateways, user profiles, and authentication. A gatekeeper is defined by the H.323 standard. See also *gateway*, *H.323*, *MultiVoice™*, *MVAM*, *MultiVoice™ Gatekeeper*, *MultiVoice™ Gateway*.

gatekeeper virtual zone—A subset of all MultiVoice gateways that are administered and registered with a single MultiVoice Access Manager (MVAM) application. Each virtual zone is managed by a virtual gatekeeper that exists on the same server as the MVAM implementation. Each virtual gatekeeper has its own set of distinct gateway, gatekeeper, and user databases that are separate and distinct from the other databases maintained for the MVAM application itself, or for other virtual gatekeepers that exist on the same server.

Figure 35 shows an example of a MultiVoice network using an MVAM implementation with gatekeeper virtual zones.

Figure 35. Example of a MultiVoice network using gatekeeper virtual zones



Each group of MultiVoice gateways interacts with each gatekeeper virtual zone as thought it were a single gatekeeper. In this instance, MVAM has four gatekeeper virtual zones, in addition to the one "real" H.323 zone. See also *MultiVoice™*, *MVAM*.

gateway—A device or program that provides mapping at all seven layers of the OSI model, and translates between two otherwise incompatible networks or network segments to facilitate traffic between data highways of different architectures. See also *OSI Reference Model*.

Also, a device that connects the Public-Switched Telephone Network (PSTN) to an IP network. A caller dials a local gateway, and the gateway provides access to the IP network and destination device. A gateway is defined by the H.323 standard. See also *gatekeeper*, *H.323*, *MultiVoice™*, *MVAM*, *MultiVoice™ Gateway*.

gateway Home Agent—In an Ascend Tunnel Management Protocol (ATMP) configuration, a Home Agent that tunnels packets from the Foreign Agent to the home network across an open WAN connection. The WAN connection must be online. The gateway Home Agent does not establish a WAN connection to the home network in response to a packet it receives through the tunnel. For this reason, the gateway Home Agent must have a dedicated WAN connection to the home network. Compare with *router Home Agent*. See also *ATMP*, *dedicated circuit*, *Foreign Agent*, *Home Agent*, *home network*.

Gbps—An acronym meaning gigabits (one billion bits) per second, and a measure of the capacity of a device.

GCAC—Generic Connection Admission Control. A process that determines whether a link has sufficient resources to support an Asynchronous Transfer Mode (ATM) connection. See also *ATM*.

G.DMT—A type of Asymmetric Digital Subscriber Line (ADSL) technology that provides a maximum downstream data rate of 8Mbps and a maximum upstream data rate of 1.544Mbps. The G.DMT standard is based on Discrete MultiTone (DMT) modulation. See also *ADSL*, *DMT*.

general frame—On an X.25/T3POS network, a frame defined as any sequence of octets received from or sent to the Data Terminal Equipment (DTE) within the period specified by the Char-to-Char timer. (A general frame is also known as a *data frame*.) In Local and Binary Local modes, and in opening frames, general frames are encapsulated in the following format:

`STX [data] ETX XRC`

where:

- `STX` is the ASCII character \002.
- *`data`* is the user data being sent in the frame.
- `ETX` is the ASCII character \003.
- `XRC` is the checksum. For all modes except Binary Local, the checksum is a one-character Longitudinal Redundancy Check (LRC) checksum. For Binary Local mode, the checksum is a two-character Cyclic Redundancy Check (CRC) checksum.

Compare with *Control frame*, *I-frame*. See also *Binary Local mode*, *Blind mode*, *Char-to-Char timer*, *CRC*, *DTE*, *LRC*, *X.25/T3POS*.

Generic Connection Admission Control—See *GCAC*.

generic filter—A packet filter that examines the byte- or bit-level contents of a packet and compares them with a value defined in the filter. To use a generic filter effectively, you need to know the contents of certain bytes in the packets you want to filter. Protocol specifications are usually the best source of such information. Compare with *IP filter*, *IPX filter*, *TOS filter*. See also *call filter*, *data filter*, *packet filter*.

Generic Flow Control—See *GFC*.

Generic Routing Encapsulation—See *GRE*.

GFC—Generic Flow Control. GFC denotes the field in the Asynchronous Transfer Mode (ATM) cell that controls the flow of traffic across the User-to-Network Interface (UNI) and into the network. See also *ATM*, *UNI*.

GGP—Gateway-to-Gateway Protocol. GGP is a TCP/IP protocol that transfers routing information between gateways. See also *gateway*, *TCP/IP*.

GHz—Gigahertz. GHz is a unit of wave frequency equal to one billion hertz (1,000,000,000Hz). In some computers, microprocessor clock speed is measured in GHz. Personal computer clock speeds are generally a few tenths of a GHz, but are increasing toward 1GHz.

gigabyte—A data measurement unit equal to 1,073,741,824 bytes, or 1024 megabytes.

glare—A signal that the switch sends when you attempt to place an outgoing call and to answer an incoming call simultaneously.

global hunt-group number—A telephone number that spans all the T1 channels of all the TAOS units in a stack. The telephone company has set up the global hunt group to distribute incoming calls equally among TAOS units.

global IP address pool—A pool used by several TAOS units for dynamically allocating IP addresses to dial-in clients. By default, each TAOS unit handles dynamic IP address allocation from a pool of addresses individually assigned to it. However, you can also set up RADIUS to allocate IP addresses from a global pool that many units share. To do so, you must install RADIPAD, the central manager for global IP address pools on a network. Although multiple hosts can run the RADIUS daemon, only one host on the network should run RADIPAD. See also *dynamic IP*, *IP address pool*, *RADIPAD*, *RADIUS*, *RADIUS daemon*.

Global System for Mobile Communication—See *GSM*.

global VRouter—A group of all the IP or IPX interfaces that are not explicitly grouped with a defined VRouter. See also *VRouter*.

GloBanD—A European data service consisting of a single circuit whose bandwidth is a multiple of 64Kbps. The circuit consists of one or more B channels. For example, if a caller requests 512Kbps service, the line uses eight B channels to supply the requested bandwidth. GloBanD service is available over T1 PRI lines only. It differs from MultiRate in being an overlay network, rather than an integral part of the worldwide switched digital infrastructure. See also *bandwidth*, *B channel*, *MultiRate*, *T1 PRI line.*

GMT—Greenwich Mean Time. This term has been changed to *Coordinated Universal Time (UTC)*. See *UTC*.

graceful discard—A feature that turns red frames into best-effort frames. If you do not enable this feature, the system discards some frames. See also *best-effort packets*, *red frame*.

GRE—Generic Routing Encapsulation. GRE provides a simple, general-purpose mechanism for encapsulating an arbitrary Network-layer protocol in another arbitrary Network-layer protocol. When a system needs to route data, it first encapsulates the information in a GRE packet. The system then encapsulates the GRE packet in a protocol supported by the network and forwards the packet to its destination.

green frame—A type of frame that the Frame Relay network never discards, except under extreme congestion conditions. If the number of bits received during the current time interval (Tc), including those in the current frame, is less than the value of the Committed Burst (Bc) size, the frame is designated as a green frame.

Congested nodes that must discard packets use the color designations to determine which frames to discard. Red frames are discarded first, followed by amber frames, and then green frames. Compare with *amber frame*, *red frame*. See also *Bc*, *Frame Relay*, *Tc*.

Greenwich Mean Time—This term has been changed to *Coordinated Universal Time (UTC)*. See *UTC*.

ground-start signaling—A signaling method in which the Customer Premises Equipment (CPE) transmits an off-hook condition by creating a zero-voltage condition. Compare with *loop-start signaling*, *wink-start signaling*.

group address—An address that enables a Switched Multimegabit Data Service (SMDS) data unit to be delivered to multiple Subscriber Network Interfaces (SNIs). Compare with *individual address*. See also *SMDS*, *SNI*.

GSM—Global System for Mobile Communication. GSM is the most commonly used digital wireless telephone technology. It performs analog-to-digital (A-D) conversion, compressing data and transmitting it on a channel with two other data streams, each in its own time slot. Compare with *CDMA*. See also *wireless technology*.

GSM 1900—Also known as *PCS 1900* or *DCS 1900*, one of the three Personal Communications Services (PCS) technologies in North America. GSM is the only one that provides data services and allows movement between North America and Europe. Omnipoint, Pacific Bell, BellSouth, Sprint Spectrum, Microcell, Western Wireless, Powertel, and Aerial all support GSM 1900.

guaranteed packets—Data delivered with high reliability within a specified time constraint.

H

H channel—An ISDN channel comprised of multiple B channels. See also *H0 channel, H11 channel, H12 channel*.

H0 channel—In the Switched-384 data service, a circuit combining six B channels for a data rate of 384Kbps. See also *B channel, Switched-384.*

H0 data service—See *Switched-384.*

H11 channel—In the Switched-1536 data service, a circuit combining 24 B channels for a data rate of 1536Kbps. See also *B channel, Switched-1536.*

H11 data service—See *Switched-1536*.

H12 channel—A circuit combining 30 B channels for a data rate of 1920Kbps.

H.221—An International Telecommunication Union (ITU) standard that defines inverse multiplexing for videoconferencing systems. Compare with *H.261*. See also *ITU*.

H.225—An International Telecommunication Union (ITU) standard for setting up connections between H.323 end points. H.225 call signaling occurs when end points exchange H.225 protocol messages over a reliable call-signaling channel. See also *ITU*.

H.245—An International Telecommunication Union (ITU) standard that specifies how to establish logical channels for the transmission of audio, video, and data. See also *ITU*.

H.261—An International Telecommunication Union (ITU) standard that defines a method of digitally encoding and decoding video images, enabling different types of videoconferencing systems to interoperate. Compare with *H.221*. See also *ITU*.

H.323—A set of International Telecommunication Union (ITU) standards that define a framework for the transmission of real-time voice communication over IP-based packet-switched networks. Created in response to customers who needed to use their existing IP networks to support voice communications, the H.323 standards define a gateway and a gatekeeper. See also *gatekeeper, gateway, ITU, MultiVoice™, MVAM, MultiVoice™ Gatekeeper, MultiVoice™ Gateway*.

H.330—A set of International Telecommunication Union (ITU) standards that define a method of enabling videoconferencing systems from different manufacturers to interoperate. See also *ITU*.

half duplex—A type of communication in which data can be transmitted in only one direction at a time. Compare with *full duplex.*

handing off—See *cell switching*.

handshaking—The process of exchanging signaling information between two communications devices in order to establish the manner and speed of data transmission. You can use either hardware handshaking or software handshaking. See also *hardware handshaking, software handshaking*.

hardware address—An address assigned by the hardware manufacturer and unique to a device.

hardware flow control—A method of flow control that uses separate wires in the modem cable to signal stop and start requests between two directly connected systems. Compare with *software flow control*. See also *flow control*.

hardware interface—A hardware link between two devices. A hardware interface has electrical, physical, and functional specifications that determine how two devices communicate. An electrical specification defines the characteristics of the electrical signals. A physical specification might define the number of pins and wires required, and the order in which the pins and wires are laid out. The functional specification describes how the hardware interprets the electrical signals. Examples of commonly used hardware interfaces are RS-232 and V.24. See also *interface*, *RS-232*, *V.24*.

hardware handshaking—A method of synchronizing data transmissions by using the Request To Send (RTS) and Clear To Send (CTS) signals on a wire. Compare with *software handshaking*. See also *CTS*, *handshaking*, *RTS*.

hash value—A number generated from a text string in such a manner that the result would not be the same for any other text string. A system can use a hash value to ensure that data has not been tampered with during transmission. The sending device generates a hash value for the data, encrypts it, and sends it with the data itself. The receiving device decrypts the data and the hash value, generates another hash value from the data, and compares the two hash values. If the hash values are identical, it is unlikely that the data was tampered with. See also *MD5-HMAC*, *SHA1*, *SHA1-HMAC*.

Hayes-compatible modem—Any modem that recognizes commands in the AT command set. See also *AT command set*, *modem*.

HCS—Header Check Sequence. An HCS is an eight-bit Cyclic Redundancy Check (CRC) in an Asynchronous Transfer Mode (ATM) cell.

HDLC—High-Level Data Link Control. HDLC is a synchronous, bit-oriented Data Link layer protocol for data transmission. Frame Relay is an example of an HDLC-based packet protocol. HDLC offers half- or full-duplex communications over circuit- or packet-switched networks, allows point-to-point and multipoint configurations, and provides transmission over both wires and wireless media. See also *circuit switching*, *Data Link layer*, *Frame Relay*, *full duplex*, *half duplex*, *multipoint link*, *packet-switched network*, *point-to-point link*.

HDLC-NRM—High-Level Data Link Control-Normal Response Mode. HDLC-NRM is a link-layer encapsulation protocol similar to the Link Access Procedure, Balanced (LAPB) protocol and other Layer 2 HDLC protocols. When it receives an HDLC-NRM call on a Short-Duration Transaction Network (SDTN), the system authenticates the call by means of Calling-Line ID (CLID) or Dialed Number Information Service (DNIS). If the call passes authentication, the system answers it, completes HDLC negotiations, and forwards the packets to its Quick Transaction Protocol (QTP) software, which routes the packets by means of User Datagram Protocol (UDP) to a transaction server.

Unlike LAPB, in which the connected stations are peers and each has the right to send data at any time, HDLC-NRM is a half-duplex protocol, so only one station is allowed to send data at a time. To enable this feature, one of the connected stations is the primary station, and the other is the secondary station. The primary station can send data packets at any time. The secondary station must be polled before it can send data packets as synchronous I-frames.

See also *CLID*, *DNIS*, *HDLC*, *LAPB*, *QTP*, *SDTN*, *UDP*.

HDSL—High-Bit-Rate Digital Subscriber Line. HDSL is a symmetric DSL technology that enables modems on either side of copper twisted-pair wires to transmit data at a rate of 1.5Mbps each way over two telephone lines or 2Mbps each way over three telephone lines. T1 data rates require two lines. E1 data rates require three lines. Compare with *ADSL*, *IDSL*, *RADSL*, *SDSL*, *VDSL*. See also *DSL*.

header—The initial portion of a data block, packet, or frame. The header provides basic information about the handling of the data portion of the block, packet, or frame.

Header Check Sequence—See *HCS*.

Header Error Control—See *HEC*.

heartbeat polling process—An exchange of sequence numbers between a network and a user device. The Link Management Interface (LMI) exchanges this information by means of DLCI 1023 at both ends of the link. The user device initiates the link-management polling process by sending a Status Enquiry message. Using a Link Integrity Verification Report, as well as a Full Status Report about the status of all Permanent Virtual Circuits (PVCs), the polling process provides information about the user device's physical connection to the network. See also *DLCI*, *LMI*, *PVC*.

HEC—Header Error Control. In the fifth byte of an Asynchronous Transfer Mode (ATM) cell, a field that provides protection against the misdelivery of cells with address errors. Using HEC, an ATM device can check for multiple errors and correct a single bit error in the header. See also *ATM*.

Hello—A routing protocol that enables packet switches to discover routes that have minimal delays. See also *Hello interval*, *Hello packet*.

Hello interval—The number of seconds between sending Hello packets on an interface. See also *Hello packet*.

Hello packet—A packet sent periodically to verify that the device sending the packet is operational. See also *Hello interval*.

hertz—See *Hz*.

heterogeneous network—A network that consists of workstations, servers, network interface cards, operating systems, and applications from many different vendors, all operating together as a single unit. Compare with *homogeneous network*.

hierarchical routing—A routing scheme based on a hierarchy of elements. For example, IP routing is based on a two-tier hierarchy in which the address contains a network number and a host number. See also *IP routing*.

High-Bit-Rate Digital Subscriber Line—See *HDSL*.

High-Level Data Link Control—See *HDLC*.

High-Level Data Link Control-Normal Response Mode—See *HDLC-NRM*.

High-Order Domain-Specific Part—See *HO-DSP*.

High-Speed Serial Interface—See *HSSI*.

HMP—Host Monitoring Protocol. HMP is a protocol for collecting information from hosts on various networks, including servers, workstations, switches, and gateways. Using HMP, a device can monitor hosts both on the Internet and on a private network.

HO-DSP—High-Order Domain-Specific Part. The HO-DSP is a subfield of the Domain-Specific Part (DSP) of an ATM End System Address (AESA). It specifies a segment of address space assigned to a particular device or network. Compare with *ESI*, *SEL subfield*. See also *AESA format, DSP*.

Home Agent—A TAOS unit that represents the terminating part of an Ascend Tunnel Management Protocol (ATMP) tunnel. The Home Agent must be able to communicate with the home network directly, through another router, or across a dedicated WAN connection. See also *ATMP*, *dedicated circuit, home network, router*.

home gateway—The end point of a Layer 2 Forwarding (L2F) tunnel. The home gateway transmits outgoing calls and receives incoming calls from a Network Access Server (NAS). See also *L2F*.

home network—A private corporate network in an Ascend Tunnel Management Protocol (ATMP) configuration. A private network is one that cannot communicate directly on the Internet (for example, an IP network with an unregistered network number). See also *ATMP*, *IP network, IP network number*.

home server proxy—See *SAP home server proxy*.

homogeneous network—A network that consists of one type of workstation, server, network interface card, and operating system, with a limited number of applications, all purchased from a single vendor. All nodes use the same protocol and the same control procedures. Compare with *heterogeneous network*.

hop—A single message or packet transmission between a host and a router, or between two routers. See also *hop count*, *host*, *router*.

hop count—The number of routers through which a packet passes to get from its source to its destination. See also *hop*, *host*, *router*.

host—A computer on a network, also called a *node* or a *station*.

host address—The IP address of a node on a network. See also *IP address*.

host card—A slot card that terminates incoming calls. Compare with *network card*. See also *dual-capacity card, host device, slot card*.

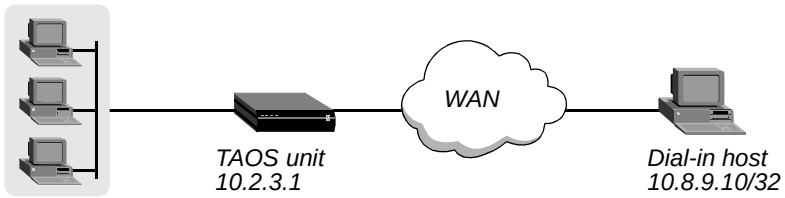
host device—An individual modem or channel on a host card. See also *host card*.

Host Monitoring Protocol—See *HMP*.

host number—The portion of an IP address that denotes an individual node on a network. The class of an IP address determines which portion of the address belongs to the network number and which portion belongs to the host number. See also *IP address, IP network number*.

host route—An IP address with a subnet mask of 255.255.255.255, representing a single host rather than a remote router. A host route requires a static IP address. Figure 36 shows a sample connection in which a dial-in host with an ISDN modem card calls into a TAOS unit and requires a static address for a host route.

Figure 36. Dial-in host requiring a static IP address (a host route)



See also *host, route, router, subnet mask*.

host-route connection—A connection that enables a dial-in host to keep its own IP address when logging in to an IP network. See also *host route*.

host-side address—The interface address of the device that terminates the WAN circuit for an incoming call to a TAOS unit. An analog-encoded call handled by a digital modem and a digital call handled by an HDLC circuit are two examples of a route to a host-side address. Compare with *network-side address*.

host-side port—A port on the device that terminates the WAN circuit for an incoming call to a TAOS unit.

hot swappable—A feature that enables a user to add, replace, or remove interface processors without interrupting the operations of the device.

HSSI—High-Speed Serial Interface. HSSI is a serial interface that operates at speeds of up to 52Mbps and at distances of up to 50 feet. It is similar to the RS-232 and V.35 serial interfaces, but operates at a higher speed. See also *RS-232, V.35*.

HTTP—Hypertext Transfer Protocol. HTTP enables Internet users to request, receive, and provide documents on the World Wide Web.

hub—A device that serves as a termination point for multiple hosts, sending signals onto the proper paths. Typically, a hub contains four to eight connectors. In addition to providing connectors for hosts, many hubs include connectors that you can use to link one hub to another. See also *active hub, passive hub, smart hub*.

hunt group—A group of channels that share the same telephone number. When a call comes in using the telephone number assigned to the hunt group, the switch hunts for an available channel in the group. See also *channel*, *switch*.

hybrid LAN—A network in which some links are capable of sending and receiving analog signals, while others handle digital signals. See also *analog signal*, *digital signal*.

Hypertext Transfer Protocol—See *HTTP*.

Hz—Hertz. Hz is the measure of a signal's frequency, in cycles per second.

I

IAB—Internet Architecture Board. Part of the Internet Society, the IAB oversees technical innovation on the Internet. The IAB supervises a number of committees, including the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the Internet Assigned Numbers Authority (IANA), and the Internet Registry. See also *IANA*, *IETF*, *Internet Registry*, *IRTF*.

IAD—Integrated Access Device. An IAD is a device that plugs into a computer through an Ethernet connection, and to an analog telephone, fax machine, or answering machine through an analog port. The IAD supports all the communication devices in a home office using a single ISDN line. The ISDN line replaces multiple analog lines while providing improved speed and throughput. The IAD also supports bridging and dynamic bandwidth management. A Pipeline 85 unit is an example of an IAD. See also *ISDN line*.

IAM—Initial Address Message. An IAM is a message sent by an SS7 network to a signaling gateway. See also *signaling gateway*, *SS7 network*.

IANA—Internet Assigned Numbers Authority. The IANA is the part of the Internet Society responsible for assigning IP addresses to new Points of Presence (POPs). See also *Internet Society*, *POP*.

ICD—International Code Designator. The ICD is a two-byte portion of an ATM End System Address (AESA) and identifies an international organization. See also *AESA format*.

ICD AESA format—International Code Designator ATM End System Address format. In ICD AESA format, the ICD is specified in the address, identifying an international organization. The British Standards Organization administers these values. Compare with *Custom AESA format*, *DCC AESA format*, *E.164 AESA format*. See also *AESA format*.

ICD for Softswitch—Internet Call Diversion for Softswitch. ICD for Softswitch is a standards-based Signaling System 7 (SS7) signaling gateway designed for alleviating congestion on voice networks by diverting data calls away from circuit switches. By enabling remote access equipment to communicate with carrier SS7 networks, ICD for Softswitch supports the redirection of resource-consuming Internet traffic from the Public Switched Telephone Network (PSTN) directly onto data networks. This capability enables service providers to prevent Internet call busy signals, cut the cost of providing dial-up connections, and free up PSTN circuits to carry voice traffic only. See also *PSTN*, *signaling gateway*, *SS7*.

ICMP—Internet Control Message Protocol. ICMP is an error-reporting mechanism integral to the TCP/IP protocol suite. Gateways and hosts use ICMP to send reports of datagram problems to the sender. ICMP also includes an echo request/reply function that tests whether a destination is available and responding. See also *gateway*, *host*, *TCP/IP*.

ICMP Redirect packet—A packet that instructs the receiver to override a setting in its routing table. A router can use an ICMP Redirect packet to tell a host that it is sending packets to the wrong router, and to inform the host of the correct route. However, a forged ICMP Redirect packet can alter the host's routing table and compromise the security of the network. For this reason, many firewalls reject ICMP traffic. See also *DoS attack*, *firewall*, *ICMP*.

IDI—Initial Domain Identifier. The IDI is a subfield of the Initial Domain Part (IDP) of an ATM End System Address (AESA). The IDI identifies the subauthority that allocated the address. Compare with *AFI*. See also *AESA format*, *IDP*.

idle connection—A connection between end points on which no data is being transmitted.

idle disconnect—A disconnect that occurs when no data is transmitted on a link for a specified period of time. See also *idle timer*.

idle limit—The value specified for the Ascend Tunnel Management Protocol (ATMP) inactivity timer. See also *inactivity timer*.

idle timer—A value that specifies how long a session can remain idle before the TAOS unit disconnects it. By default, any traffic across an active connection resets the connection's idle timer. When you apply a call filter, its forwarding action determines which packets can initiate a connection or reset a session's timer. When a session's idle timer expires, the TAOS unit terminates the session. The idle timer is set to 120 seconds by default, so if a connection is inactive for two minutes, the TAOS unit terminates the connection. Compare with *inactivity timer*. See also *call filter*.

IDP—Initial Domain Part. The IDP is a portion of an Asynchronous Transfer Mode (ATM) address in ATM End System Address (AESA) format. The IDP specifies the Authority and Format Identifier (AFI) and Initial Domain Identifier (IDI) subfields. Compare with *DSP*. See also *AESA format*, *AFI*, *IDI*.

IDSL—ISDN Digital Subscriber Line. IDSL is a standard that uses ISDN technology to enable devices to transmit data into an IDSL modem bank connected to a router. IDSL offers data rates of up to 128Kbps. Compare with *ADSL*, *HDSL*, *RADSL*, *SDSL*, *VDSL*. See also *DSL*.

IE—Information Element. In a message, a set of parameters specifying addressing, signaling, and other types of connection-related information. The signaling packets used to set up an Asynchronous Transfer Mode (ATM) call contain called-party and calling-party address IEs. The Q.931 setup message includes a bearer-capability IE that specifies the type of application using the B channel. See also *ATM*, *Q.931*.

IEC—Interexchange Carrier. An IEC is a type of telephone service that provides long-distance links between local telephone companies. Well-known IECs include AT&T, MCI, and Sprint. Compare with *LEC*.

IEEE—Institute of Electrical and Electronics Engineers. The IEEE is an organization that maintains the standards for 10BaseT and other communications specifications. See also *10BaseT*.

IETF—Internet Engineering Task Force. Responsible for developing the TCP/IP protocol suite, the IETF operates under the auspices of the Internet Society's Internet Architecture Board (IAB). See also *IAB*, *Internet Society*.

IFAP—Incoming Fax Authentication Packet. The first packet that a TAOS unit sends to a fax server on a Transmission Control Protocol (TCP) connection after the unit receives an incoming fax call. An IFAP includes a 16-byte security code, the original dialed number, and the caller ID (if available). See also *fax server*, *FCRP*, *TCP*.

I-frame—Information frame. An I-frame transports data over an X.25 access link. Compare with *general frame*, *supervisory frame*. See also *X.25*.

IGMP—Internet Group Management Protocol. IGMP is a protocol implemented by multicast clients and routers. A TAOS unit responds as a client to the IGMP packets it receives from a Multicast Backbone (MBONE) router. The packets can use IGMP version-1, IGMP version-2, or IGMP Multicast Trace (MTRACE). Clients wanting MBONE service must implement IGMP. See also *MBONE*, *multicast*, *multicast network*, *router*.

IGP—Interior Gateway Protocol. IGP transmits routing information internal to a network. See also *routing*.

IISP—Interim Inter-switch Signaling Protocol. IISP is an Asynchronous Transfer Mode (ATM) signaling protocol that facilitates switch-to-switch communication. See also *ATM*, *ATM IISP-DCE*, *ATM IISP-DTE*.

ILMI—Integrated Local Management Interface. ILMI is a specification for network-management functions for the link between a public network and a private network, or between a user and a network. See also *ATM*.

immediate mode—A terminal-server access mode in which the terminal server does not display the command-line prompt or a menu of hosts, but uses TCP, Rlogin, or Telnet to immediately direct a dial-in user to a designated host. When you use Telnet to initiate the connection to the host, you can configure the terminal server to pass the call to the host before authentication. In this case, the responsibility for authentication belongs to the host. See also *Rlogin*, *TCP*, *Telnet*.

immediate modem service—A feature that enables terminal-server users to have direct access to a particular Telnet port on the TAOS unit for modem dial-out, bypassing the terminal-server interface. See also *modem dial-out*.

IMT—Inter-Machine Trunk. An IMT is a high-speed circuit between switches.

IN—Intelligent Network. Created by Bellcore, IN is a telephone network architecture in which a specific portion of a dialed telephone number (for example, 800 or 900) signals a request for a particular service.

inactivity timer—A value that specifies the number of minutes that an Ascend Tunnel Management Protocol (ATMP) Home Agent maintains an idle tunnel before disconnecting it. Compare with *idle timer*. See also *ATMP*, *Home Agent*.

inband signaling—A type of signaling in which a line uses 8Kbps of each 64Kbps channel for WAN synchronization and signaling. The remaining 56Kbps handle the transmission of user data. When a line is configured for inband signaling, the TAOS unit does not receive bearer-capability information from the carrier. Therefore, it does not know whether a call uses voice service or digital service. For call-routing purposes, the unit assumes that all calls on an inband-signaling line are digital. Another term for inband signaling is *robbed-bit signaling*. Robbed-bit refers to the 8Kbps used for signaling in each channel. Compare with *ISDN D-channel signaling*.

inclusion area—On a MultiVoice gateway, a dial string such as a country code, area code, combined country and area code, area code and exchange combination, or complete telephone number. For example, an inclusion area might be specified by the partial telephone number `1732`. This number is composed of a country code of `1` and area code of `732`. A MultiVoice gateway with this inclusion area would cover all telephone numbers within the 732 area code. Together, several inclusion areas represent the coverage area for a MultiVoice gateway. See also *coverage area*, *gatekeeper*, *gateway*, *MultiVoice™*.

incoming call—A call that a TAOS unit receives from a remote user or device. Compare with *outgoing call*.

incoming continuity test—In a Signaling System 7 (SS7) network, a test in which the telephone switch generates a tone after requesting that the TAOS unit put a DS0 channel into loopback mode. If the switch receives the tone in return, the continuity test is successful. Compare with *outgoing continuity test*. See also *2-wire continuity test*, *4-wire continuity test*, *4-wire-to-2-wire continuity test*, *continuity test*, *SS7 network*.

Incoming Fax Authentication Packet—See *IFAP*.

individual address—In Switched Multimegabit Data Service (SMDS), an address uniquely assigned to a single Subscriber Network Interface (SNI). Each SNI can have a maximum of 16 addresses. Compare with *group address*. See also *SMDS*, *SNI*.

Information frame—See *I-frame*.

Information Request message—See *IRQ message*.

Initial Address Message—See *IAM*.

Initial Domain Part—See *IDP*.

input filter—A filter applied to an incoming packet. See also *filter*, *packet filter*, *route filter*.

Input/Output—See *I/O*.

Institute of Electrical and Electronics Engineers—See *IEEE*.

Integrated Access Device—See *IAD*.

Integrated Local Management Interface—See *ILMI*.

Integrated Services Digital Network—See *ISDN*.

Integrated Small Digital Exchange—See *ISDX*.

Intelligent Network—See *IN*.

interarrival jitter—An estimate of the statistical variance among the arrival times of Real-Time Transport Protocol (RTP) packets, which is equivalent to the difference in their relative transit times. Relative transit time is the difference between a packet's RTP timestamp at the sender and the receiver's clock at the time of arrival. See also *RTP*.

interdigit timer—A value that specifies the number of milliseconds that a T1 Digital Signal Processor (DSP) waits between digits before considering Dialed Number Information Service/Automatic Number Identification (DNIS/ANI) collection complete. See also *ANI, DNIS, DSP*.

Interexchange Carrier—See *IEC*.

interface—A connection between two devices, programs, or program elements. See also *hardware interface*.

interface-based routing—An IP-routing method in which each physical or logical interface on a unit has its own IP address. The interface becomes a numbered interface. Reasons for using numbered interfaces include troubleshooting dedicated point-to-point connections and forcing routing decisions between two links going to the same final destination. Interface-based routing enables a TAOS unit to operate somewhat like a multihomed host.

You can configure each link as numbered (interface-based) or unnumbered (system-based). If no interfaces are numbered, a TAOS unit operates as a purely system-based router. Compare with *system-based routing*. See also *IP routing, multihomed host, numbered interface, point-to-point link, unnumbered interface*.

interface cost—See *link-state metric*.

Interim Inter-switch Signaling Protocol—See *IISP*.

Interior Gateway Protocol—See *IGP*.

Inter-Machine Trunk—See *IMT*.

internal clocking—A TAOS unit's transmission of the transmit and receive clocks to the user equipment.

internal Link State Advertisement—See *internal LSA*.

internal LSA—Internal Link State Advertisement. An internal LSA is exchanged by Open Shortest Path First (OSPF) routers within a single Autonomous System (AS). Compare with *external LSA*. See also *AS, LSA, OSPF*.

International Code Designator—See *ICD*.

International Code Designator ATM End System Address format—See *ICD AESA format*.

International Standards Organization—See *ISO*.

International Telecommunication Union–Telecommunication Standardization Sector—See *ITU-T*.

internal testing—A hardware diagnostic that performs an internal loopback test on a slot card. See also *loopback*.

internet—See *internetwork*.

Internet—The complex of WANs joining government, university, corporate and private computers in a vast web of network interconnection.

Internet Architecture Board—See *IAB*.

Internet Assigned Numbers Authority—See *IANA*.

Internet Call Diversion for Softswitch—See *ICD for Softswitch*.

Internet Control Message Protocol—See *ICMP*.

Internet Engineering Task Force—See *IETF*.

Internet gateway—A gateway for accessing the Internet. See also *gateway*.

Internet Group Management Protocol—See *IGMP*.

Internet Network Information Center—See *InterNIC*.

Internet Protocol—See *IP*.

Internet Protocol Control Protocol—See *IPCP*.

Internet Protocol Device Control—See *IPDC*.

Internet Protocol over X.25—See *X.25/IP*.

Internet Protocol Security—See *IPSec*.

Internet Registry—A branch of the Internet Society's Internet Architecture Board (IAB). The Internet Registry supervises the Domain Name System (DNS). See also *DNS*, *IAB*, *Internet Society*.

Internet Reliable Transaction Protocol—See *IRTP*.

Internet Service Provider—See *ISP*.

Internet Society—An international nonprofit organization that focuses on Internet standards, education, and policy issues. Founded in 1992 and located in Reston, Virginia, the Internet Society oversees the Internet Architecture Board (IAB), which in turn oversees a number of committees, including the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the Internet Assigned Numbers Authority (IANA), and the Internet Registry. See also *IAB*, *IANA*, *IETF*, *Internet Registry*, *IRTF*.

internetwork—A series of networks connected by gateways or routers. See also *gateway*, *router*.

Internetwork Packet Exchange—See *IPX*.

InterNIC—Internet Network Information Center. InterNIC is an organization that provides Internet information services, oversees the registration of Internet addresses and Domain Name System (DNS) names, assigns RFC numbers, and assists users in gaining access to the Internet. See also *DNS*, *RFC*.

interoperability—Compatibility with the devices and services of multiple vendors. Interoperable devices can be integrated into a network containing a wide range of vendor products. Interoperability is a significant factor among expansion considerations, because any device must have the versatility to function in an expanding network structure. The technical elements of interoperability can include a bundle of protocols and a flexible architecture to accommodate upgrades. A remote-access server should include capabilities such as translation, encapsulation, and filtering.

intra-area route—A route imported into the Open Shortest Path First (OSPF) database from within the router's area. Compare with *external route*. See also *area*, *OSPF*, *route*, *router*.

Intragy™—A Lucent Technologies enterprise access solution that provides corporations with the multiprotocol support needed for flexible access to a corporate network. Intragy combines the IntragyCentral™ network-access solution with IntragyAccess™ cross-platform desktop client software. Together, these components provide complete network access for all users of the corporate network: LAN users, telecommuters, remote users, and mobile workers. Intragy combines multiprotocol routing, Ethernet bridging, desktop client dial-out, and desktop client software to deliver open access to centralized corporate resources.

inverse multiplexer—Equipment that performs inverse multiplexing at each end of a connection. An inverse multiplexer is also known as an *inverse mux*. See also *inverse multiplexing*.

inverse multiplexing—A method of sending a single data stream in multiple concurrent transmissions across separate channels, and then reconstructing the original data stream at the destination device. Each end of the connection uses an inverse multiplexer (also called an *inverse mux*). See also *circuit-level inverse multiplexing*, *inverse multiplexer*, *packet-level inverse multiplexing*, *T1 line*.

inverse mux—See *inverse multiplexer*.

I/O—Input/Output. A manner of describing a process, program, or device that transfers information to or from a computer. Common I/O devices are hard disks, printers, keyboards, diskettes, and CDs.

IP—Internet Protocol. IP provides connectionless, nonguaranteed transmission of Transport-layer data packets. IP can fragment packets, enabling them to take different paths across the WAN, and can then reassembles them into the proper order at their destination. See also *Transport layer*.

IP address—An address that uniquely identifies each host on an IP network or internetwork. An IP address has a length of 32 bits, and is divided into four 8-bit parts, each separated by a period, as in 149.122.3.30. This kind of notation is called *dotted decimal notation*. Each part can consist of a number from 1 through 255.

An IP address consists of a network number and a host number. IP addresses come in three types: Class A, Class B, and Class C. The class of an IP address determines which portion of the address belongs to the network number and which portion belongs to the host number. The first bits of the IP address identify the class. The Internet Network Information Center (InterNIC) determines the type of class assigned to a network.

A Class A address starts with 0 (zero) as the class identifier, followed by 7 bits for the network number and 24 bits for the host number. Therefore, the first number in dotted decimal notation is the network number. The next three numbers make up the host number. For example, in the IP address 127.120.3.8, the network number is 127 and the host number is 120.3.8. This type of address is used by the largest organizations, because this scheme allows for over 16 million different host numbers. However, it also limits network numbers to a total of 128.

A Class B address starts with binary 10 as the class identifier, followed by 14 bits for the network number and 16 bits for the host number. Therefore, the first two dotted decimal numbers are the network number, and the second two dotted decimal numbers are the host number. For example, in the IP address 147.14.86.24, the network number is 147.14 and the host number is 86.24. More network numbers are available than in a Class A address, but fewer hosts (approximately 65,000).

A Class C address starts with binary 110 as the class identifier, followed by 21 bits for the network number and 9 bits for the host number. Therefore, the first three dotted decimal numbers are the network number, and the last dotted decimal number is the host number. For example, in the IP address 225.135.38.42, the network number is 225.135.38 and the host number is 42. Many network numbers are available, but only 254 hosts per network number are possible. The host numbers 0 and 255 are reserved.

You can determine the type of class an IP address falls into by looking at the first 8-bit portion of the dotted decimal form of the address. Class A addresses begin with a number from 0 through 127. Class B addresses begin with a number from 128 through 223. Class C addresses begin with a number from 192 through 233. In addition to an IP address, you can use a symbolic name provided by Domain Name System (DNS) to designate an Internet address. See also *DNS, dotted decimal notation, host number, internetwork, InterNIC, IP, network, IP network number, IP subnet, subnet mask.*

IP address pool—A pool from which a TAOS unit dynamically allocates an IP address to a calling unit. You can configure up to 128 address pools on a TAOS unit, and up to 50 in RADIUS. See also *dynamic IP, global IP address pool, IP address, pool chaining.*

IP address spoofing—A way for a remote device to illegally acquire a local address in order to break through a firewall or data filter. You can configure WAN IP interfaces so that the system checks the source IP address in all received packets and drops the packets if the address does not match the address negotiated for the remote subnet. This type of configuration enables a TAOS unit to detect packets with a spoofed source IP address and discard them.

When the system initially detects a spoofing attempt (a mismatched source address), it logs a message that includes the port number on which the attempt occurred. For example:

```
[1/4/1/1] Spoofing Attempt:from port 1 [MBID 1;1119855018][ed-mc1-p75]
```

See also *filter, firewall, IP address*.

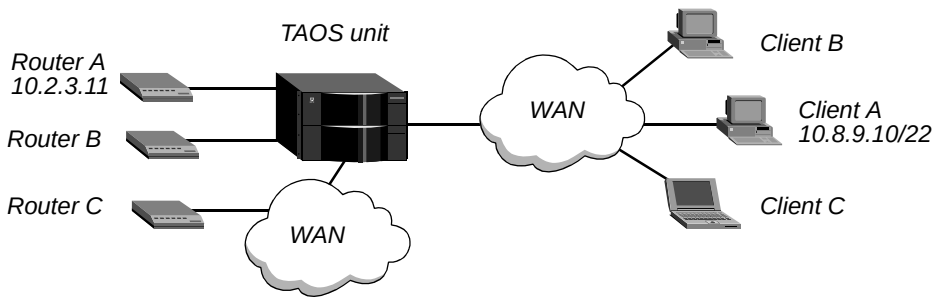
IPCP—Internet Protocol Control Protocol. Described in RFC 1332, IPCP is a protocol for configuring, enabling, and disabling the IP protocol modules on both ends of a point-to-point link. It allows both ends of a Point-to-Point Protocol (PPP) link to exchange their IP addresses and to negotiate Van Jacobson (VJ) compression. IPCP is activated when PPP reaches the Network-layer protocol phase. Elements of IPCP include packet encapsulation, code fields, and timeouts. See also *IP*, *Network layer*, *point-to-point link*, *PPP*.

IPDC—Internet Protocol Device Control. IPDC is a third-party proprietary protocol developed by Level (3) Communications in order to establish Voice over IP (VoIP) calls originating from the Public Switched Telephone Network (PSTN). When you use the Signaling System 7 (SS7) IPDC license, the system uses IPDC for communication between the signaling gateway and the TAOS unit. Compare with *ASGCP*. See also *PSTN*, *signaling gateway*, *SS7*, *SS7 network*, *VoIP*.

IPDC message tag—Internet Protocol Device Control message tag. On a Signaling System 7 (SS7) network, IPDC message tags define voice encoding type, packet loading, Internet Protocol (IP) and Real-Time Transport Protocol (RTP) ports and other variables used for processing Voice over IP (VoIP) calls. See also *IP*, *RTP*, *SS7 network*, *VoIP*.

IP direct—A configuration in which the TAOS unit automatically redirects incoming IP packets to a host you specify on the local IP network. When you specify IP direct, the TAOS unit bypasses all internal routing tables and sends all packets it receives on a connection's WAN interface to the specified IP address. Figure 37 shows an example of the traffic flow for IP direct.

Figure 37. IP direct connections



The TAOS unit redirects incoming packets from Client A to Router A, and from Client B to Router B, on the LAN side of the TAOS unit. From Client C, the TAOS unit redirects incoming packets to Router C through a switched connection.

Packets destined for the clients A, B, or C are routed normally by the TAOS unit. These client connections can *receive* packets from any source connected to the TAOS unit, not just from the IP address to which their packets are redirected. See also *IP address*, *IP routing table*.

IP fax—A feature that enables a TAOS unit to interact with a third-party fax server, such as the servers provided by Open Port Technology, Inc. IP fax technology enables ISPs and corporate hubs to use the Internet to deliver faxes.

When the IP fax feature is enabled on a TAOS unit, the system acts as a Remote Access Server (RAS), accepting fax calls on the same ports and telephone lines used for dial-in modem connections. The unit also performs modem dial-out functions to deliver faxes from the Internet to fax machines on the Public Switched Telephone Network (PSTN).

Figure 38 shows the basic structure of an incoming IP fax operation. The TAOS unit receives an incoming fax from the PSTN and interacts with the fax server to transfer it to the Internet. The transfer to the Internet is transparent to the person sending the fax, because a hardware device called a *redialer* is connected to the fax machine. The redialer intercepts the number dialed on the fax machine and initiates a call to the TAOS unit instead. When the fax server begins transferring the fax to the Internet, the redialer and the TAOS unit become transparent pipes for the fax data.

Figure 38. Incoming IP fax from fax machine to Internet

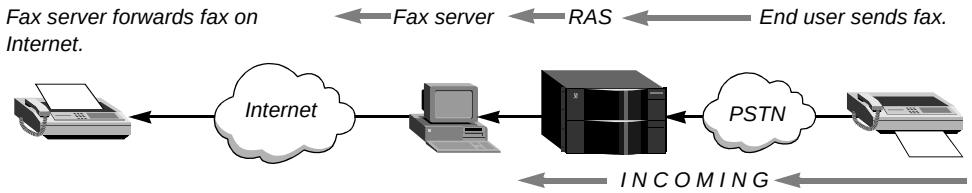
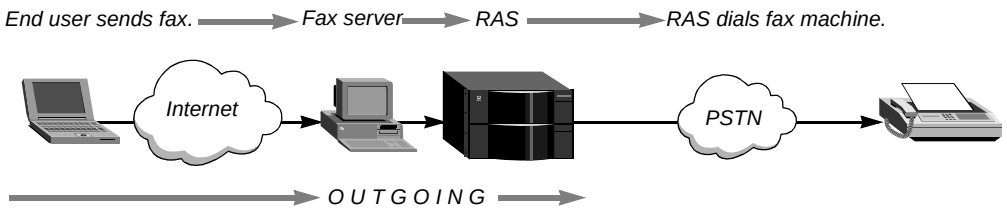


Figure 39 shows the basic structure of an outgoing IP fax operation. The fax server receives an outgoing fax from the Internet and interacts with the TAOS unit to transfer it to the PSTN. The fax server logs in to the TAOS unit and is authenticated before seizing one of the unit's modems for dial-out to the destination fax machine.

Figure 39. Outgoing IP fax from Internet to fax machine



IP fax is also known as *store-and-forward fax*. See also *fax server*, *PSTN*, *RAS*.

IP filter—A packet filter that examines fields specific to IP packets. An IP filter focuses on known fields, such as source or destination address and protocol. It operates on logical information that is relatively easy to obtain. In an IP filter, a number of distinct comparisons occur in a defined order. When a comparison fails, the packet goes on to the next comparison. When a comparison succeeds, the filtering process stops and the TAOS unit applies the forwarding action that the filter specifies for the packet. Compare with *generic filter*, *IPX filter*, *TOS filter*. See also *call filter*, *data filter*, *packet filter*.

IP-in-IP encapsulation—A way to alter an IP packet's normal routing by encapsulating it within another IP packet. The encapsulating header specifies the address of a router that would not be selected as a next-hop router on the basis of the packet's real destination address. The intermediate node decapsulates the packet, which is then routed to the destination as usual.

This method of rerouting packets by using encapsulation is referred to as *tunneling* the packet, and the *end points* of the tunnel are the system that encapsulates the packets (the Foreign Agent) and the system that decapsulates the packets (the tunnel server). For complete information about how this process takes place, see RFC 2003, *IP Encapsulation within IP.*

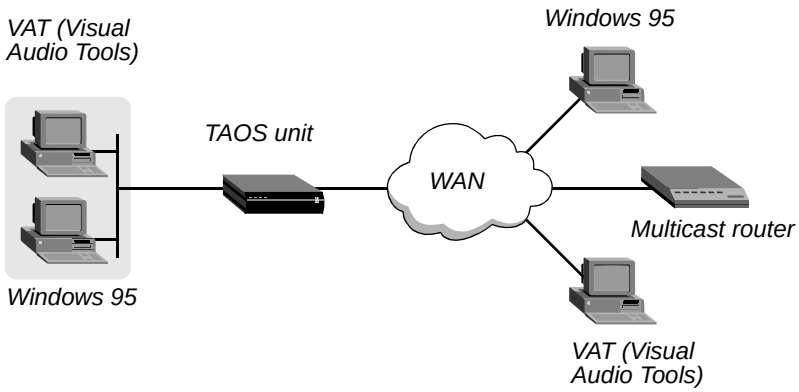
A TAOS unit operates only as a Foreign Agent and not as a tunnel server. It encapsulates the incoming IP packet in another IP packet, forming an IP-in-IP packet. It does not decapsulate an IP-in-IP packet. The source address in the outer IP header of the IP-in-IP packet is set to the Foreign Agent IP address, and the destination IP address is set to the IP address of the tunnel server. The encapsulated packet is then routed to the tunnel server in the usual way.

If the Foreign Agent receives an incoming packet that is larger than the IP-in-IP Maximum Transmission Unit (MTU) size, it fragments the packet before encapsulation. Each fragment is then encapsulated in its own IP header. The IP-in-IP MTU size is currently fixed at 1480 bytes.

See also *Foreign Agent*, *IP address*, *tunneling*, *tunnel server*.

IP multicast forwarding—A process by which a TAOS unit forwards traffic it receives on one of its Ethernet or WAN interfaces from an Multicast Backbone (MBONE) router. Figure 40 shows a multicast router on a WAN interface with both local and WAN multicast clients.

Figure 40. Forwarding multicast traffic on both Ethernet and WAN interfaces



To the MBONE, the TAOS unit looks like a multicast client, and it responds as a client to Internet Group Membership Protocol (IGMP) packets it receives. The TAOS unit resends the multicast packets to all of its own clients connected to it for MBONE service. The clients wanting MBONE service must implement IGMP.

To enable multicast forwarding, you must configure each Ethernet or WAN interface that supports multicasting. When you do so, the TAOS unit begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until you set the multicast rate limit. Compare with *Frame Relay multicasting*. See also *IGMP, MBONE, MBONE router, multicast, multicast heartbeat, multicast network, multicast rate limit.*

IP network—A network that uses the Internet Protocol (IP) to transmit packets at the Network layer. An IP network has a packet-switched architecture. Devices transmit data in packets, and the path from end to end can vary for successive IP packets. In addition to data, each packet contains IP addressing information. Routing devices use this information to forward data to each packet's destination. Routing protocols, such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF), define methods that routers use to update their routing tables.

In the past, the Public Switched Telephone Network (PSTN) was the only network supporting voice communication. But with the introduction of MultiVoice, voice traffic can now be sent over IP-based packet-switched networks. See also *IP*, *IP routing*, *IP routing table*, *MultiVoice™*, *packet-switched network*, *PSTN*.

IP network number—The portion of an IP address that denotes the network on which a host resides. The class of an IP address determines which portion of the address belongs to the network number and which portion belongs to the host number. See also *host number*, *IP address*, *subnet mask.*

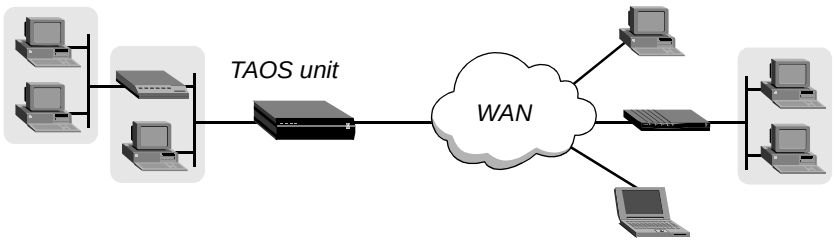
IP pool chaining—See *pool chaining*.

IP route—A path from one IP network to another. See also *dynamic route*, *IP network*, *multipath route*, *static IP route*.

IP router—A device that sends IP packets from a source to a destination by multiple paths. As an IP router, a TAOS unit routes IP packets between its Ethernet interfaces and across any WAN interface configured for IP routing. See also *IP route*, *IP routing*.

IP routing—A method of determining how to forward an IP packet to the proper destination. When acting as an IP router, a TAOS unit routes IP packets between its Ethernet interfaces and across any WAN interface configured for IP routing. Figure 41 shows a TAOS unit that routes IP packets between WAN interfaces and a LAN interface.

Figure 41. IP-routing configuration



The TAOS unit consults its internal routing table to determine where to forward each IP packet it processes. First, the unit tries to find a match between the packet's destination address and a Destination field in its routing table. If it finds a match, it establishes the required connection (if necessary) to reach the next-hop router specified for that route, and forwards the packet. If it does not find a match for the packet's destination address, it searches for a default route (destination address 0.0.0.0). If it finds a default route, it establishes the required connection (if necessary) and forwards the packet. If the routing table has no default route, and no route that matches a packet's destination address, the TAOS unit drops the packet. See also *default route*, *hop*, *IP route*, *IP router*, *IP routing table.*

IP routing table—A table that contains information about how to forward IP packets. On a TAOS unit, each record in the routing table contains the following fields:

Field	Indicates
Destination	Target address. To send a packet to the address specified in a record's Destination field, the TAOS unit uses the route defined by the record. Note that the router uses the most specific route (having the longest subnet mask) that matches a given destination.
Gateway	Address of the next-hop router that can forward packets to the destination. Direct routes do not show a gateway address.
IF	Name of the interface through which the TAOS unit sends a packet.
Flg	Flag values describing the route. Following are the possible values: • C—directly connected route, such as Ethernet • I—ICMP Redirect dynamic route • N—route placed in the table by the SNMP MIB II • O—route learned from OSPF • R—route learned from RIP • r—transient RADIUS-like route that will disappear when the connection is broken • S—static route • ?—route of unknown origin, which indicates an error • G—indirect route through a gateway • P—private route • T—temporary route • M—multipath route • *—backup static route for a transient RADIUS-like route
Pref	Preference value of the route.
Metric	RIP-style metric for the route, with a valid range of 0 through 16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.
Use	Number of times the route was referenced since it was created. (Many of these references are internal, so this value is not a count of the number of packets sent on the route.)
Age	Age of the route in seconds. The Age field is used for troubleshooting and for determining when routes are changing rapidly.

See also *direct route*, *dynamic route*, *gateway*, *hop*, *IP route*, *IP router*, *metric*, *multipath route*, *OSPF*, *preference*, *RIP*, *static IP route*.

IPSec—Internet Protocol Security. IPSec is the security standard for use at the network or packet-processing level of network communication. IPSec provides authentication, data confidentiality, and data integrity. By and large, IPSec is used in the design and implementation of Virtual Private Networks (VPNs) and for dial-in connections to remote networks. See also *AH*, *ESP*, *replay protection*, *SA*, *SPI*, *transform*, *VPN*.

IP subnet—A portion of an IP network. IP subnetting is a way to subdivide a network into smaller networks, resulting in a greater number of hosts on a network associated with a single IP network number. An IP address that uses a subnet has three elements: network, subnet, and host. You identify a subnet by combining an address with a subnet mask. For example, in the address 195.112.56.75/14, /14 is the subnet mask. See also *host number*, *IP address*, *IP network number*, *subnet mask*.

IP switch—A device that can determine the destination of large volumes of incoming IP packets and send them to the appropriate outgoing ports at high speeds. An IP switch is a high-performance device designed for high-volume, large-scale public and private backbone applications. See also *switch*.

IPX—Internetwork Packet Exchange. IPX is Novell's connectionless Network-layer protocol. Derived from XNS' Internetwork Datagram Protocol (IDP), IPX performs addressing and routing functions. At the server, IPX passes outgoing datagrams to the network interface software. At the packet's destination, IPX passes the data to upper-layer processes. Along an IPX route, intermediate devices use IPX to route packets to their destinations. When routing, IPX relies on information supplied by the Routing Information Protocol (RIP). See also *IPX network*, *IPX route*, *IPX routing*, *IPX server*, *RIP*.

IPX bridging—At the Data Link layer, a way of passing IPX packets between networks. See also *Data Link layer*, *IPX network*.

IPX client—A user or device that gains access to the services of an IPX server. See also *IPX server*.

IPXCP—Internet Packet Exchange Control Protocol. As specified by RFC 1552, IPXCP is a protocol for configuring, enabling, and disabling the IPX protocol modules on both ends of a point-to-point link. IPXCP is tied to Point-to-Point Protocol (PPP), and is activated when PPP reaches the Network-layer protocol phase. See also *IPX*, *point-to-point link*, *PPP*.

IPX filter—A packet filter that examines fields specific to IPX packets. An IPX filter focuses on known fields, such as source or destination address. It operates on logical information that is relatively easy to obtain. In an IPX filter, a number of distinct comparisons occur in a defined order. When a comparison fails, the packet goes on to the next comparison. When a comparison succeeds, the filtering process stops and the TAOS unit applies the forwarding action that the filter specifies for the packet. Compare with *generic filter*, *IP filter*, *TOS filter*. See also *call filter*, *data filter*, *packet filter*.

IPX frame—The type of packet frame used by an IPX server. An IPX frame can follow the IEEE 802.2, IEEE 802.3, SubNetwork Access Protocol (SNAP), or Ethernet II protocol specification for the Media Access Control (MAC) header. See also *802.2*, *802.3*, *Ethernet II*, *IPX server*, *MAC*, *SNAP*.

IPX Nearest Server Query—In an Ascend Tunnel Management Protocol (ATMP) configuration, a message sent to a Home Agent from a mobile client, asking whether the Home Agent knows about a server on the home network. See also *ATMP*, *Home Agent*, *home network*, *mobile client*.

IPX network—A network consisting of one or more IPX servers and IPX clients. See also *IPX client*, *IPX server*, *virtual IPX network*.

IPX network number—The portion of an IPX address that denotes the IPX network on which a node resides. If a TAOS unit is routing IPX and there are other IPX servers on the LAN interface, the IPX network number assigned to the TAOS unit for that interface must be consistent with the number in use by the other routers.

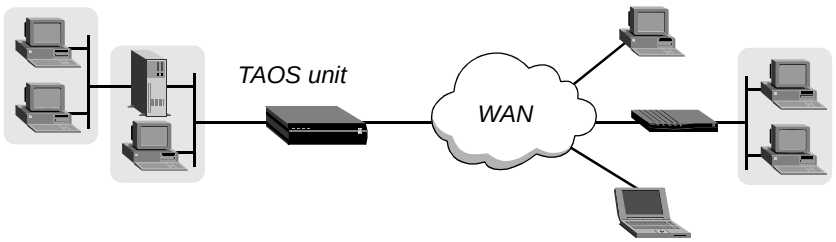
If you do not specify an IPX network number in the TAOS unit's configuration, the unit learns its network number from another router on the interface or from the Routing Information Protocol (RIP) packets received from the IPX router. If you specify an IPX network number in the TAOS unit's configuration, the unit becomes a seed router, and other routers can learn the network number from the TAOS unit. See also *IPX router*, *seed router*.

IPX route—A path from one IPX network to another. See also *IPX network*, *IPX router*, *IPX routing*.

IPX router—A device that sends IPX packets from a source to a destination by various paths. See also *IPX route*, *IPX routing*.

IPX routing—A method of sending IPX packets from a source to a destination at the Network layer. A TAOS unit configured for IPX routing enables NetWare clients and distributed Novell networks to use NetWare services across the WAN. The NetWare version must be 3.11 or later. Figure 42 shows a TAOS unit that routes IPX between WAN interfaces and a local Novell network.

Figure 42. IPX-routing configuration



IPX routers broadcast RIP updates periodically and when a WAN connection is established. The TAOS unit receives IPX RIP broadcasts from a remote device, adds 1 to the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

The TAOS unit follows standard IPX RIP behavior for routers when connecting to non-TAOS units. However, when it connects to another TAOS unit configured for IPX routing, both ends of the connection immediately exchange their entire RIP tables. In addition, the TAOS unit maintains those RIP entries as static until the unit is reset or turned off and on.

The TAOS unit recognizes network number –2 (0xFFFFFFFE) as the IPX RIP default route. When it receives a packet for an unknown destination, the unit forwards the packet to the IPX router advertising the default route. If more than one IPX router is advertising the default route, the unit makes a routing decision based on the hop and tick count. For example, if the TAOS unit receives an IPX packet destined for network 77777777 and it does not have a RIP table entry for that destination, the unit forwards the packet toward network number FFFFFFFE, if available, instead of simply dropping the packet.

The TAOS unit incorporates changes to standard IPX behavior with regard to IPX Service Advertising Protocol (SAP), IPX Routing Information Protocol (RIP), and IPXWAN negotiation. In addition, Lucent Technologies has added IPX extensions that enable TAOS units to operate as clients expect for NetWare LANs. These extensions include creating a virtual network for dial-in IPX clients, accepting or rejecting RIP and SAP updates, establishing connections in response to a SAP query, creating static IPX routes, and defining SAP filters. See also *default route*, *dial query*, *distance-vector metric*, *hop*, *IPX*, *IPX network*, *IPX route*, *IPX router*, *IPX server*, *IPXWAN*, *RIP*, *router*, *routing*, *SAP*, *SAP filter*, *split horizon*, *static IPX route*, *TCP/IP*, *tick*, *virtual IPX network*.

IPX SAP—See *SAP*.

IPX SAP filter—See *SAP filter*.

IPX server—A server that runs the NetWare operating system, manages network resources, and communicates with IPX clients. See also *IPX*, *IPX client*.

IPX spoofing—A procedure that enables a device to mimic a legitimate network host and gain illegal access to data within a private IPX network. Spoofing can lead to severe security breaches and damage the integrity of a company's operations. See also *IP address spoofing*, *IPX network*.

IPX Type 20—A type of packet that applications such as NetBIOS over IPX use to broadcast names over a network. By default, these broadcasts are not propagated over routed links and are not forwarded over links that have less than 1Mbps throughput. However, if you are using an application such as NetBIOS over IPX, which requires these packets in order to operate, you can enable the router to propagate IPX Type 20 packets over a LAN interface. See also *IPX*.

IPXWAN—The WAN version of NetWare's IPX protocol. TAOS units support the IPXWAN protocol, which is essential for communicating with Novell software that supports dial-in connections, and for communicating with the Multi-Protocol Router. For full specifications of the IPXWAN protocol, see RFC 1634 and *NetWare Link Services Protocol Specification—IPX WAN Version 2*.

When an IPX connection is established between two TAOS units, all options are negotiated during the IPXCP phase. IPXWAN negotiation never takes place between two TAOS units, because neither unit sends out an IPXWAN Timer_Request packet to initiate the negotiation process.

Connections with non-TAOS devices that use Novell software operating over Point-to-Point Protocol (PPP) do not negotiate options during the IPXCP phase, so all options are negotiated during the IPXWAN phase of link establishment. The remote device sends an IPXWAN Timer_Request packet, which triggers IPXWAN negotiation in the TAOS unit. The devices compare internal network numbers and assign the slave role to the unit with the lower number. The other unit becomes the master of the link for the duration of the IPXWAN negotiation. The slave unit returns an IPXWAN Timer_Response packet, and the master unit initiates an exchange of information about the final router configuration. The TAOS unit supports the following routing options:

- TAOS routing (unnumbered RIP/SAP without aging).
- Novell routing (unnumbered RIP/SAP with aging).
- None (The peer is a dial-in client. Neither RIP nor SAP is operational, except on request. Network and node numbers can be assigned.)

Header compression is rejected as a routing option. After IPXWAN negotiation is complete, transmissions of IPX packets use the negotiated routing option. See also *IPX, IPXCP*, *RIP*, *SAP*.

IRQ message—Information Request message. An H.323 Registration, Admission, and Status (RAS) message used to request status information from an H.323 end-point (gateway, gatekeeper, or terminal). See also *gatekeeper*, *gateway*, *H.323*, *RAS*.

IRTF—Internet Research Task Force. The IRTF is overseen by the Internet Society's Internet Architecture Board (IAB) and is composed of a number of focused, long-term research groups. These groups are concerned with issues related to Internet protocols, architecture, and technology. See also *IAB*, *Internet Society*.

IRTP—Internet Reliable Transaction Protocol. IRTP is a full-duplex, transaction-oriented, host-to-host protocol providing reliable, sequenced delivery of data packets and a constant connection between two hosts. Unlike the User Datagram Protocol (UDP), IRTP provides reliable, sequenced delivery of packets. Unlike the Transaction Control Protocol (TCP), IRTP sequencing takes place on a packet-by-packet basis, and only one connection is defined between Internet addresses. See also *TCP*, *UDP*.

ISDN—Integrated Services Digital Network. ISDN is a telecommunications architecture capable of sending voice, data, and video in digital form on a digital line. It can support bandwidth of up to 2Mbps, and uses a single digital line for telephone, fax, computer, and video communications. ISDN supports circuit-switched and Frame Relay connections. See also *circuit switching*, *digital data*, *E1 PRI line*, *Frame Relay*, *ISDN BRI line*, *T1 PRI line*.

ISDN Basic Rate Interface line—See *ISDN BRI line*.

ISDN BRI line—ISDN Basic Rate Interface line. An ISDN line uses two B channels for user data, and one 16Kbps D channel for ISDN D-channel signaling. Both B channels can be switched, both channels can be dedicated, or one channel can be switched and the other dedicated. An ISDN BRI line can connect to standard voice service, the Switched-56 data service, or the Switched-64 data service. Compare with *E1 PRI line*, *T1 PRI line*. See also *B channel*, *D channel*, *dedicated channel*, *ISDN D-channel signaling*, *Switched-56*, *Switched-64*, *switched channel*.

ISDN Call Setup message—A message that an ISDN device sends to the network when you make a call. The Call Setup message requests a voice or data bearer service. The ISDN device passes along the information in the Call Setup message until it reaches the party you are calling, and then sends a Call Setup message to the ISDN device receiving the call. The called device routes the call to a telephone or to a computer, depending on whether the Call Setup message specifies voice or data bearer service. If the message specifies a data call, the device signals the computer. If the message specifies a voice call, the device rings the telephone. See also *bearer service*, *ISDN*.

ISDN D-channel signaling—A type of signaling in which a D channel handles WAN synchronization and signaling, and the B channels carry the user data. ISDN D-channel signaling is also called *out-of-band signaling*. T1 PRI, E1 PRI, and ISDN BRI lines use ISDN D-channel signaling. See also *B channel*, *D channel*, *E1 PRI line*, *ISDN BRI line*, *T1 PRI line*.

ISDN Digital Subscriber Line—See *IDSL*.

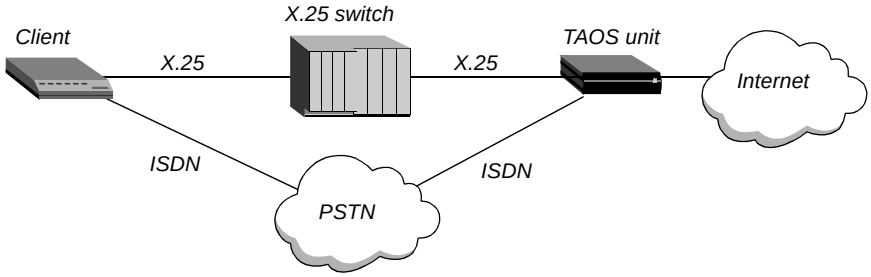
ISDN Disconnect message—A message that initiates the release of an ISDN connection. See also *ISDN*.

ISDN line—A line that uses ISDN D-channel signaling. E1 PRI, ISDN BRI, and T1 PRI are all examples of ISDN lines. See also *E1 PRI line*, *ISDN BRI line*, *ISDN D-channel signaling*, *T1 PRI line*.

ISDN modem—See *V.120 TA*.

ISDN packet mode—A feature that enables a client to dial in to a TAOS unit over a switched X.25 connection, and enables a TAOS unit to establish a switched X.25 connection supporting up to two X.25 sessions. If the client requires extra bandwidth, it can dial in to the TAOS unit. Figure 43 illustrates a configuration that uses ISDN packet mode.

Figure 43. ISDN packet mode



See also *X.25*.

ISDN PRI line—See *T1 PRI line*.

ISDN Primary Rate Interface line—See *T1 PRI line*.

ISDN Q.931 Layer 3 SETUP_ACK timer—See *T302 timer*.

ISDN subaddress—See *subaddress*.

ISDN User Part—See *ISUP*.

ISDX—Integrated Small Digital Exchange. ISDX is a telephone switch manufactured by GEC Plessey Telecom (GPT).

island—A group of networks on the Multicast Backbone (MBONE). The islands are connected by tunnels and support IP. See also *MBONE*.

ISLX—A DPNSS switch type. See also *DPNSS*.

ISO—International Standards Organization. The ISO is an international organization devoted to the definition of standards particular to national and international data communications. The U.S. representative to the ISO is the American National Standards Institute (ANSI).

ISP—Internet Service Provider. An ISP is a company that provides access to the Internet. By establishing Points of Presence (POPs) containing remote-access servers and a suite of user software packages, the ISP acts as a commercial on-ramp to the Internet. Providers typically charge a monthly fee, and supply technical support and advice to customers.

ISUP—ISDN User Part. ISUP is the Signaling System 7 (SS7) protocol for setting up, managing, and disconnecting trunk circuits carrying voice and data between a calling device and a called party. See also *SS7*.

ITU—International Telecommunication Union. Headquartered in Geneva, Switzerland, the ITU is an international organization that enables governments and the private sector to coordinate global telecommunication networks and services.

ITU Annex A—See *Frame Relay Annex A*.

ITU-T—International Telecommunication Union–Telecommunication Standardization Sector. The ITU-T is the committee that replaced the Consultative Committee for International Telegraphy and Telephony (CCITT) on March 1, 1993. The ITU-T is responsible for a wide array of telecommunications and networking standards.

J

Java—An object-oriented programming language developed by Sun Microsystems, Inc. You can use Java to create applets for distribution on the World Wide Web. Java programs run inside a Java-enabled Web browser or inside a Java Virtual Machine (JVM).

Java-based configurator—A utility that guides you through the configuration and management of a TAOS unit by means of a graphical user interface (GUI).

Java-Based Pipeline Configurator—See *JBPC*.

Java Virtual Machine—See *JVM*.

JBPC—Java-Based Pipeline Configurator. A JBPC is a graphical point-and-click interface that enables you to configure, save, and restore a configuration for a Pipeline unit over the same Ethernet connection that carries network traffic. See also *Pipeline*™.

JEDEC—Joint Electronic Device Engineering Council. JEDEC is an organization that creates and supervises industry standards for electronic devices. See also *JEDEC file*.

JEDEC file—A text file containing information for configuring a device. See also *JEDEC*.

jitter—A type of distortion found on analog communication lines, resulting in data transmission errors. A variation in the time it takes for a voice packet to traverse the link between sending and receiving end points. See also *jitter buffer*.

jitter buffer—In voice communications, an area of memory that holds a voice packet before the device plays out the audio data. See also *jitter*.

Joint Electronic Device Engineering Council—See *JEDEC*.

JVM—Java Virtual Machine. A JVM is an abstract computer that runs compiled Java code. The JVM is *virtual* because it is software that runs on top of a hardware platform and an operating system. All Java programs are compiled for a JVM. See also *Java*.

K

K56flex—A 56Kbps modem specification developed by Rockwell and Lucent Technologies for calls between a digital modem and an analog modem. K56flex allows 56Kbps data transfers on the downstream portion of a call, and 33.6Kbps data transfers on the upstream portion. See also *digital modem*, *modem*.

KB—A kilobyte, defined as 1024 bytes.

Kb—A kilobit, defined as 1024 bits.

Kbps—Kilobits per second, the amount of data transferred in a second between two end points. For example, 1Kbps is 1024 bits per second.

keepalive message—A message used by the Link Management Interface (LMI) of a Frame Relay port to verify link integrity. See also *LMI*.

keepalive registration—In a MultiVoice system, a process by which a TAOS unit reregisters with its currently registered gatekeeper at a specified interval. See also *MultiVoice™*, *registration.*

key system—Customer Premises Equipment (CPE) used to route calls within an organization and to and from the outside telephone network. A key system is a scaled-down version of a PBX, usually with less functionality, and is geared toward smaller organizations. A key system can be either analog or digital. Some digital key systems can terminate analog as well as digital connections. Moreover, key systems work in conjunction with channel banks to distribute channels from the T1/E1 circuit for voice, video, fax, and data. See also *CPE*, *E1 line*, *PBX*, *T1 line*.

kilobit—See *Kb*.

kilobits per second—See *Kbps*.

kilobyte—See *KB.*

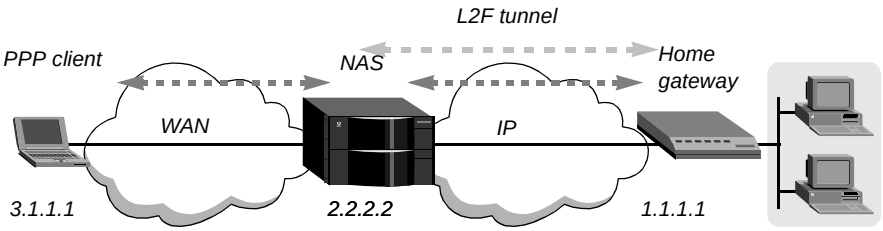
KR2 processing—A variation of R2 signaling for the Czech Republic. See also *R2 signaling*.

L

L2F—Layer 2 Forwarding. As specified by RFC 2341, L2F is a protocol that permits a system to tunnel the Data Link layer High-Level Data Link Control (HDLC) or Serial Line Internet Protocol (SLIP) frames associated with higher-level protocols, such as Point-to-Point Protocol (PPP). A TAOS unit can operate as an L2F Network Access Server (NAS) in communication with an L2F home gateway that is a Cisco router running IOS 11.3.

Figure 44 shows the elements of an L2F tunnel. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within PPP. The TAOS unit answers the call and passes it to the home gateway (a Cisco router running IOS 11.3). Communication between the NAS and the home gateway requires IP connectivity.

Figure 44. L2F tunneling



The connection to the home gateway is an Internet Protocol (IP) link, which consists of a control link and one or more data links. The control and data links use User Datagram Protocol (UDP) port 1701 and are encapsulated in UDP.

The control link carries information used to query whether the home gateway can accept the current call, and to establish a tunnel. L2F implements a periodic Hello mechanism by which the NAS and home gateway verify that the other is still operational. If the Hello message does not arrive within a specified period, the tunnels are disconnected. Each tunneled client connection has one data link, which consists of PPP frames.

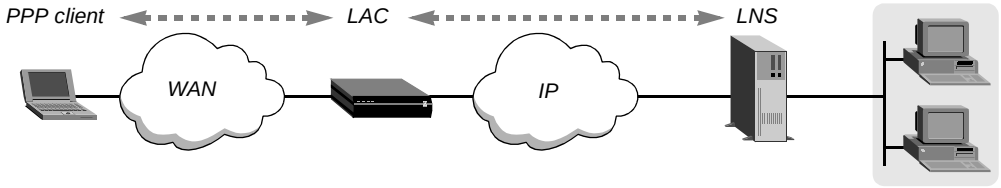
TAOS units support both shared-secret and distinct-secret L2F tunnel authentication. The default method is to use a shared secret between the tunnel end points.

See also *distinct secret*, *HDLC*, *home gateway*, *IP*, *NAS*, *PPP*, *shared secret*, *SLIP*, *tunneling*, *UDP*.

L2TP—Layer 2 Tunneling Protocol. As specified in RFC 2661, L2TP provides cross-Internet tunneling at OSI Layer 2. For example, L2TP provides tunneling at the High-Level Data Link Control (HDLC) layer of a Point-to-Point Protocol (PPP) connection.

The basic elements of an L2TP tunnel are shown in Figure 45. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within a PPP connection. A TAOS unit functioning as an L2TP Access Concentrator (LAC) answers the call and passes it to the LNS specified in the PPP client's profile. LAC-to-LNS communication requires IP connectivity.

Figure 45. L2TP tunnel

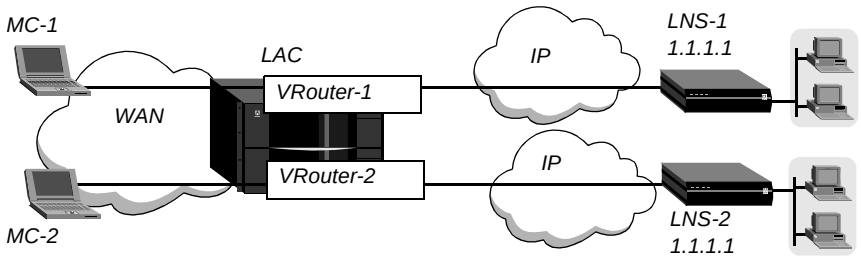


The L2TP Network Server (LNS) is the system that terminates the PPP connection from the client. All PPP negotiations with the client are handled by the LNS. Because it relies only on a connection with the LAC, the LNS can have only a single LAN or WAN interface. However, the LNS can still terminate calls that come into the LAC on a variety of PPP interfaces, such as asynchronous PPP, synchronous ISDN, and V.110.

The connection from the LAC to the LNS is an IP link, which consists of a control link and zero or more data links. Both the control and data links use UDP port 1701 and are encapsulated in UDP. The control link carries information used to query whether the LNS will accept the current call, and information used to establish a tunnel. L2TP implements a Hello mechanism by which the LAC and LNS verify that the other is still operational. They send each other a control message every minute or so. If the Hello message does not arrive for several minutes, the tunnel and all the tunneled connections are dismantled. Data links carry the client data, which consists of PPP frames. There is one data link per tunneled client connection.

L2TP tunnels can be built on the main Virtual Router (VRouter) and on specific VRouters. L2TP packets are sent through the configured VRouter for a particular tunnel. Because each VRouter maintains its own routing table and knows about only those interfaces that explicitly specify the same VRouter, this feature enables the system to separate traffic for different LNS systems. For example, Figure 46 shows two dial-in clients, MC-1 and MC-2. Each client tunnels to a different LNS, but both LNS systems have the IP address 1.1.1.1. Because the tunnels are built on separate VRouters, the traffic is kept separate and directed to the appropriate server end point.

Figure 46. L2TP tunnels built on separate VRouters



See also *LAC*, *LNS*, *VRouter*.

L2TP Access Concentrator—See *LAC*.

L2TP client—Layer 2 Tunneling Protocol client. An L2TP client is a dial-in user whose profile requires an L2TP tunnel. When the user is authenticated, the system builds a tunnel to the L2TP Network Server (LNS), which handles the Point-to-Point Protocol (PPP) connection. Both a local profile and a RADIUS user profile can initiate an L2TP tunnel on the basis of Dialed Number Information Service (DNIS) or Calling-Line ID (CLID) information, or after terminal-server or PPP authentication. See also *CLID*, *DNIS*, *L2TP*, *LNS*.

L2TP list attempt—A feature that enables a TAOS unit operating as an L2TP Access Concentrator (LAC) to use the DNS list attempt feature to attempt to connect to a series of server end points if the first attempt fails. See also *DNS list attempt*, *L2TP*, *LAC*.

L2TP Network Server—See *LNS*.

LAC—L2TP Access Concentrator. A LAC performs the following functions:

- Sends requests to L2TP Network Server (LNS) units, requesting creation of tunnels
- Encapsulates and forwards all traffic from clients to the LNS by means of the tunnel
- Decapsulates traffic received from an established tunnel, and forwards it to the client
- Sends tunnel-disconnect requests to LNS units when clients disconnect

A MAX unit can operate as a LAC or as an LNS. Any other TAOS unit with L2TP functionality can operate as a LAC only. See also *L2TP*, *LNS*.

LAN—Local Area Network. A LAN is a network in which two or more computers, located within a limited distance of one another, are connected in order to share files and resources. A PC-based LAN consists of a dedicated server running a network operating system and attached to several workstations. A host-based LAN consists of one or more hosts and terminals. Examples of LAN architectures are Ethernet, ARCnet, Fiber Distributed Data Interface (FDDI), and Token Ring. See also *ARCnet*, *Ethernet*, *FDDI*, *Token Ring*.

LAN adapter—See *NIC*.

landline telephone communication—A communications method in which a signal is carried over a copper local loop. Compare with *cellular communication*, *local loop*.

LAN packet display—A display of packet performance over a specified time, measured graphically or by counters.

LAN Service Unit—See *LSU*.

LAN-to-LAN modem access—A configuration in which two remote-access devices use a dial-up modem connection to route or bridge traffic between LANs. Compare with *dial-in modem access*, *dial-out modem access*. See also *dial-up line*.

LAN-WAN connectivity—The ability to link Local Area Networks (LANs) and Wide Area Networks (WANs). A wide range of tools, from translation protocols and communications features to support services, make a TAOS remote-access device an effective link between LANs and WANs. See also *LAN*, *WAN*.

LAP—Link Access Procedure. LAP is a protocol containing a subset of High-Level Data Link Protocol (HDLC) features. In order to maintain compatibility with HDLC, LAP was changed to create LAPB. See also *LAPB*.

LAPB—Link Access Procedure, Balanced. LAPB is a Layer-2 (Data Link) protocol for synchronous channels in packet-switching mode. It is an enhanced version of High-Level Data Link Control (HDLC). LAPB supports one data link per channel and is used, in particular, by X.25 and X.75. See also *B channel, packet switching, X.25, X.75*.

LAPB T1 timer—On an X.25 link, a value that specifies the maximum amount of time, in seconds, the transmitter should wait for an acknowledgment before initiating a recovery procedure. On a transmission line between a user and the network, a particular frame or acknowledgment can be incorrectly transmitted or discarded. To keep the transmitter from waiting indefinitely for an acknowledgment, you can specify the maximum amount of time the transmitter should wait. When you choose a value, you must take into account any frame transmission and processing delays you might encounter. In most cases, you should use the default value suggested by the network. See also *LAPB, X.25*.

LAPD—Link Access Procedure, D channel. LAPD is a Layer-2 (Data Link) protocol that transmits information between Network-layer devices across a Frame Relay network. The D channel transmits the signaling information. LAPD provides the mechanism for multiplexing multiple data links into a single channel, and for monitoring and controlling the flow of data. LAPD is used for ISDN D-channel signaling, for X.25 in the D channel, and as the base protocol for V.120. See also *D channel, ISDN D-channel signaling, V.120, X.25*.

LAPF—Link Access Procedure, Frame. LAPF is a protocol for Frame-mode bearer services. See also *bearer service*.

LAPM—Link Access Procedure, Modem. LAPM is a protocol for detecting and correcting data-communication errors occurring on the link between two modems. It is described by the ITU-T recommendation V.42. See also *V.42*.

LAT—Local Area Transport. Developed by Digital Equipment Corporation in 1981, the LAT protocol enables you to connect a number of asynchronous devices, such as terminals, printers, modems, and hosts, on an Ethernet network.

LATA—Local Access and Transport Area. A geographic area covered by one or more Local Exchange Carriers (LECs). See also *FGC, FGD, LEC*.

latency—For a communications channel, the amount of time before the channel is available for a transmission. For data transmissions, the amount of time it takes for a packet to reach its destination. The following elements contribute to latency:

- The type of physical media in use.
- Physical interference from noise or other signals.
- Required setup and teardown times.
- Signal interfaces. An Ethernet interface consumes a minimum of 0.3 milliseconds (ms). A 28.8 modem takes about 300 times longer.
- Bottlenecks, such as the 50ms it takes to move data through a serial port.
- Data conversion (for example, converting data from digital signals to the analog signals required by a modem).
- Compression.

Once latency is present, it cannot be optimized away. You must remove the cause. To maximize throughput, use the highest bandwidth available. All services go as fast as the medium allows. For example, if the medium is copper, the speed of the electrical signal through the copper does not vary with the type of line in use. A T1 line is considered faster than a single analog line only because its bandwidth is greater.

Layer 2 Tunneling Protocol—See *L2TP*.

Layer 2 Forwarding—See *L2F*.

LCN—Logical Channel Number. On an X.25 link, an LCN is a unique number assigned to one end of a Virtual Circuit (VC). See also *VC*, *X.25*.

LCP—Link Control Protocol. LCP sets up, manages, and disconnects a connection between two Point-to-Point Protocol (PPP) end points. See also *PPP*.

LCV—Line Code Violations. LCV indicates that the TAOS unit detected a Bipolar Violation on the DS3 or E1 line. One of the low-level rules for encoding data was violated on the receive signal. See also *DS3 line*.

Leaky Bucket Algorithm—An Asynchronous Transfer Mode (ATM) open-loop congestion control mechanism that enables a TAOS unit to regulate Variable Bit Rate (VBR) traffic at the entry point of the network.

When it has data to send, the host places the data flow's cells into the bucket. Cells drain out of the bottom of the bucket and onto the network. The rate is enforced by a regulator, called the Sustainable Cell Rate (SCR), at the bottom of the bucket. The bucket's size, called the Maximum Burst Size (MBS), limits how much data can build up waiting for entry onto the network. If the flow, known as the Peak Cell Rate (PCR), presents more data than the bucket can store, the excess data eventually begins to spill over the top of the bucket. Consequently, cells are delayed or discarded.

The primary effect of the Leaky Bucket Algorithm is to force a burst source of data into a flow of equally spaced cells. See also *ATM*, *MBS*, *PCR*, *SCR*, *VBR-NRT*, *VBR-RT*.

learning bridge—See *transparent bridge*.

leased address—In a network address translation (NAT) for LAN configuration, an IP address offered by a Dynamic Host Configuration Protocol (DHCP) server for a limited duration. See also *DHCP*, *DHCP server*, *IP address*, *NAT for LAN*.

leased channel—See *dedicated channel*.

leased circuit—See *dedicated circuit*.

leased line—See *dedicated line*.

lease time—As defined by the Dynamic Host Configuration Protocol (DHCP) in a network address translation (NAT) for LAN configuration, the time in which a host is assigned an IP address. If the host renews the address before its lease period expires, the DHCP service reassigns the same address. Plug-and-play addresses always expire in 60 seconds. See also *DHCP*, *DHCP server*, *IP address, leased address*, *NAT for LAN*.

Least Significant Bit—See *LSB*.

LEC—Local Exchange Carrier. An LEC is a local telephone company. See also *IEC*.

LED—Light Emitting Diode. An LED is a semiconductor light source that emits light in the optical frequency band or the infrared frequency band. A major light source for optical fiber transmission, LEDs are used with multimode optical fiber in applications that require a low-cost light source.

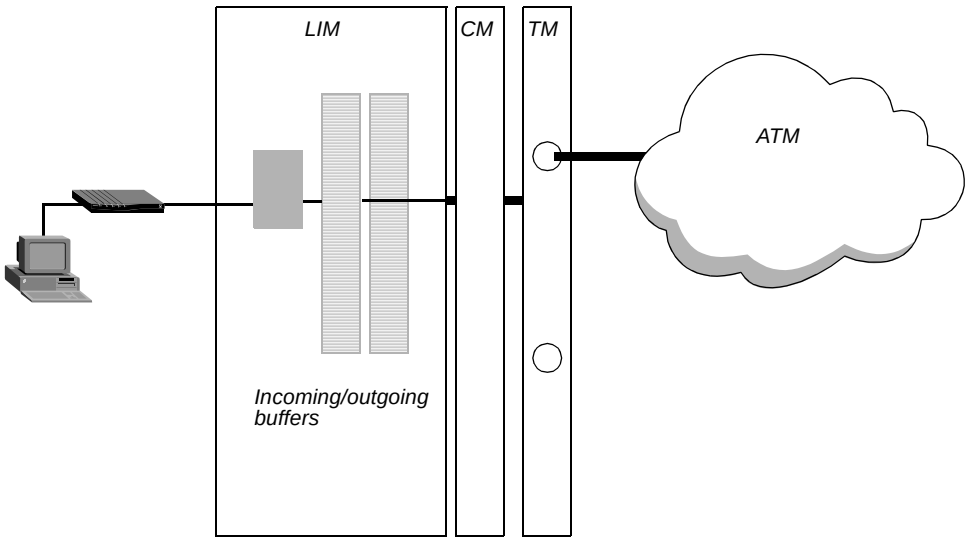
Level 2 Window Size—On an X.25 connection, the maximum number of sequentially numbered frames that a given DTE-DCE link can have unacknowledged at any given time. See also *DCE*, *DTE*, *X.25*.

LGN—Logical Group Node. In a Private Network-to-Network Interface (PNNI) configuration, a node that represents the lowest-level peer group in each higher-level peer group. See also *PNNI peer group*.

Light Emitting Diode—See *LED*.

LIM—Line Interface Module. On a Stinger unit, a module that communicates with xDSL subscriber-side Customer Premises Equipment (CPE). Each LIM performs per-port traffic management. Incoming cells received from the CPE are processed by the LIM and then queued for transmission to the Control Module (CM), as shown in Figure 47. Congestion occurs on the LIM when buffers become full.

Figure 47. Buffering incoming cell stream



Each LIM is responsible for verifying that traffic received from and transmitted to the CPE conforms to the Quality of Service (QoS) contract specified for the connection. The LIM polices the traffic stream on this basis, and if necessary, performs traffic shaping and congestion management. See also *CM*, *congestion management*, *CPE*, *QoS contract*, *traffic shaping*.

LIM port redundancy—Line Interface Module port redundancy. A feature that enables an individual port of a Line Interface Module (LIM) to be backed up by the corresponding port of a spare LIM. The LIM to be backed up (the primary LIM) must be of the same type as the spare. The remaining ports on the spare LIM remain available to back up other failed ports on any LIMs of the same type in the system.

More than one kind of LIM port can be backed up. An additional Line Interface Module-Path Selector Module (LIM-PSM) pair or Line Interface Module-Copper Loop Test module (LIM-CLT module) pair of another type installed in a Stinger can be used to back up other LIMs of that type in the system. For example, a spare SDSL LIM in slot 16 can back up any failed port on any other SDSL LIMs in the Stinger chassis. Likewise, a spare ADSL LIM in slot 14 can back up any failed ADSL ports.

However, because the midplane redundancy bus in a Stinger chassis contains only one path for each port number, port redundancy can back up only one path of a particular number at a time. When a port on a LIM that is being backed up is replaced, the Virtual Channels (VCs) for that port are terminated and set up on the spare. All other line parameters are also transferred to the spare port.

See also *automatic LIM port redundancy*, *CLT module*, *LIM*, *PSM*.

LIM redundancy—A Stinger feature that provides a one-to-one backup function for Line Interface Modules (LIMs). Each type of LIM to be backed up requires a spare LIM with a Path Selector Module (PSM) or Copper Loop Test (CLT) module plugged in behind or next to it. When the redundancy function is invoked, the primary LIM is deactivated. Its logical connections are terminated and then reestablished on the spare (secondary) LIM. When the redundancy function is disabled, the spare LIM is deactivated. Its logical connections are terminated and then reestablished on the primary LIM. See also *automatic LIM redundancy*, *CLT module*, *LIM*, *PSM*.

line—As a physical interface to the WAN, a line consists of one or more channels, each of which can transmit data. On a SONET network, a line consists of one or more sections, and line-terminating equipment originates and terminates the line signal. Compare with *path*, *section*. See also *channel*, *SONET*.

line buildout—See *buildout*.

Line Code Violations—See *LCV*.

Line Interface Module—See *LIM*.

Line Interface Module port redundancy—See *LIM port redundancy*.

Line Interface Module redundancy—See *LIM redundancy*.

Line Protection Module—See *LPM*.

Line Quality Monitoring—See *LQM*.

line-side connection—A link that extends from the telephone company's Central Office (CO) to the customer. Line-side connections can be high- or low-bandwidth, digital or analog. Compare with *trunk-side connection*. See also *analog line*, *digital line*.

Line Termination Mode—See *LT mode*.

Link Access Procedure—See *LAP*.

Link Access Procedure, Balanced—See *LAPB*.

Link Access Procedure, D Channel—See *LAPD*.

Link Access Procedure, Frame—See *LAPF*.

Link Access Procedure, Modem—See *LAPM*.

link compression—A process that removes redundancy from the data on a connection, enabling faster throughput. For a TAOS unit to use link compression, both sides of the connection must be configured to use the same compression method. You can use Stac compression (a modified version of draft 0 of the CCP protocol), Stac-9 compression (the method specified by draft 9 of the Stac LZS compression protocol), or Microsoft Stac compression (the method implemented by Windows 95). V.42bis is also a standard for link compression. For compression to be useful, the data link must be error corrected. See also *CCP*, *slot compression*, *V.42bis*, *VJ compression*.

Link Control Protocol—See *LCP*.

Link Management Interface—See *LMI*.

link quality monitoring—See *LQM*.

link state—The condition of an Open Shortest Path First (OSPF) link. See also *OSPF*.

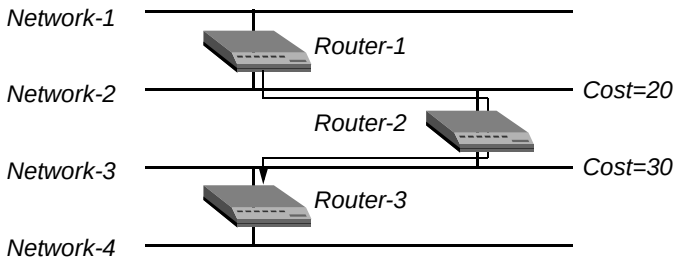
Link State Advertisement—See *LSA*.

link-state database—A database that contains Open Shortest Path First (OSPF) routing information. Link-state routing algorithms require that all routers within a domain maintain identical link-state databases, and that the databases describe the complete topology of the domain. An OSPF router's domain can be an Autonomous System (AS) or an area within one.

Based on the exchange of information, OSPF routers create a link-state database, which is updated on the basis of packet exchanges among the routers. Link-state databases are synchronized between pairs of adjacent routers. In addition, each OSPF router uses its link-state database to calculate a self-rooted tree of shortest paths to all destinations. The routing table is built from these calculated shortest-path trees. Externally derived routing data is advertised throughout the AS but is kept separate from the link-state data. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

For example, suppose you have the network topology shown in Figure 48.

Figure 48. Sample OSPF network topology

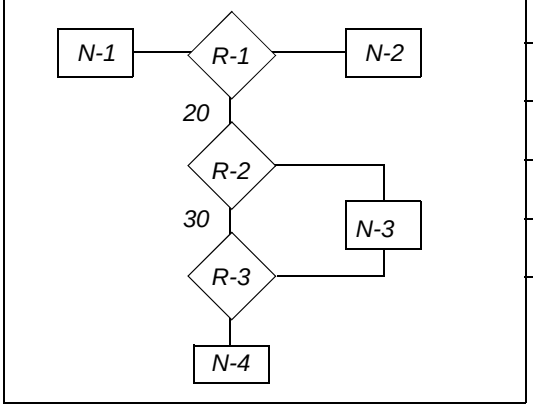


The cost value indicates the likelihood that the TAOS unit will use the interface to transmit data. The lower the cost, the more likely is the TAOS unit to use the interface. The following information appears in the link-state databases of the three routers:

Router-1	**Router-2**	**Router-3**
Network-1/Cost 0	Network-2/Cost 0	Network-3/Cost 0
Network-2/Cost 0	Network-3/Cost 0	Network-4/Cost 0
Router-2/Cost 20	Router-1/Cost 20	Router-2/Cost 30
	Router-3/Cost 30	

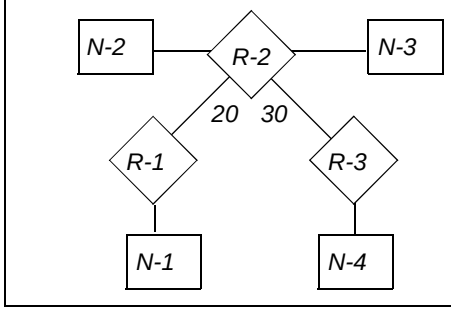
Each router builds a self-rooted shortest-path tree and then calculates a routing table stating the shortest path to each destination in the AS (Figure 49, Figure 50, and Figure 51).

Figure 49. Shortest-path tree and resulting routing table for Router-1



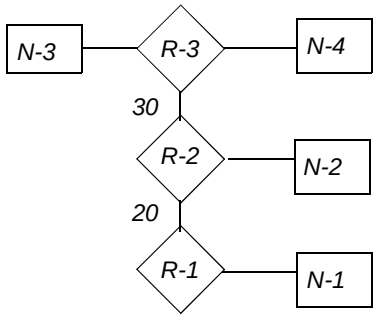
Destination	**Next hop**	**Metric**
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-3	50

Figure 50. Shortest-path tree and resulting routing table for Router-2



Destination	Next hop	Metric
Network-1	Router-1	20
Network-2	Direct	0
Network-3	Direct	0
Network-4	Router-3	30

Figure 51. Shortest-path tree and resulting routing table for Router-3



Destination	Next hop	Metric
Network-1	Router-2	50
Network-2	Router-2	30
Network-3	Direct	0
Network-4	Direct	0

See also *adjacency*, *AS*, *OSPF*.

link-state metric—A metric that takes into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network. Open Shortest Path First (OSPF) is a link-state protocol. Compare with *distance-vector metric*. See also *OSPF*.

Link-State-Request packet—An Open Shortest Path First (OSPF) request for an updated database. To make routing decisions, OSPF uses a link-state database of the network and propagates only changes to the database. See also *link-state database*, *OSPF*, *routing*.

link-state routing protocol—A sophisticated method of determining the shortest paths through the network. See also *OSPF*.

Link-State-Update packet—A packet exchanged between Open Shortest Path First (OSPF) routers for the purpose of updating link-state databases. See also *OSPF*, *router*.

list attempt—See *DNS list attempt.*

listening pattern—In an X.25/T3POS configuration, a called address that the Data Terminal Equipment (DTE) is expecting. Calls initiated by the host are answered by the DTE connecting to the T3POS PAD and listening for host-initiated calls. The host must send a called address matching the pattern the DTE is listening for. This pattern does not need to be a complete X.121 address, but could be a subpattern (including wildcard characters). See also *DTE*, *X.25/T3POS*, *X.121*.

LLC—Logical Link Control. In the IEEE's Local Area Network/Reference Model, LLC denotes a sublayer above the Media Access Control (MAC) sublayer. Combined, the LLC and MAC sublayers are equivalent to the Data Link layer in the OSI Reference Model. They give higher-level protocols access to the physical media. See also *MAC*, *OSI Reference Model*.

LMI—Link Management Interface. LMI is a synchronous polling scheme used for the link management of a Frame Relay channel. It provides the user with dynamic notification of the addition and deletion of Permanent Virtual Circuits (PVCs), and monitors each network connection through a periodic heartbeat keepalive polling process.

See also *DLCI*, *Frame Relay*, *heartbeat polling process*, *PVC.*

LNS—L2TP Network Server. An LNS performs the following functions:

- Provides Point-to-Point Protocol (PPP) functionality for L2TP clients.
- Responds to requests by L2TP Access Concentrator (LAC) units for the creation of tunnels.
- Encapsulates and forwards all traffic from the private network to clients by means of the tunnel.
- Decapsulates traffic received from an established tunnel, and forwards it to the private network.
- Disconnects tunnels on the basis of requests from the LAC.
- Disconnects tunnels on the basis of the expiration of the value you set. You can also manually disconnect tunnels from the LNS by means of SNMP, the terminal-server Kill command, or the DO Hangup command.

A MAX unit can operate as a LAC or as an LNS. Any other TAOS unit with L2TP functionality can operate as a LAC only. See also *L2TP*, *LAC.*

load balancing—A technique that distributes network traffic along parallel paths in order to maximize the available network bandwidth and provide redundancy.

Local Access and Transport Area—See *LATA.*

Local Area Network—See *LAN*.

Local Area Transport—See *LAT*.

local device—A device directly connected to the TAOS unit or residing on the local Ethernet network.

local DNS table—Local Domain Name System table. A local DNS table resides in the TAOS unit's RAM. It contains up to eight hostnames and one or more IP addresses for each hostname. The unit consults the local DNS table for address resolution only if requests to the DNS server fail. The local table acts as a safeguard to ensure that the TAOS unit can resolve the local set of DNS names if all DNS servers become unreachable or inoperable. The table can contain up to 35 IP addresses per hostname entry.

Following is a sample DNS table:

```
 Name                          IP Address       # Reads Time of last read
_____________________________ _________________ ________ _________________

 1: "barney"                   200.65.212.12 *   2       Aug 10 10:40:44 00
 2: "rafael"                   200.65.212.23     3       Aug 10  9:30:00 00
 3: "donatello"                200.65.212.67     1       Aug 11 11:41:33 00
 4: "wheelers"                 200.65.212.9      1       Aug 12  8:35:22 00
 5: "tiktok"                   200.65.212.148    4       Aug 12  7:01:01 00
 6: ""                         -------           -       ---
 7: "wilma"                    200.65.212.8      10      Aug 15 10:02:58 00
 8: ""                         -------           -       ---
```

The table contains the following fields:

Field	Description
`Name`	Hostname.
`IP address`	IP address. An asterisk (*) indicates that the entry has been automatically updated by a DNS query.
`# Reads`	Number of times the entry was read since it was created.
`Time of last read`	Time and date the entry was last read. The time and date appear only if Simple Network Time Protocol (SNTP) is in use. If SNTP is not in use, the field contains a row of hyphens.

See also *DNS*.

Local Exchange Carrier—See *LEC*.

local hunt-group number—A telephone number assigned to a hunt group for a single TAOS unit. Compare with *global hunt-group number*. See also *hunt group*.

local loop—The last segment of the carrier network. The local loop extends from a telephone company's Central Office (CO) to an end user's residence, and is still primarily used for analog connections. See also *CO*.

local loopback—A port diagnostic procedure in which data originating at the local site is looped back to its originating port without going out over the WAN. It is as though a data mirror were held up to the data at the WAN interface, and the data were reflected back to the originator. The serial port on the TAOS unit must be idle when you run the local loopback test. Compare with *remote loopback*. See also *analog loopback, digital loopback, loopback*.

Local mode—A data-transfer mode for calls on an X.25/T3POS network. In Local mode, error recovery is performed locally. The TAOS unit does not send supervisory frames across the X.25 network. The T3POS PAD is responsible for sending supervisory frames to the T3POS Data Terminal Equipment (DTE) device. Compare with *Binary Local mode*, *Blind mode*, *Transparent mode*. See also *DTE*, *PAD*, *supervisory frame*, *X.25/T3POS*.

local profile—A profile configured on the TAOS unit, in contrast to a user profile configured in RADIUS, TACACS, or TACACS+. See also *user profile*.

local user—A user at a device directly connected to the TAOS unit or residing on the local Ethernet network.

logical address—An address assigned by a network administrator to associate several devices with one another in a logical hierarchy or group. A router uses the logical address to help transmit a packet to its destination. An example of a logical address is an IP address. Compare with *hardware address*. See also *IP address*, *router*.

logical channel—One end of a packet-switched communications circuit between two or more network hosts. Many logical channels can exist simultaneously on a single physical channel. See also *LCN*, *VC*.

Logical Channel Number—See *LCN*.

logical gateway—On a MultiVoice gateway, a selected trunk group that a MultiVoice Access Manager (MVAM) device treats as a unique Voice over IP (VoIP) gateway. A MultiVoice gateway must have T1, T1 PRI, and T3 trunks to support logical gateways. See also *MultiVoice™*, *MVAM*, *T1 line*, *T3 line*.

Logical Group Node—See *LGN*.

logical interface—A Permanent Virtual Circuit (PVC) end point on a Frame Relay network. The logical interface requires a Data Link Connection Identifier (DLCI). A DLCI uniquely identifies the logical end point of a Virtual Circuit (VC). See also *DLCI*, *Frame Relay network*, *PVC*, *VC*.

Logical Link Control—See *LLC*.

logical port—A configured circuit that defines protocol interaction between a Frame Relay or Asynchronous Transfer Mode (ATM) switch and user equipment, a switch, or a network. Lucent Technologies supports the following logical-port configurations for Frame Relay:

- User-to-Network Interface–Data Circuit-terminating Equipment (UNI-DCE)
- User-to-Network Interface–Data Terminal Equipment (UNI-DTE)
- Network-to-Network Interface (NNI)
- Frame Relay Access Device (FRAD)
- PPP (Point-to-Point Protocol) Translation FRAD

Lucent Technologies supports the following logical-port configurations for ATM:

- ATM direct trunk
- ATM Interim Inter-switch Signaling Protocol–Data-Circuit-terminating Equipment (ATM IISP-DCE)
- ATM Interim Inter-switch Signaling Protocol–Data Terminal Equipment (ATM IISP-DTE)
- ATM User-to-Network Interface–Data Circuit-terminating Equipment (ATM UNI-DCE)
- ATM User-to-Network Interface–Data Terminal Equipment (ATM UNI-DTE)

See also *ATM*, *ATM direct trunk*, *ATM IISP-DCE*, *ATM IISP-DTE*, *ATM UNI–DCE*, *ATM UNI–DTE*, *FRAD*, *Frame Relay*, *NNI*, *PPP Translation FRAD*, *UNI-DCE interface*, *UNI-DTE interface*.

login prompt—The string used to prompt for a username in the terminal-server interface when authentication is in use and an interactive user initiates a connection. See also *terminal server*.

login timeout—The number of seconds a terminal-server user can use for logging in. After the specified number of seconds, the login attempt fails. See also *terminal server*.

Longitudinal Redundancy Check—See *LRC*.

loopback—A test in which a signal is sent to a destination and then returned to the sending device in order to test the connection between interfaces. See also *analog loopback*, *digital loopback*, *local loopback*, *remote loopback*.

loop-start signaling—A type of signaling in which the Customer Premises Equipment (CPE) signals an off-hook condition by closing a relay at the Central Office (CO). Compare with *ground-start signaling*, *wink-start signaling*.

low latency mode—A feature that allows real-time fax operation on networks with low packet loss and low latency characteristics (2.5 seconds or less of aggregate latency between pages). See also *real-time fax over IP*.

LPM—Line Protection Module. An LPM is a special backup module that acts as a spare Line Interface Module (LIM) for other LIMs in the system. See also *LIM*, *LIM redundancy*.

LQM—Link quality monitoring. LQM is a feature that enables a TAOS unit to monitor the quality of a link. When you enable LQM, the TAOS unit counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link-quality problems. LQM is described in RFC 1989.

LRC—Longitudinal Redundancy Check. LRC is an error-detection method that adds one character, known as the Block Check Character (BCC), to the end of each packet. The system determines the value of the first bit of the BCC by counting the number of 1s in the first bits of all the characters in the packet. It then sets the first bit of the BCC to 1 (one) if the sum is even, or to 0 (zero) if the sum is odd. The system determines the value of the second bit of the BCC by counting the number of 1s in the second bits of all the characters in the packet, then by counting the number of 1s in the third bits, and so forth. Compare with *CRC*.

LSA—Link State Advertisement. An LSA is a packet that describes various aspects of an Open Shortest Path First (OSPF) route. The LSA types are:

Type	Description
Type 1 (RTR)	Router-LSA that describes the collected states of the router's interfaces.
Type 2 (NET)	Network-LSA that describes the set of routers attached to the network.
Types 3 and 4 (STUB)	Summary-LSA that describes point-to-point routes to networks or Area Border Routers (ABRs).
Type 5 (ASE)	AS-external-LSA that describes routes to destinations external to the AS. An AS-external-LSA can also describe a default route for the AS.

See also *AS*, *ASE*, *ASE Type-5*, *OSPF*, *point-to-point link*, *route*, *router*.

LSB—Least Significant Bit. The lowest-order bit in a binary value. Compare with *MSB*.

LSU—LAN Service Unit. Part of the Multiband™ product, the LSU connects LAN bridges and routers to create WANs that use a combination of dedicated circuits and digital dial-up circuits. By creating such hybrid networks, you can match bandwidth to real-time traffic loads. See also *Multiband*™.

LSU packet—Link-State-Update packet. LSU packets are exchanged between Open Shortest Path First (OSPF) routers for the purpose of updating link-state databases. See also *OSPF*, *router*.

LT mode—Line Termination mode. LT mode is the termination point of a WAN connection. Typically, it is the Customer Premises Equipment (CPE). See also *CPE*, *WAN*.

M

MAC—Media Access Control. In the IEEE's Local Area Network/Reference Model, MAC denotes a sublayer below the Logical Link Control (LLC) sublayer. Combined, the LLC and MAC sublayers are equivalent to the Data Link layer in the OSI Reference Model. They give higher-level protocols access to the physical media. See also *LLC*, *MAC address*, *OSI Reference Model*.

MAC address—The six-byte hexadecimal address that the manufacturer assigns to the Ethernet controller for a port. See also *hardware address*, *MAC*.

management DLCI—A value that specifies a Permanent Virtual Circuit (PVC) or Switched Virtual Circuit (SVC) from a LAN to a switch over a Frame Relay network. See also *DLCI*, *Frame Relay*, *PVC*, *SVC*.

Management Information Base—See *MIB*.

manager—An application that receives Simple Network Management Protocol (SNMP) information from an agent. An agent and manager share a database of information, called the Management Information Base (MIB). An agent can use a message called a traps-PDU to send unsolicited information to the manager. A manager that uses the Ascend Enterprise MIB can query a TAOS agent, set parameters, sound alarms when certain conditions appear, and perform other administrative tasks. See also *agent*, *community name*, *MIB*, *SNMP*, *traps-PDU*.

mark pattern—A pattern of 1s (11111111) that a TAOS unit can use as the idle indicator on a dynamic Ascend Inverse Multiplexing (AIM) call. Compare with *flag pattern*.

mask—In a generic filter, a 12-byte value that a TAOS unit applies to a packet before comparing its contents to the value you include in a filter specification. The mask hides the bits that appear behind each binary 0 (zero). A mask of all ones (FF:FF:FF:FF;FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents. See also *generic filter*.

MAU—See *Ethernet transceiver*.

MAX™—A family of multiprotocol WAN access routers designed for central-site remote-access applications. A MAX unit offers the following features:

- Digital WAN access and services
- Digital and analog modems that dial in over channelized T1 PRI and E1 PRI access lines
- IP and IPX routing, bridging, and terminal-server functions
- Multiple-call aggregation for bandwidth-on-demand
- Multiple security methods
- Sophisticated management and control features
- Optional slot cards

See also *bandwidth-on-demand*, *bridging*, *digital modem*, *E1 PRI line*, *IP*, *IPX*, *T1 PRI line*, *terminal server*.

MAXDAX™—A type of software enhancement added to the MAX product, enabling the unit to cross connect videoconferencing, voice, and data traffic between T1 or E1 lines. The MAXDAX software gives users on multiple private networks access to each other and to the public network. See also *MAX™*.

maximum aggregate power level—The maximum output power allowed on the line at the transmitter output, expressed in dBm. A lower value means that the line consumes less power and has a lower capacity. A higher value means that the line consumes more power and has a higher capacity.

Maximum Burst Size—See *MBS*.

Maximum Receive Unit—See *MRU*.

Maximum Reconstructed Receive Unit—See *MRRU*.

Maximum Transfer Unit—See *MTU*.

MAX TNT®—Product name of a multiprotocol WAN access switch that enables carriers, Internet Service Providers (ISPs), corporations, and major network providers to offer a variety of access services, such as analog, ISDN, dedicated T1 and E1, and Frame Relay. A MAX TNT unit has a scalable, modular card-and-backplane architecture that lets you design solutions that satisfy your specific application and bandwidth requirements.

The MAX TNT system hardware consists of a shelf controller and redundant, load-balancing power supplies. You can enhance the base system by adding one or more slot cards. See also *analog data*, *dedicated line*, *DS0 channel*, *DS3 line*, *E1 line*, *Frame Relay*, *ISDN*, *T1 line*, *T3 line*.

MB—A megabyte, defined as 1,048,576 bytes.

Mb—A megabit, defined as 1,048,576 bits.

MBONE—Multicast Backbone. The MBONE is a virtual network layered on top of the Internet to support IP multicast routing across point-to-point links. Because multicasting is a fast and inexpensive way to communicate information to multiple hosts, the MBONE is used for transmitting audio and video on the Internet in real time.

The MBONE consists of groups of networks called *islands*. These islands are connected by tunnels and support IP. When a TAOS unit gains access to an MBONE network, it starts receiving MBONE multicasts. It resends the multicast packets to all of its own clients connected to it for MBONE service. The clients wanting MBONE service must implement Internet Group Membership Protocol (IGMP).

To the MBONE, the TAOS unit looks like a multicast client. The unit responds as a client to IGMP packets it receives from an MBONE router. The MBONE router can reside on the TAOS unit's Ethernet interface or across a WAN link. If the router resides across a WAN link, the TAOS unit can respond to multicast clients on its Ethernet interface and across the WAN. To multicast clients on a WAN or Ethernet interface, the TAOS unit looks like a multicast router, although it simply forwards multicast packets on the basis of group memberships.

See also *IP multicast forwarding*, *multicast*, *multicast heartbeat*, *multicast network*, *multicast rate limit*, *point-to-point link.*

MBONE interface—On a TAOS unit, the interface that connects to an MBONE router. See also *MBONE router*.

MBONE router—A router that directs multicast packets to a group of clients on a subscription list. See also *IP multicast forwarding, MBONE, MBONE interface, multicast, multicast heartbeat, multicast network, multicast rate limit.*

Mbps—Megabits per second, a unit for measuring data rates.

MBS—Maximum Burst Size. In an Asynchronous Transfer Mode (ATM) transmission, MBS is the maximum number of cells that can be received at the Peak Cell Rate (PCR). If the burst is larger than anticipated, the additional cells are either tagged or dropped. MBS applies only to Variable Bit Rate (VBR) traffic. It does not apply to Constant Bit Rate (CBR) or Unspecified Bit Rate (UBR) traffic. See also *ATM, CBR, PCR, UBR.*

MCR—Minimum Cell Rate. An Available Bit Rate (ABR) service traffic descriptor that specifies the minimum rate at which the source can send data over an Asynchronous Transfer Mode (ATM) connection. See also *ABR*, *ATM*.

MCU—Multipoint Control Unit. An MCU is a device that connects several videoconferencing units to create a videoconferencing session. See also *videoconferencing*.

MD5—Message Digest 5. MD5 is an algorithm for security applications in which a large message is compressed and then signed with a private key. MD5 takes a message of an arbitrary length and creates a 128-bit message digest. See also *authenticator field, CHAP, IPSec*, *SHA1*.

MD5-HMAC—Message Digest 5–Keyed Hashing for Message Authentication. MD5-HMAC represents version 2 of the MD5 algorithm. See also *hash value*, *IPSec*, *MD5*.

Media Access Control—See *MAC.*

Medium Access Unit—See *Ethernet transceiver*.

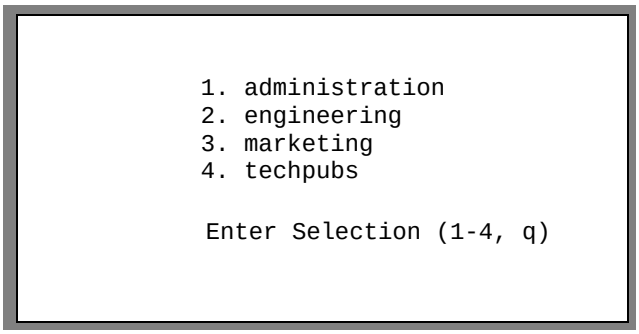
megabit—See *Mb*.

megabyte—See *MB.*

MegaMAX MP+—A MAX 6000 feature that enables you to set up several Multilink Protocol Plus (MP+) connections on a T1 or E1 line and specify that each connection use a different data service. For example, a MegaMAX MP+ session might use three H11 connections and three H0 connections. See also *H0 data service, H11 data service, MP+*.

menu mode—A mode in which the terminal server presents a banner message and a menu of hosts. In menu mode, a user cannot enter terminal-server commands, but can connect by means of Telnet, Rlogin, or raw TCP to the hosts an administrator specifies. The TAOS unit authenticates the user's login name and password, and then displays a text-based menu such as the one shown in Figure 52.

Figure 52. Menu mode



Users can connect to the specified host by pressing 1, 2, 3, or 4, or can quit the menu by pressing Q. Quitting the menu terminates the connection.

If you configure the menu locally, you can specify up to four hosts. If you configure the menu in RADIUS, you can configure up to ten. Compare with *command mode*, *immediate mode*. See also *RADIUS*, *Raw TCP*, *Rlogin*, *Telnet*.

message—Data transmitted from one location to another with a header field, information field, and trailer. The term *message* is often used interchangeably with *packet* and *frame*.

Message Digest 5—See *MD5*.

Message Digest 5–Keyed Hashing for Message Authentication—See *MD5-HMAC*.

Message Transfer Part—See *MTP*.

metric—A value that determines how quickly a packet can reach its destination. Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol use different types of metrics, which differ as follows:

- RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regardless of the speed or reliability of the link.
- OSPF is a link-state protocol. When determining the best path to a destination network, OSPF can take into account a variety of link conditions, such as the reliability or speed of the link.

See also *hop count*, *OSPF*, *preference*, *RIP*, *route*.

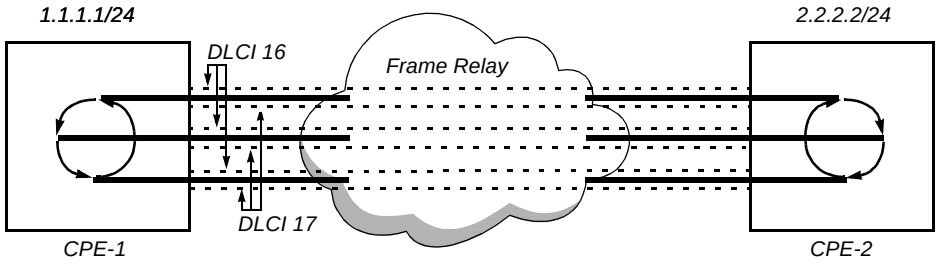
MFC-R2 signaling—Multifrequency Carrier R2 signaling. A standard for European analog and digital trunk signaling, MFC-R2 signaling requires handshaking on every multifrequency signaling digit. Compare with *DTMF-R2 signaling*. See also *R2 signaling*.

MFR—Multilink Frame Relay, a feature that enables the TAOS unit to bundle multiple Frame Relay data links so that they appear as a single logical data link with the aggregate bandwidth of the individual connections. The bundled links are referred to as an *MFR bundle*. See also *Frame Relay*, *MFR bundle*.

MFR bundle—Multilink Frame Relay bundle. An MFR bundle is a group of Frame Relay data links. The data links appear as a single logical data link with the aggregate bandwidth of the individual connections. Each data link within the bundle requires at least one Data Link Connection Identifier (DLCI) identifying the Virtual Circuit (VC) to the remote device (the MFR peer).

Figure 53 shows three bundled data links going through the Frame Relay network. Each Frame Relay link supports two DLCIs: 16 and 17. Data for each DLCI is sent to each of the member data links in a round-robin fashion.

Figure 53. MFR peers with three data links supporting two DLCIs

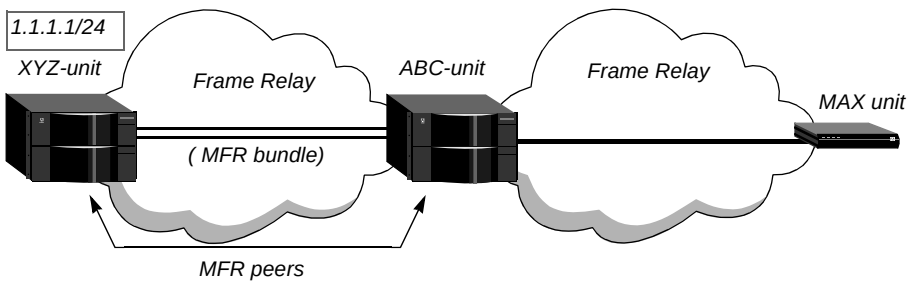


Because the DTE-DTE Permanent Virtual Circuit (PVC) goes through a non-MFR network, all of the individual links support the full User-to-Network Interface (UNI) standards. As long as one DLCI from any of the bundled data links is active, that DLCI is considered active by the higher layers. For example, if data link 1 is down and DLCI 16 in data link 2 is active, the MFR peers (CPE-1 and CPE-2) consider DLCI 16 to be active.

The bandwidth in an MFR bundle must be dedicated. All member data links of an MFR bundle must reside on the same card. See also *CPE*, *DLCI*, *DLCI bundling*, *DTE–DTE aggregation*, *Frame Relay network*, *PVC*, *UNI*.

MFR circuit switching—Multilink Frame Relay circuit switching. MFR circuit switching allows you to configure a circuit that switches an MFR bundle to another MFR bundle, or to a single data link. Data coming in on an MFR bundle (with multiple DLCIs) is switched to the other circuit end point, which can also support a single DLCI or an MFR bundle. Figure 54 shows a TAOS unit that switches between an MFR bundle on one side and single data link interface on the other.

Figure 54. MFR circuit switching from a bundle to a single T1 interface



For MFR circuit switching, both sides of the circuit must be DLCI interfaces. ATM-Frame Relay circuits are not supported with MFR. See also *circuit switching*, *DLCI*, *Frame Relay network*, *MFR*, *MFR bundle*.

MFR1 tones—Multifrequency Register 1 tones. A set of register signals used in R1 signaling for addressing purposes. See also *R1 signaling*.

MHRP—Mobile Host Routing Protocol. MHRP is a protocol designed to support the mobility of a host. Using MHRP, a developer can design a product that provides continuous network connectivity for traveling computer users.

MIB—Management Information Base. A MIB is a Simple Network Management Protocol (SNMP) database of information available to network-management programs. An agent creates a MIB. A network manager queries the MIB for information, and might create a MIB of its own. The MIB on the agent contains machine-specific information. The manager's MIB has more general information. See also *agent*, *manager*, *SNMP*.

Microcom Networking Protocol—See *MNP*.

Microsoft CHAP—See *MS-CHAP*.

Microsoft Point-to-Point Compression—See *MPPC*.

Microsoft Stac—Microsoft's version of the Stac LZS compression method. Compare with *Stac compression*, *Stac-9 compression*.

mild congestion—In Frame Relay, the state of a link when the data threshold is exceeded. When the link is mildly congested, the following occurs:

- All red frames are discarded.
- All frames transmitted on the mildly congested link are marked with the Forward Explicit Congestion Notification (FECN) bit.
- Before being forwarded to another link, all frames received on the mildly congested link are marked with the Backward Explicit Congestion Notification (BECN) bit.

Compare with *absolute congestion*, *severe congestion*. See also *BECN*, *congestion*, *FECN*, *red frame*.

Minimum Cell Rate—See *MCR*.

MNP—Microcom Networking Protocol. MNP is a communications hardware protocol developed by Microcom, Inc. Used by high-speed modems, MNP supports several classes of communication:

- Class 4 provides error detection, and can vary the modem's transmission speed in accordance with the quality of the line.
- Class 5 offers data compression, and can enable a device to double its transmission speed.
- Class 6 tries to detect the highest transmission speed supported by the modem at the other end of the connection, and then attempts to transmit data at that speed.

A modem can support more than one class. The most commonly used MNP classes are Class 4 and Class 5, also called MNP-4 and MNP-5, respectively. MNP-4 is the same as V.42 Annex A. See also *compression*, *V.42*.

mobile client—A user or device that gains access to a private home network across the Internet through an Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F) tunnel. Using ATMP, L2TP, or L2F, a traveling salesperson or technical support specialist can dial in to a local ISP and log in to his or her home network. See also *ATMP*, *home network*, *L2F*, *L2TP*.

Mobile Host Routing Protocol—See *MHRP*.

modem—MOdulator/DEModulator. A modem is Data Circuit-terminating Equipment (DCE) installed between Data Terminal Equipment (DTE) and an analog transmission channel, such as a telephone line. A modem takes digital data from a DTE device, modulates the 1s and 0s into analog form and sends the data over the channel. The receiving modem demodulates the analog signal into digital data and sends it to the DTE to which the modem is attached. Compare with *digital modem*. See also *analog data*, *analog signal*, *DCE*, *digital data*, *digital signal*, *DTE*.

modem dial-out—A feature that enables local users to connect to the terminal server by means of Telnet, and then issue AT commands to the digital modem as though connected locally to the modem's asynchronous port. You can configure a TAOS unit for modem dial-out to any Telnet port, or you can specify direct access to a particular Telnet port. See also *digital modem*, *direct-access dial-out*.

modem rate control—A method of controlling the downstream modem data rates for individual Asymmetric Digital Subscriber Line (ADSL) Customer Premises Equipment (CPE) user sessions. A TAOS unit initially establishes a CPE session at the maximum available data rate. If the CPE profile specifies a lower data rate, the unit terminates the session and then reestablishes it at the specified rate. The next time the CPE initiates a connection, the TAOS unit does not retrain if the initial rate is the same or lower than the rate used previously for that CPE. See also *ADSL*, *autobaud*, *CPE*, *digital modem*.

modem ringback—See *ringback tone*.

modem server—See *asynchronous communications server*.

modem speed—The data rate for analog-modem transmissions. Most modem users currently receive data and voice across the local loop by means of a modulation process that employs protocols such as V.32bis, V.34, or V.90. See also *local loop*, *modem*, *V.32bis*, *V.34*, *V.90*.

Mode Switch Frame—See *MSF*.

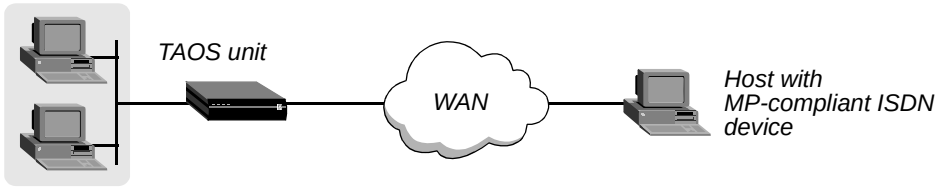
module—On a TAOS unit, hardware that provides functionality for the base system or that plugs into an expansion slot. See also *slot*.

Most Significant Bit—See *MSB*.

mount point—A directory at which a mounted file system is added to the device.

MP—Multilink PPP. MP uses the encapsulation defined in RFC 1990, enabling a TAOS unit to interact with MP-compliant equipment from other vendors. MP is an extension of Point-to-Point Protocol (PPP) and supports the ordering of data packets across multiple channels. Figure 55 shows an MP connection.

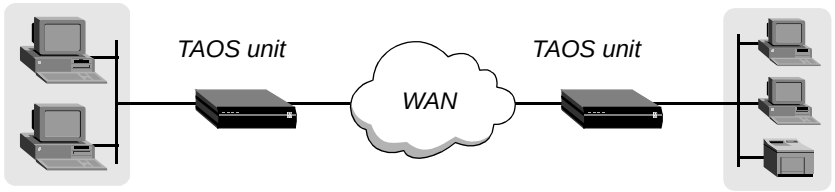
Figure 55. Multilink PPP (MP) connection



If you configure an MP connection and the TAOS unit cannot successfully negotiate the session, the unit falls back to using single-channel PPP. Compare with *MP+*, *PPP*.

MP+—Multilink Protocol Plus. MP+ uses Point-to-Point Protocol (PPP) encapsulation with Lucent Technologies extensions, as described in RFC 1934, to extend the capabilities of Multilink PPP (MP). MP+ supports session and bandwidth management, enabling a TAOS unit to connect to another TAOS unit by means of multiple channels. Using MP+, you can combine up to 30 individual channels into a single high-speed connection. The connection in Figure 56 uses MP+ encapsulation between two TAOS units.

Figure 56. Multilink Protocol Plus (MP+) connection



MP+ consists of two components:

- A low-level channel-identification, error-monitoring, and error-recovery mechanism
- A session-management level for supporting bandwidth modifications and diagnostics

MP+ enables a TAOS unit to add or remove channels from a connection as bandwidth needs change, without disconnecting the link. This capability is called Dynamic Bandwidth Allocation (DBA).

Both the dialing side and the answering side of the link must support MP+. If you configure an MP+ connection and the TAOS unit cannot successfully negotiate the link, the unit falls back to MP. If the TAOS unit also fails to negotiate an MP connection, the unit falls back to using single-channel PPP.

MP+ calls cannot combine an ISDN BRI channel with a channel on a T1 PRI line. Compare with *MP*, *PPP*. See also *DBA, ISDN BRI line, T1 PRI line.*

MPP—Multichannel Point-to-Point Protocol. This acronym has been superseded by MP+. See *MP+*.

MPPC—Microsoft Point-to-Point Compression. MPPC is a method of compressing Point-to-Point Protocol (PPP) packets transmitted between a Microsoft client device and a TAOS unit. The MPPC algorithm optimizes bandwidth to support multiple simultaneous connections. See also *PPP*.

MRRU—Maximum Reconstructed Receive Unit. MRRU is a packet field indicating that the system implements Multilink PPP (MP). The MRRU field is two octets, and specifies the maximum number of octets in the Information fields of reassembled packets. A system must be able to receive the full 1500-octet Information field of any reassembled MP packet, although it might attempt to negotiate a different value. See also *MP*.

MRU—Maximum Receive Unit. An MRU is the largest packet that a host on a link can receive. Compare with *MTU, MRRU.*

MSB—Most Significant Bit. The highest-order bit in a binary value. Compare with *LSB.*

MS-CHAP—Microsoft CHAP. MS-CHAP is a close derivative of Challenge Handshake Authentication Protocol (CHAP). However, CHAP is designed to authenticate WAN-aware secure software. It is not widely used to support remote workstations, on which an insecure plain text login might be required. MS-CHAP addresses this issue, integrating the encryption and hashing algorithms used on Windows networks. Microsoft Windows NT and LAN Manager platforms implement MS-CHAP. Compare with *CHAP*.

MSF—Mode Switch Frame. After the call has been established for an X.25/T3POS connection, the Data Terminal Equipment (DTE) sends the host an MSF to inform the host of the mode of the call. See also *DTE, X.25/T3POS*.

MTP—Message Transfer Part. On an SS7 network, MTP is a Transport-level protocol that consists of three levels:

- MTP Level 1 is equivalent to the OSI Physical layer, and defines the electrical characteristics of the link.
- MTP Level 2 is equivalent to the OSI Data Link layer. To guarantee reliable end-to-end transmission across a link, MTP Level 2 offers flow control, message sequencing, and error checking.
- MTP Level 3 is equivalent to the OSI Network Layer, and provides routing between nodes.

See also *OSI Reference Model, SS7, SS7 network.*

MTU—Maximum Transfer Unit. The size of the largest packet that can be transmitted over a particular medium. If a packet's size exceeds the MTU value, the packet must be fragmented or segmented, and then reassembled at the receiving end. Compare with *MRU*.

Mu-Law—See *U-Law*.

Multiband™—A family of bandwidth-on-demand controllers that use inverse multiplexing for setting up high-quality desktop, room, and multipoint videoconferencing operations. See also *inverse multiplexing, LSU, Multiband RPM™, VSU*.

Multiband PLUS™—A dynamic-bandwidth controller designed for users needing high-speed access for multiple applications. The Multiband PLUS provides bandwidth-on-demand at speeds from 56Kbps to 3Mbps and handles as many as four concurrent applications, including videoconferencing, LAN connectivity, electronic imaging, disaster recovery, private network backup, and private network overflow. See also *bandwidth-on-demand*.

Multiband Remote Port Module—See *Multiband RPM™*.

Multiband RPM™—Multiband Remote Port Module. A Multiband RPM is a self-contained port-extension device that allows Multiband products to communicate over regular copper wire and existing data jacks instead of special wiring. See also *Multiband™*, *Multiband PLUS™*.

multicast—A transmission method in which one device communicates with destination hosts by means of a single transmission to all recipients on a subscriber list. The IP multicast destination addresses are 224.0.0.0 through 239.255.255.255. See also *Frame Relay multicasting*, *IP multicast forwarding*, *MBONE*, *multicast heartbeat*, *multicast network*, *multicast rate limit.*

Multicast Backbone—See *MBONE*.

multicast default route—A route to the MBONE interface on a TAOS unit. When the TAOS unit acts as a multicast forwarder, and finds that there is no member in a particular group, it forwards multicast traffic for that group to the MBONE interface. See also *IP multicast forwarding*, *MBONE*.

multicast forwarding—See *Frame Relay multicasting*, *IP multicast forwarding*.

multicast group—A group of subscribers to whom a device sends multicast transmissions. Membership in a multicast group is voluntary. Using Internet Group Membership Protocol (IGMP), you can configure an application on your PC to declare itself a member of a multicast group. See also *IGMP*, *MBONE*, *multicast*, *multicast network.*

multicast heartbeat—A feature that enables you to monitor possible connectivity problems. Using the multicast heartbeat feature, you configure a TAOS unit to poll continuously for multicast traffic. Heartbeat monitoring is optional. It is not required for multicast forwarding. To set up heartbeat monitoring, you configure several parameters that define what packets will be monitored, how often the TAOS unit polls for multicast packets, and what threshold must be reached for the TAOS unit to generate an alarm. See also *MBONE*, *multicast*, *IP multicast forwarding*, *multicast network*, *multicast rate limit*, *SNMP*.

multicast network—A network in which a router sends packets to all addresses on a subscriber list. This type of network is different from both a unicast network (in which the router sends packets to one user at a time) and a broadcast network (in which the router sends packets to all users, whether they appear on a subscription list or not). The Multicast Backbone (MBONE) is an example of a multicast network. Compare with *broadcast network*, *unicast network.* See also *IP multicast forwarding*, *MBONE*, *multicast*, *multicast heartbeat*, *multicast rate limit*.

multicast rate limit—A way to limit the rate at which a TAOS unit accepts multicast packets from its clients. To begin forwarding multicast traffic on the MBONE interface, you must set the multicast rate limit to a number less than 100. For example if you set the limit to 5, the TAOS unit accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded. See also *IP multicast forwarding, MBONE, MBONE interface, multicast, multicast heartbeat, multicast network.*

Multichannel Point-to-Point Protocol—See *MPP*.

MultiDSL™—A family of products that provides multiple Digital Subscriber Line (DSL) services at speeds ranging from 128Kbps to 6Mbps. Supporting high-bandwidth applications such as remote access, Internet access, and telecommuting, MultiDSL includes Asymmetric Digital Subscriber Line (ADSL), ISDN Digital Subscriber Line (IDSL), Rate-Adaptive Digital Subscriber Line (RADSL), and Symmetric Digital Subscriber Line (SDSL). See also *ADSL*, *DSL*, *IDSL*, *RADSL*, *SDSL*.

Multifrequency Carrier R2 signaling—See *MFC-R2 signaling*.

Multifrequency Register 1 tones—See *MFR1 tones.*

multihomed host—A single Internet device connected to multiple data paths. Each link can reside on a different network.

multilink Frame Relay—See *MFR.*

multilink Frame Relay bundle—See *MFR bundle*.

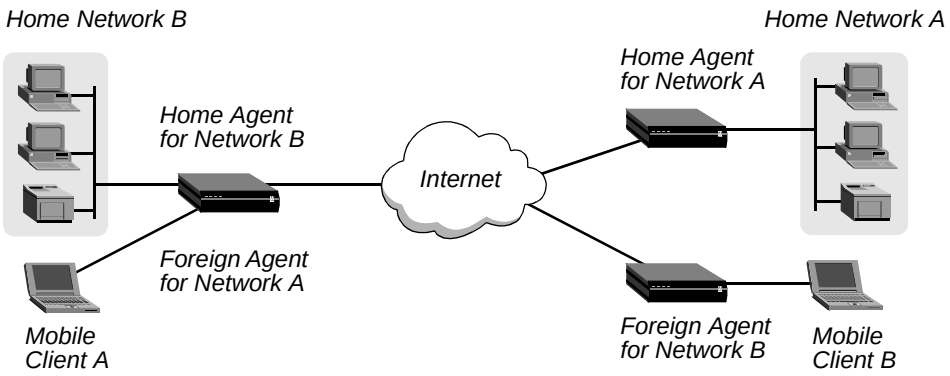
multilink Frame Relay circuit switching—See *MFR circuit switching*.

Multilink PPP—See *MP*.

Multilink Protocol Plus—See *MP+*.

Multimode Agent—A TAOS unit that acts as either a Home Agent or a Foreign Agent on a tunnel-by-tunnel basis in an Ascend Tunnel Management Protocol (ATMP) configuration. In Figure 57, the TAOS unit operates as a Home Agent for network B and as a Foreign Agent for network A.

Figure 57. TAOS unit acting as both Home Agent and Foreign Agent



See also *ATMP*, *Foreign Agent*, *Home Agent*.

multinetwork PVC—Multinetwork Permanent Virtual Circuit. A multinetwork PVC is a PVC that spans multiple Frame Relay networks. Multinetwork PVCs are interconnected across networks by Network-to-Network Interfaces (NNIs). See also *Frame Relay*, *NNI*, *PVC*.

multipath route—A static route that distributes the traffic load across multiple interfaces to a single destination. See also *route*, *static IP route*.

multipath route caching—A feature that enables the IP cache entries on slot card interfaces to distribute the load of packets meant for a particular destination among multiple gateways to that destination.

multiple-address NAT—Multiple-address network address translation. Multiple-address NAT provides a method of translating addresses for more than one host on the local network. The TAOS unit borrows an official IP address for each host from a Dynamic Host Configuration Protocol (DHCP) server on the remote network (or on a network accessible from the remote network).

When you use multiple-address NAT, hosts on the remote network can connect to any of the official IP addresses that the TAOS unit borrows from the DHCP server. If the local network must have more than one IP address visible to the remote network, you must use multiple-address NAT. If hosts on the remote network need to connect to specific hosts on the local network (not just specific services), you can configure the DHCP server to assign the same address when that local host requests an address.

When multiple-address NAT is enabled, the TAOS unit attempts to perform IP address translation on all packets received. It cannot distinguish between official and private addresses. See also *DHCP server*, *IP address*, *NAT for LAN*.

multiplexer—At one end of a communications link, a device that combines several lower-speed transmission channels into a single high-speed channel. A demultiplexer at the other end reverses the process. A multiplexer is sometimes called a *mux*. See also *multiplexing*.

multiplexing—The process of transmitting several signals over a single communications channel. See also *FDM*, *multiplexer*, *TDM*.

Multipoint Control Unit—See *MCU*.

multipoint link—A connection that links multiple hosts on a single line.

multipoint mode—A telephone service that provides a way for a single interface to have multiple telephone numbers.

multiprotocol routing—The ability to route multiple network protocols, including AppleTalk, IP, and IPX. See also *AppleTalk routing*, *IP routing*, *IPX routing*.

MultiRate—A data service on a circuit consisting of multiple B channels. The bandwidth of the circuit must be a multiple of 64Kbps. For example, a user can dial a first call at 384Kbps (using six B channels), and then dial a second call at 512Kbps (using eight B channels). MultiRate service is available over T1 PRI lines only. MultiRate is also known as the *Switched Nx64 data service*. See also *B channel*, *T1 PRI line*.

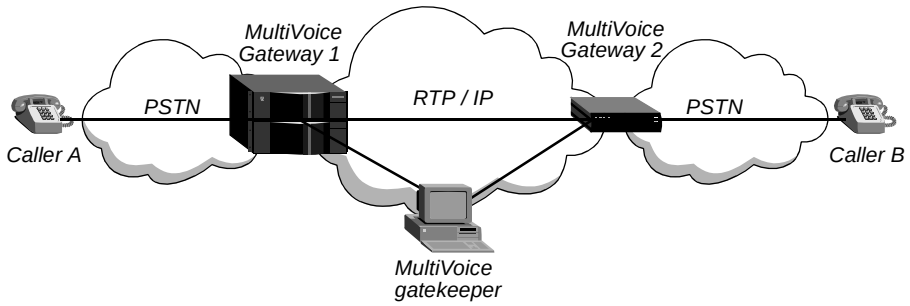
MultiVoice™—A family of Lucent Technologies products that supports Voice over IP (VoIP), transparent modem functionality, and real-time fax over IP. The following MultiVoice software licenses can be enabled on a TAOS unit:

- VoIP, which enables the TAOS unit to act as an H.323v2 MultiVoice gateway for transmission of real-time voice calls and transparent modem calls across IP networks.
- VoIP and SS7, which enables the TAOS unit to act as a MultiVoice gateway that communicates with a Signaling System 7 (SS7) signaling gateway to transmit real-time voice calls and transparent modem calls from an SS7 network across IP networks.
- Real-time fax (T.38) over IP, which uses the VoIP framework for call establishment, fax detection, and fax initiation.

A VoIP-enabled TAOS unit operates as a MultiVoice gateway. Callers dial in to a local TAOS unit through the Public Switched Telephone Network (PSTN). The TAOS unit then communicates with a MultiVoice gatekeeper to establish communication channels to a remote MultiVoice gateway. Workstations running MultiVoice Access Manager (MVAM) software operate as H.323 MultiVoice gatekeepers. The gatekeepers handle all call control functions, including bandwidth control, authentication, call detail reporting (CDR), and alias translation.

In the sample configuration shown in Figure 58, two gateways connect Caller A to Caller B. A system running MVAM performs the H.323 gatekeeper functions.

Figure 58. MultiVoice in H.323 environment



When Caller A dials Caller B, the following events occur:

1 Caller A dials Gateway 1, and enters his or her PIN authentication (if required) and Caller B's telephone number.

2 Gateway 1 establishes a session with the gatekeeper, and then forwards the telephone number and PIN authentication to the gatekeeper.

3 The gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.

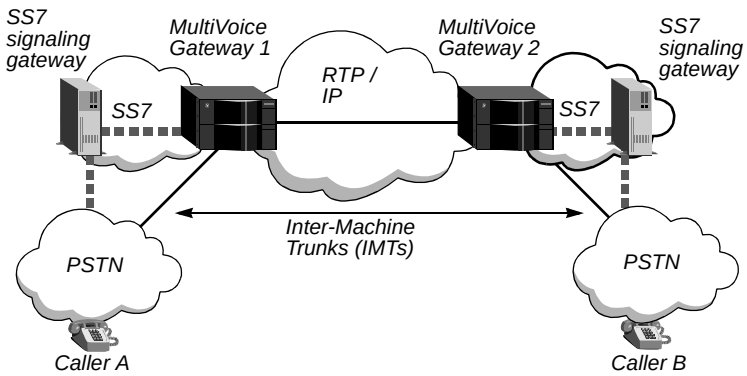
4 Gateway 1 establishes a session with Gateway 2.

5 Gateway 2 forwards the call request to Caller B.

6 When Caller B answers the telephone (goes off-hook), voice traffic is tunneled in IP packets between Gateway 1 and Gateway 2.

In an SS7 environment, a VoIP-enabled TAOS unit acts as a MultiVoice gateway that communicates with an SS7 signaling gateway to establish communication channels to a remote MultiVoice gateway. The SS7 signaling gateways initiate and manage call setup and release, and execute call routing. Each signaling gateway communicates call setup information to the TAOS unit by means of IPDC 0.15. IPDC message tags define voice encoding type, packet loading, IP and Real-Time Transport Protocol (RTP) ports, and other variables used for processing VoIP calls. In the sample gateway configuration shown in Figure 59, the gateways support VoIP calls controlled by IPDC over Inter-Machine Trunks (IMTs) for SS7 calls originating from the PSTN.

Figure 59. MultiVoice in SS7 environment



When Caller A dials Caller B, the following events occur:

1 Caller A dials the number for the SS7 service provider plus Caller B's telephone number. For example, Caller A dials a number such as 10-10-999-1-888-555-1212.

2 The signaling gateway assembles call routing information and other information required to connect the call.

3 The signaling gateway then sends an SS7 message to the PSTN to ring Caller B's telephone.

4 The signaling gateway uses IPDC to initiate a connection across the packet network between Gateway 1 and Gateway 2. The signaling gateway sends IPDC setup information to both Gateway 1 and Gateway 2.

5 When Caller B answers the telephone (goes off-hook), the signaling gateway converts the SS7 signals into IPDC packets, and voice traffic is tunneled in IP packets between Gateway 1 and Gateway 2 by means of RTP.

6 Gateway 2 passes the IPDC packets to the signaling gateway at the remote end, which converts the IPDC packets to SS7 messages and routes the call across the appropriate signaling links to Caller B.

Real-time fax calls begin when a VoIP call is placed from an originating fax machine to the destination fax machine. If the TAOS unit is configured to perform out-of-band Dual Tone Multi-Frequency (DTMF) signaling, a Digital Signal Processor (DSP) automatically enables inband DTMF signaling at the start of the fax call. When the destination fax machine picks up the call and sends an answer tone, the destination gateway detects this tone and initiates a switchover to real-time fax on both itself and the gateway at the other end of the call. When the switchover is complete, the fax transmission proceeds normally.

See also *DTMF*, *DSP*, *gatekeeper*, *gateway*, *H.323*, *IPDC*, *IMT*, *IP network*, *MVAM*, *MultiVoice™ Gateway*, *MultiVoice™ Gatekeeper*, *PSTN*, *QoS*, *real-time fax over IP*, *RTP*, *SS7 network*, *T.38*, *transparent modem*, *VoIP*.

MultiVoice™ Access Manager—See *MVAM*.

MultiVoice™ Gatekeeper—A MultiVoice component that supports the International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) H.323 standard for managing an IP network. A computer running the MultiVoice Gatekeeper component of the MultiVoice Access Manager (MVAM) software supports all gateways, user profiles, and authentication. See also *MultiVoice™*, *MultiVoice™ Gateway*, *MVAM*.

MultiVoice™ Gateway—A MultiVoice component that supports the International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) H.323 standard for transmitting voice over an IP network. When a voice call is received at a local unit using the MultiVoice Gateway software, the gateway uses voice-compression technologies and standard protocols to compress the voice data, divide it into packets, and transmit it. At the remote end, the process is reversed and the call is delivered over the remote packet network to its intended destination. See also *H.323*, *MultiVoice™*, *MultiVoice™ Gatekeeper*.

mux—See *multiplexer*.

MVAM—MultiVoice™ Access Manager. MVAM is a MultiVoice component that provides the following features:

- Telephone-to-IP address translation
- Web-based administration interface
- PIN-based user authentication
- Voice Virtual Private Network (VPN) support
- Telephone number aliases
- Call detail reporting (CDR)
- Gateway and user database support
- Third-party billing system support

See also *CDR*, *MultiVoice™*, *VPN*.

N

NADH—North American Digital Hierarchy. A digital hierarchy created by AT&T, the NADH defines the rate and format of T-carrier and E-carrier digital communication circuits. This classification is referred to as the Digital Signal level (DSx), and is related to the following T-carrier and E-carrier designations:

DSx	For T-carrier circuits			For E-carrier circuits		
	T-carrier equivalent	**Number of 64Kbps channels**	**Data rate**	**E-carrier equivalent**	**Number of 64Kbps channels**	**Data rate**
DS0	Fractional T1 (1/24th)	1	64Kbps	Fractional E1 (1/30th)	1	64Kbps
DS1	T1	24	1.544Mbps	E1	30	2.048Mbps
DS2	T2	96	6.31Mbps	E2	120	8.448Mbps
DS3	T3	672	44.7Mbps	E3	480	34.37Mbps
DS4	T4	4032	274.14Mbps	E4	1920	139.3Mbps

See also *DSx, E-carrier circuit, T-carrier circuit*.

nailed channel—See *dedicated channel*.

nailed circuit—See *dedicated circuit*.

nailed line—See *dedicated line*.

nailed-up channel—See *dedicated channel*.

nailed-up circuit—See *dedicated circuit*.

nailed-up line—See *dedicated line*.

NAK—Negative Acknowledgment. A NAK is a packet sent from a receiver to a sender, informing the sender that data is missing or corrupted. When a device receives a packet, it sends back either an ACK packet or a NAK packet to the sending device. If all the data arrived without corruption, the receiving device sends an ACK. If some of the data is missing or corrupted, the receiving device sends a NAK, which acts as a request that the sender retransmit the data.

name and password authentication—A form of authentication in which a TAOS unit attempts to match a caller's username and password to the parameters or attributes specified in a profile. See also *authentication, RADIUS, RADIUS server, TACACS, TACACS+*.

Name Binding Protocol—See *NBP*.

name server—A server that converts network names into network addresses. See also *DNS, primary DNS server, secondary DNS server*.

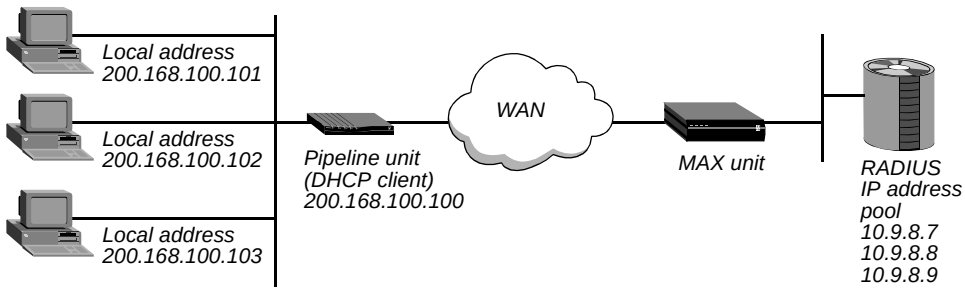
NAPT—Network Address Port Translation. A protocol that enables hosts on a private network domain to gain access to hosts in an external network by means of a single registered address. NAPT works by multiplexing Transport-layer identifiers of private hosts into the Transport-layer identifiers of a single assigned address. NAPT supports only applications based on Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP). Compare with *NAT for LAN*. See also *ICMP*, *TCP*, *UDP*.

NAS—Network Access Server. An NAS is a device that provides LAN and WAN access for network hosts.

NAT for LAN—Network address translation for LAN. NAT for LAN is a feature that enables a Pipeline unit to connect a LAN to a remote network even if devices on the LAN have addresses that are not valid for the remote network. The Pipeline unit translates between the local network addresses and the remote network addresses.

Access to public networks requires the use of an official IP address that is unique across the entire network. Typically, a central authority assigns a range of addresses, and a local administrator distributes them. If access to a public network is not necessary, the local manager can assign addresses as he or she sees fit, even if the addresses are unofficial or belong to another company. Because the supply of addresses is rapidly diminishing, a company might not be able to get official addresses for its entire network. A site might already have unofficial addresses, but now needs access to the Internet, which requires an official address. For these reasons, you might need a facility for borrowing an official address and dynamically translating between the local and official addresses. NAT for LAN provides this facility. Figure 60 illustrates a basic NAT for LAN setup.

Figure 60. NAT for LAN setup



In Figure 60, the Pipeline unit itself does not have an address on the remote network. Therefore, clients can access the unit only from the local network, not from the WAN. When a client on the LAN requests access to the remote network, the Pipeline unit gets an address for the client from the MAX unit. When subsequent clients request access to the remote network, the Pipeline unit sends the MAX unit a DHCP request packet, asking for an address. In return, the MAX unit sends an address from its IP address pool. The Pipeline unit uses the dynamic addresses it receives from the MAX unit to translate IP addresses on behalf of local clients.

As it receives packets on the LAN, the Pipeline unit determines whether the source IP address has a corresponding translated address. If so, the unit translates the packet and forwards it out over the WAN. If the Pipeline unit has not assigned a translated address (and one is not pending), the unit issues a new DHCP request for the IP address. While waiting for the MAX unit to offer an IP address, the Pipeline unit drops corresponding source packets. For packets it receives from the WAN, the Pipeline unit checks the destination address against its table of translated addresses. If the destination address exists and is active, the unit forwards the packet. If the destination address does not exit, or is not active, the unit drops the packet.

You can set up either multiple-address NAT or single-address NAT. See also *IP address*, *multiple-address NAT*, *single-address NAT*.

National Center for Supercomputing Applications—See *NCSA*.

National Institute of Standards and Technology—See *NIST*.

native E.164 address—An ISDN number that designates an Asynchronous Transfer Mode (ATM) end point. A native E.164 address can contain up to 15 ASCII digits. Compare with *AESA format*. See also *ATM*.

NavisAccess™—An application that delivers superior management for the dial-up and dedicated portions of the network, providing extensive support for discovery and mapping, device configuration, fault and performance management, and security. See also *NavisRadius*™.

NavisConnect™—A Java-based configuration utility for a MAX TNT unit.

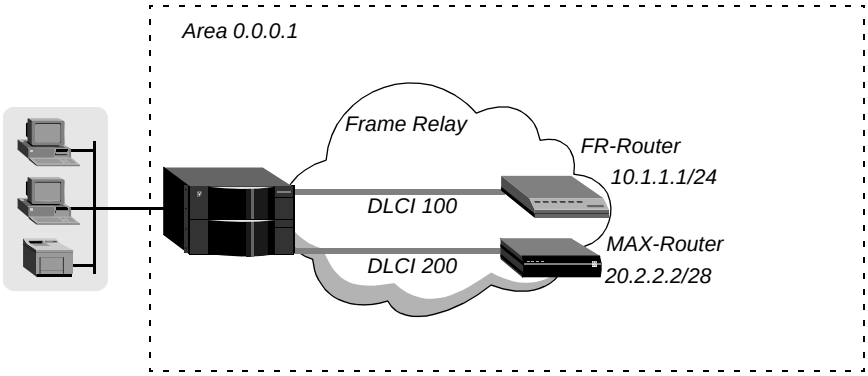
NavisRadius™—A software package that provides authentication, authorization, and accounting services. NavisRadius enables you to authenticate users, configure incoming WAN connections, configure dial-out connections, establish routes, install filters, and gather accounting data. See also *RADIUS*.

NBMA network—Non-Broadcast Multi-Access network. An NBMA network is an Open Shortest Path First (OSPF) network that has multiple points of access (more than two routers) and does not support broadcast capability. Frame Relay and X.25 are typically NBMA networks.

OSPF routers operate on an NBMA network much as they do on a broadcast network, using the Hello protocol to form adjacencies and identify the Designated Router (DR). A TAOS unit can form adjacencies with other OSPF routers on an NBMA network. These adjacencies enable the unit to route OSPF over Frame Relay networks, and to interoperate with the switches that do not support the serial (point-to-point) model over Frame Relay.

Figure 61 shows an OSPF NBMA network using Frame Relay. The system named FR-Router is eligible to become the DR. The MAX-Router unit is not DR-capable.

Figure 61. NBMA network



A router that is eligible to become the DR is configured with a list of all other OSPF routers connected to the network. At startup, these routers send Hello packets to each other to discover the DR. The DR then begins sending Hello packets to the entire list of routers on the network. When an NBMA interface becomes active on the TAOS unit, it sends Hello packets only to neighboring routers that are eligible to become the DR, until it is notified about which router is the DR.

See also *DR*, *Frame Relay*, *OSPF*, *X.25*.

NBP—Name Binding Protocol. NBP is an AppleTalk protocol that enables you to make your application visible to users on an AppleTalk network. NBP associates the socket address assigned to a process or application with a name that contains three parts: the object, type, and zone fields. See also *AppleTalk*, *zone*.

NCP—NetWare Core Protocol. NCP is a protocol that enables an IPX server to respond to client requests. See also *IPX server*.

NCP—Network Control Protocol. NCP is a collection of protocols for setting up and configuring Network-layer protocols over Point-to-Point Protocol (PPP). See also *PPP*.

NCSA—National Center for Supercomputing Applications. The NCSA is the home of the first Web browser with a Graphical User Interface (GUI).

Near-End Block Error—See *NEBE*.

Nearest Server Query—See *IPX Nearest Server Query*.

NEBE—Near-End Block Error. A signal that the remote end sends to indicate that it has detected an error in the data it has transmitted. A block error is detected each time the calculated checksum of the data does not correspond to the control checksum transmitted in the successive superframe. One block error indicates that one superframe has not been transmitted correctly. No conclusion with respect to the number of bit errors can be drawn. Compare with *FEBE*.

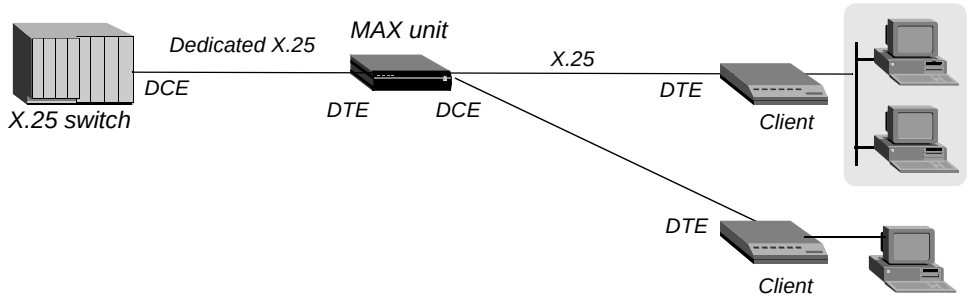
negative acknowledgment—See *NAK*.

neighbor node—In a Private Network-to-Network Interface (PNNI) configuration, a node that is directly connected to another node by means of a logical link. See also *PNNI*.

neighbors—Open Shortest Path First (OSPF) routers that have interfaces to a common network. On multiaccess networks, neighbors are dynamically discovered by OSPF Hello packets. See also *Hello packet*, *OSPF*.

Net2Net circuit mode—A method of routing incoming calls to a dedicated X.25 connection by enabling several X.25 clients to share a single connection into the X.25 switch network. In Figure 62, the X.25 switch connects to a MAX unit. To the X.25 switch, the MAX unit is a terminating device or a Data Terminal Equipment (DTE) device. To the clients, the MAX unit is an X.25 switch or a Data Communications Equipment (DCE) device.

Figure 62. Net2Net circuit mode



See also *X.25*.

NetBIOS—Network Basic Input/Output System. Developed by IBM, NetBIOS is a protocol that provides network access to upper-layer programs. NetBIOS functionality includes that of the Session, Presentation, and Application layers of the OSI Reference Model, and provides naming services, connectionless best-effort datagram delivery, and support for virtual circuits. See also *OSI Reference Model*.

NetWare Core Protocol—See *NCP*.

NetWare server—See *IPX server*.

network—A group of computers, often called *hosts*, *nodes*, or *stations*, that are connected to one another for the purpose of sharing files and other resources. Each computer has a Network Interface Card (NIC) that enables it to gain access to the network. Each host can have one or more peripherals (such as a fax modem or printer) attached to it. Each peripheral can be shared with other network users or can remain private to the individual computer.

Network Access Server—See *NAS*.

network adapter—See *NIC*.

network address—An address shared by all the hosts on the same physical network.

Network Address Port Translation—See *NAPT*.

network address translation for LAN—See *NAT for LAN*.

network alignment—A method of setting up IP address pools for pool summary. When you perform network alignment, you make sure that the first address in the pool is the first host address, and that the maximum number of entries you specify is two fewer than the total number of addresses in the pool. See also *IP address*, *pool summary*.

Network Basic Input/Output System—See *NetBIOS*.

network board—See *NIC*.

network card—A slot card used to establish and maintain the physical connection for a call. A network card does not support protocol stacks, but relies on another card to remove link encapsulation and process the call's protocol information. Compare with *host card*. See also *dual-capacity card*, *slot card*.

Network Control Protocol—See *NCP*.

Network File System—See *NFS*.

Network Information Center—See *InterNIC*.

Network Information Service—See *NIS*.

Network Interface Card—See *NIC*.

Network layer—Layer 3 in the OSI Reference Model. The Network layer provides address resolution and routing protocols. Address resolution enables the Network layer to determine a unique network address for a node. Routing protocols enable data packets to flow between networks and reach their proper destinations. See also *OSI Reference Model*, *routing*.

network management—See *NM*.

Network News Transfer Protocol—See *NNTP*.

network number—See *IP network number*, *IPX network number*.

network port—A channel on a T1 or E1 line. A TAOS unit always places or receives calls on a network port. See also *E1 line*, *T1 line*.

network range—A contiguous range of integers (with the range of 1 through 65,199) assigned to an AppleTalk network. Each network range must be unique. No two networks can use the same range, and no two network ranges can overlap.

In order for a TAOS unit to receive calls from dial-in AppleTalk Remote Access (ARA) clients, you must define a virtual AppleTalk network by specifying a network range. Each number in the range can be associated with up to 253 nodes, so the range determines how many AppleTalk clients can dial in to the TAOS unit. For example, a network with a range of 1000 through 1002 could support up to 3 x 253, or 759, clients.

See also *AppleTalk routing*, *ARA*, *virtual AppleTalk network*.

Network Service Access Point—See *NSAP*.

Network Service Provider—See *NSP*.

Network Services Part—See *NSP*.

network side—The Central Office (CO) end of an ISDN connection. Because ISDN links exist only between the CO and the customer, an ISDN link can be viewed as having two sides: the network side, where the Network Terminating (NT) equipment resides, and the user side, where the Terminal Equipment (TE) resides. The user side can connect only to the network side, and vice versa. Compare with *user side*.

network-side address—The interface address of the line on which a TAOS unit sends an outgoing call. A call switched to a local ISDN BRI line is an example of a route to a network-side address. Compare with *host-side address*.

network switch—A network device that selects a path or circuit for sending data to its next destination.

Network Terminating equipment—See *NT equipment*.

network tone cut-through—A feature that provides answer-supervision support for TAOS unit gateways that use non-PRI trunks. Network tone cut-through enables each TAOS unit to pass call-progress tones across the IP network for Voice over IP (VoIP) calls. Call-progress tones generated by a distant Public Switched Telephone Network (PSTN) are passed between the two TAOS unit gateways processing the call. When a remote gateway receives call progress tones from the PSTN, the tones are stored as voice frames, and then transmitted across the IP network in Real-Time Transport Protocol (RTP) packets. Upon receiving the RTP packets, the local gateway decodes and sends these tones to the calling end point. Network tone cut-through is also known as *far end cut-through*. See also *PSTN, RTP, VoIP*.

Network-to-Network Interface—See *NNI*.

Network User Identification—See *NUI*.

Network Virtual Terminal—See *NVT*.

Network Virtual Terminal ASCII—See *NVT ASCII*.

Network Voice Protocol—See *NVP*.

next-generation public network—A packet-switched network that integrates data, fax, video, and voice transmissions. See also *packet-switched network*.

next-hop router—The router that is one hop away from another device. See also *hop, router*.

NFAS—Non-Facility Associated Signaling. NFAS is a special case of ISDN signaling in which two or more T1 PRI lines use the same D channel and you can add a backup D channel. NFAS is required for the Switched-1536 data service. Because all 24 channels of the T1 PRI line carry user data, the D channel must be on another line. See also *D channel, Switched-1536, T1 PRI line*.

NFS—Network File System. NFS is an Application-layer protocol, developed by Sun Microsystems, for sharing and transferring remote files on UNIX or other types of networks. See also *Application layer*.

NIC—See *InterNIC*.

NIC—Network Interface Card. A NIC enables a PC to connect to a network. The NIC uses drivers to communicate with the host's networking software, and interacts with the physical media that connects the host to other computers. A NIC is also called a *LAN adapter, network adapter*, or *network board*.

NIS—Network Information Service. Along with the Network File System (NFS), the NIS is a method of creating a distributed database system in order to centralize common configuration files, such as the UNIX password file (`/etc/passwd`) and the `hosts` file (`/etc/hosts`). An NIS server manages copies of the database files, and NIS clients request information from them. NIS was developed by Sun Microsystems. See also *NFS*.

NIST—National Institute of Standards and Technology. NIST manages and promotes measurement standards, aiding in their development and use. See also *SDTN*.

NM—Network management. A set of NavisAccess features that enable you to administer both the switched and dedicated portions of your network. The following three options are available:

- Network Management—Voice over IP (VoIP) Enabled (NMV)
- Network Management—High Density enabled (NM+)
- Network Management—High Density/VoIP Enabled (NM+V)

The following table shows the complete set of NM features and the associated line density each supports:

NM feature	Line density supported	VoIP enabled	Comment
NM	Up to 4 DS3 lines	No	Default feature
NMV	Up to 4 DS3 lines	Yes	Same as NM, plus VoIP
NM+	Up to 12 DS3 lines	No	
NM+V	Up to 12 DS3 lines	Yes	Same as NM+ plus VoIP

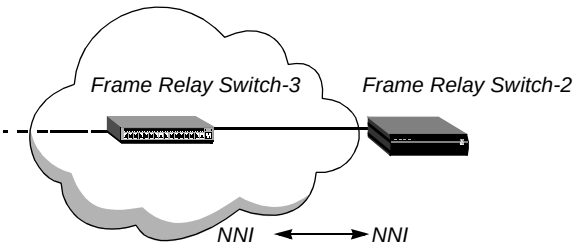
See also *NavisAccess™*.

NNI—Network-to-Network Interface. NNI is a standard that defines the interface between two Frame Relay switches located in a private or public network. NNI operation enables a TAOS unit to act as a Frame Relay switch communicating with another Frame Relay switch.

The TAOS unit uses NNI procedures to inform its peer switch about the status of Permanent Virtual Circuit (PVC) segments from its side of the Frame Relay network, and to communicate information about the integrity of the data link between them. The procedure is bidirectional. The switches act as both the user side (DTE) and network side (DCE) in that they both send status enquiries and respond to them.

Figure 63 shows an example of a TAOS unit with NNIs.

Figure 63. Frame Relay NNIs



Compare with *UNI*. See also *DCE*, *DTE*, *Frame Relay*, *Frame Relay network*, *Frame Relay switch*, *PVC*.

NNTP—Network News Transfer Protocol. NNTP is the most commonly used protocol for exchanging news on Usenet newsgroups.

node—See *host*.

node number—A value assigned to a host on a network. The node number can be hardcoded in the Network Interface Card (NIC) or assigned by means of jumper settings. It is unique among all the hosts on a local, physical network. The address for a host also contains the network address shared by all the hosts on the local network. See also *host, network address*.

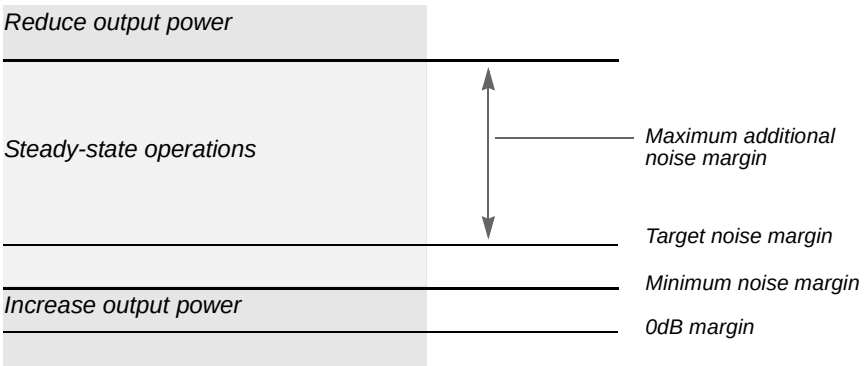
noise—On a communications channel, extraneous signals that degrade the quality or performance of the link.

noise margin—The difference, in dB, between the minimum and maximum noise levels allowed by the system. Noise margins can be controlled to ensure that the line provides a Bit Error Rate (BER) of 10^{-7}or better, as required by ANSI standards.

A BER of 10^{-7} corresponds to 0dB. The Customer Premises Equipment (CPE) tolerates a certain maximum noise level with respect to its received signal, beyond which the CPE ADSL Transceiver Unit (ATU) attempts to reduce the remote-end output power. If the noise drops below a certain minimum margin, the CPE ATU attempts to increase the remote-end power output to achieve a noise level at or above the configured minimum.

Figure 64 shows how noise-margin settings relate to power adjustments.

Figure 64. Noise margins



See also *ATU*, *BER*, *CPE*.

Non-Broadcast Multi-Access network—See *NBMA network*.

nonextended AppleTalk network—An AppleTalk network that contains a maximum of 254 nodes and is assigned a single network number. Compare with *extended AppleTalk network*. See also *AppleTalk*.

Non-Facility Associated Signaling—See *NFAS*.

nonseed router—An IPX or AppleTalk router that acquires its network configuration from another router on the network. Compare with *seed router*. See also *AppleTalk routing*, *IPX router*.

Nonvolatile Random Access Memory—See *NVRAM*.

normal area—An Open Shortest Path First (OSPF) area that allows Type-5 Link State Advertisements (LSAs) to be transmitted throughout it. Area Border Routers (ABRs) advertise external routes as Type-5 LSAs. Compare with *NSSA*, *stub area*. See also *ABR*, *area*, *ASE Type-5*, *external route*, *LSA*, *OSPF*, *router*, *routing*.

North American Digital Hierarchy—See *NADH*.

Notify Tones message—See *NTN message*.

Not So Stubby Area—See *NSSA*.

NSAP—Network Service Access Point. An Open Systems Interconnection (OSI) standard for a network address consisting of 20 bytes. Asynchronous Transfer Mode (ATM) uses E.164 addresses for public networks and NSAP addresses for private networks. See also *ATM*, *E.164 address*.

NSP—Network Service Provider. An NSP is a company that provides Internet connectivity to Internet Service Providers (ISPs) and other organization requiring high-speed access to the Internet. See also *ISP*.

NSP—Network Services Part. In Signaling System 7 (SS7), the NSP provides reliable message transfer, and corresponds to the lower three layers of the OSI Reference Model. The NSP consists of a Message Transfer Part (MTP) and a Signaling Connection Control Part (SCCP). See also *OSI Reference Model*, *SS7*.

NSSA—Not So Stubby Area. An NSSA is an Open Shortest Path First (OSPF) area that does not receive or originate Type-5 Link State Advertisements (LSAs), and that imports Autonomous System (AS) external routes in a limited fashion. OSPF version 2 defines a new Type-7 LSA for NSSAs. For NSSAs, all routes imported to OSPF have the P-bit set (P stands for *propagate*). When the P-bit is enabled, Area Border Routers (ABRs) translate Type-7 LSAs into Type-5 LSAs, which can then be transmitted to the backbone. These external routes are considered Type-7 LSAs. Compare with *normal area*, *stub area*. See also *area*, *AS*, *ASE Type-5*, *ASE Type-7*, *external route*, *LSA*, *OSPF*.

NT equipment—Network Terminating equipment. NT equipment resides on the network side of an ISDN connection. Compare with *TE*. See also *network side*, *user side*.

NT1—Network termination type 1. An NT1 device is a terminating device for an ISDN BRI line. Installed at the subscriber's location, an NT1 device provides line maintenance, timing, and echo cancellation. An NT1 device can be a standalone device, or it can be built into other types of equipment. See also *ISDN BRI line*.

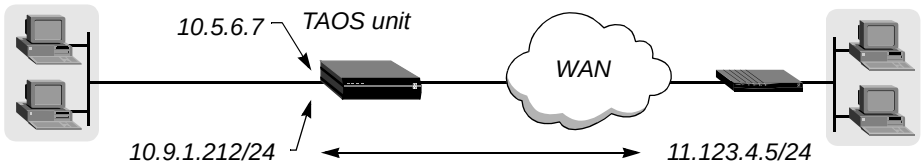
NTN message—Notify Tones message. In a MultiVoice environment, an NTN message notifies the signaling gateway when an asynchronous fax or modem tone is detected. See also *MultiVoice™*, *signaling gateway*.

NUI—Network User Identification. NUI is a name-password combination that gives you access to a commercial packet-switched network.

null modem—See *crossover cable*.

numbered interface—In interface-based IP routing, a unique address assigned to one side of a connection. Assignment of a unique address is a requirement for some applications, such as Simple Network Management Protocol (SNMP). Figure 65 shows a local interface with two addresses, one of which is used for a numbered interface connection.

Figure 65. How numbered interfaces work



Reasons for using numbered interfaces include troubleshooting dedicated point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing enables a TAOS unit to operate more as a multihomed Internet host behaves. Compare with *system-based routing*, *unnumbered interface*. See also *interface-based routing*, *IP address*, *multihomed host*, *point-to-point link*, *SNMP*.

NVP—Network Voice Protocol. NVP is a protocol developed to enable the communication of real-time interactive voice over disparate computer networks.

NVRAM—Nonvolatile Random Access Memory. NVRAM is a generic term for any type of memory that maintains its data contents across resets and power cycles. This type of memory can be ordinary Random Access Memory (RAM) with a battery backup, or a device that does not require power to preserve contents. NVRAM is useful for storing configuration information across sessions. Data is read and written, byte by byte, in any order. On a TAOS unit, NVRAM contains the current configuration stored in binary format. See also *DRAM*, *EEPROM*, *flash memory*, *RAM*.

NVT—Network Virtual Terminal. An NVT is a bidirectional character device with a printer and a keyboard. The printer responds to incoming data, and the keyboard produces outgoing data sent over a Telnet connection. The code set is seven-bit ASCII in an eight-bit field. See also *Telnet session*.

NVT ASCII—The ASCII character set used with a Network Virtual Terminal (NVT). See also *ASCII*, *NVT*.

O

OAM loopback—Operation, Administration, and Maintenance loopback. OAM loopback enables a TAOS unit to detect the failure of an Asynchronous Transfer Mode (ATM) Permanent Virtual Circuit (PVC) on a DS3-ATM interface. When it detects failure, the system clears the PVC, puts the interface in an inactive state, and attempts to reestablish the dedicated connection. See also *ATM*, *OAM protocol*, *PVC*.

OAM protocol—Operation, Administration, and Maintenance protocol. OAM offers performance monitoring, fault detection, and fault localization for an Asynchronous Transfer Mode (ATM) network. See also *ATM*, *OAM loopback*.

OC3 SONET— A SONET-based fiberoptic User-to-Network Interface (UNI), either public or private, operating at 155.52Mbps over single-mode and multimode optical fiber. See also *SONET*, *UNI*.

octet—Eight data bits, also called a *byte*.

odd parity—See *parity*.

off hook—A state that results when you lift a telephone receiver, resulting in a busy signal for an incoming call.

offset—In a generic filter, the number of bytes from the start of a frame to the data to be tested against the filter. See also *generic filter*.

Open Shortest Path First—See *OSPF*.

Open Systems Interconnection Reference Model—See *OSI Reference Model*.

Operation, Administration, and Maintenance loopback—See *OAM loopback*.

Operation, Administration, and Maintenance Protocol—See *OAM protocol*.

Operator-Controlled rate adaptation—A type of rate adaptation in which the Customer Premises Equipment (CPE) must initialize at and maintain a specific bit rate with an acceptable target noise margin. If the CPE fails to achieve the planned bit rate in either direction, it fails to initialize. The CPE does not use a higher bit rate, even if it can support one. Compare with *Automatic-at-Startup rate adaptation*. See also *CPE*.

OSI Reference Model—Open Systems Interconnection Reference Model. The OSI Reference Model describes the layers of network functionality and the way to connect communications devices on a LAN or WAN. Each layer provides services for the layer above it and uses the services of the layer below it.

The model describes the following seven layers:

Layer	Description
Application	Provides applications with access to the network. File transfer, email, and network-management software are examples of Application-layer programs. Protocols such as Simple Network Management Protocol (SNMP), Telnet, Rlogin, File Transfer Protocol (FTP), and File Transfer, Access, and Management (FTAM) provide Application-layer services.
Presentation	Presents information in a format understandable to users and their applications. Data conversion, special graphics, compression, and encryption are some of the functions implemented at the Presentation layer.
Session	Synchronizes the data in a network connection, maintains the link until the transmission is complete, handles security, and makes sure that the data arrives in the proper sequence. Gateway communications are implemented at the Session layer. Examples of Session-layer protocols are AppleTalk Data Stream Protocol (ADSP), NetBEUI (an extension of NetBIOS), NetBIOS, and Printer Access Protocol (PAP).
Transport	Provides data transfer at the proper speed, quality, and error rate, ensuring reliable delivery. Transport protocols include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Sequenced Packet Exchange (SPX).
Network	Provides address resolution and routing protocols. Address resolution enables the Network layer to determine a unique network address for a node. Routing protocols enable data to flow between networks and reach their proper destinations. Examples of Network-layer protocols are Address Resolution Protocol (ARP), Datagram Delivery Protocol (DDP), Internet Control Message Protocol (ICMP), Interior Gateway Protocol (IGP), Internetwork Packet Exchange (IPX), Internet Protocol (IP), and Packet Layer Protocol (PLP).
Data Link	Creates, sends, and receives data packets appropriate to the type of network in use. Data Link protocols include High-Level Data Link Control (HDLC), Link Access Procedure, Balanced (LAPB), Link Access Procedure, D channel (LAPD), Point-to-Point Protocol (PPP), and Serial Line Internet Protocol (SLIP).
Physical	Defines the electrical properties of the physical medium and converts the data into a series of 0s and 1s for digital transmission. Examples of Physical-layer specifications include RS-232, RS-422, RS-423, RS-449, IEEE 802.3, and IEEE 802.5.

OSPF—Open Shortest Path First. OSPF is the next generation Internet routing protocol. The *Open* in its name refers to the fact that OSPF was developed in the public domain as an open specification. The *Shortest Path First* portion refers to an algorithm developed by Dijkstra in 1978 for building a self-rooted shortest-path tree from which routing tables can be derived. As a link-state protocol, OSPF can take into account a variety of link conditions (such as the reliability or speed of the link) when determining the best path to a destination network. OSPF uses a link-state database of the network and propagates only changes to the database. See also *link-state database*, *route*, *router*, *routing*.

OSPF Trunk Administrative Cost Metric—An Open Shortest Path First (OSPF) function that enables you to control the specific path that a Virtual Circuit (VC) takes through the network. You can select a shorter hop path regardless of the available bandwidth on longer paths. See also *OSPF*, *VC*.

outgoing call—A call that the TAOS unit places to another device. Compare with *incoming call*.

outgoing continuity test—In a Signaling System 7 (SS7) network, a test in which the switch puts a DS0 circuit into a loopback and the TAOS unit generates a tone. If the TAOS unit receives the tone in return, the continuity test is successful. Note that all the setup and signaling required to coordinate a continuity test is handled by the signaling gateway by means of SS7. Compare with *incoming continuity test*. See also *2-wire continuity test*, *4-wire continuity test*, *4-wire-to-2-wire continuity test*, *continuity test*, *signaling gateway*, *SS7 network*.

out-of-band management—A management method that uses a separate channel (rather than a portion of each data channel) for diagnostic and administrative purposes.

out-of-band signaling—See *ISDN D-channel signaling*.

out-of-frame condition—A condition in which a T1 line, DS3 line, or DS2 stream cannot receive or transmit data because the TAOS unit has lost the frame alignment on the received signal. See also *DS3 line*, *T1 line*.

output filter—A filter applied to an outgoing packet. See also *filter*, *packet filter*, *route filter*.

overflow—The process of adding bandwidth to handle peak traffic conditions. See also *FT1-B&O*.

overlap receiving—A feature that affects the procedure of establishing an incoming call received on a T1 PRI or E1 PRI line. When a TAOS unit uses overlap receiving, the unit can gather the complete called number from the network switch by means of a series of Information messages, enabling the use of features such as called-number authentication. The Q.931 specification states that a system can use either en-bloc receiving or overlap receiving to handle an incoming call. Compare with *en-bloc receiving*, *Q.931*.

P

PAC—PPTP Access Concentrator. A PAC receives incoming Point-to-Point Protocol (PPP) calls and initiates a connection to the PPTP Network Server (PNS). See also *PNS*, *PPP*.

packet—A block of information containing a header, data, and trailer. Packets created at each level of the OSI Reference Model are inserted into lower-level packets. The format of a packet depends upon the protocol that creates it. A packet can be transmitted over a network or telephone line. On an X.25 network, a packet is a fixed-length unit that includes data and call-control signals. Compare with *frame*. See also *OSI Reference Model*, *packet field*.

Packet Assembler/Disassembler—See *PAD*.

packet buffering—In a TCP dial-in session that does not require V.120 processing, a method of buffering and transmitting raw TCP data as TCP packets rather than as a continuous data stream. Unless V.120 processing is required, raw TCP WAN data goes directly to the HDLC interface rather than to the terminal-server subsystem. If V.120 processing is required, the terminal server processes the call. See also *Raw TCP*.

packet field—A portion of a packet that contains a specific kind of information. For example, the data field in a packet contains the data being transmitted between applications. The header field can contain information identifying the packet type and any error-checking mechanisms. See also *packet*.

packet filter—A series of rules stating how a TAOS unit is to handle certain types of packets. Each rule specifies a condition and an action that the unit takes if the condition is met. The TAOS unit compares data in the packet to each condition, one condition at a time, until it finds a match between the data and one of the conditions. It then forwards or drops the packet, depending on the action specified for the condition.

When no filter is in use, a TAOS unit forwards all packets. But when you apply a filter to an interface, you reverse that default. The unit no longer forwards nonmatching packets automatically. It requires a rule that explicitly allows those packets to pass. You can apply a packet filter to incoming packets, outgoing packets, or both. In addition, you can specify that the TAOS unit forward or drop those packets that match the rules, or all packets *except* those that match the rules.

A TAOS unit supports four types of packet filters: generic, IP, IPX, and TOS. You can apply a packet filter as either a data filter or a call filter. The unit applies a data filter before a call filter.

Compare with *route filter*. See also *call filter*, *data filter*, *generic filter*, *IP filter*, *IPX filter*, *TOS filter*.

Packet Layer Protocol—See *PLP*.

packet-level inverse multiplexing—A method of inverse multiplexing in which the inverse multiplexer performs its function at the packet level by means of the Multilink PPP (MP) or Multilink Protocol Plus (MP+). One data packet goes over the first circuit, the next goes over the second circuit, and so on, until all the data packets are distributed over all the available circuits. The receiving end adjusts for network-induced delay and reassembles the data packets into their proper order. This inverse multiplexing technique is also referred to as *load balancing*. Telecommuting applications use packet-level inverse multiplexing. Compare with *circuit-level inverse multiplexing*. See also *inverse multiplexer*, *inverse multiplexing*.

packet processor—A switch module that performs frame-format validation, routing, queueing, and protocol conversion.

packet-radio communication—A technology for wireless modem access in which a system breaks a transmission into small packets that include a source address, destination address, and error-correction information. The packets are uplinked to a satellite, and then broadcast. The destination device receives only packets addressed to it. See also *error correction*, *wireless technology*.

Packetstar™ Connection Gateway—See *PCG*.

Packet-Switched Data Network—See *PSDN*.

packet-switched network—A network that consists of a series of interconnected circuits on which data packets can travel by one of several routes. Compare with *circuit-switched network*. See also *PSDN*, *PSPDN*.

packet-switched node—A packet switch on the ARPANet.

Packet-Switched Public Data Network—See *PSPDN*.

packet switching—A mode of data transfer that uses any available circuit to transmit packets from a specific source to a specific destination. Packets can take different paths at the same time, and they might not arrive in the order in which they were sent. Compare with *circuit switching*.

PAD—Packet Assembler/Disassembler. A PAD is an asynchronous terminal concentrator that enables several terminals (or other asynchronous devices) to share a single network line. A PAD assembles packets of asynchronous data and transmits them to a packet-switched network. It also disassembles packets from the network and transmits the data back to the asynchronous devices. See also *X.25/PAD*.

PAP—Password Authentication Protocol. PAP uses a two-way handshake method of establishing a caller's identity. Used only during the initial establishment of the data link, PAP is not a strong authentication method. Passwords travel across the line as plain text, so they are subject to eavesdroppers using software that monitors network information. Use PAP authentication only when the dial-in device does not support a stronger authentication method or when the remote device requires a plain-text password.

An extension of PAP adds the U.S. Data Encryption Standard (DES) cipher to data transmissions. The caller applies the encryption algorithm to a Point-to-Point Protocol (PPP) packet and places the resulting cipher text in the information field of another PPP packet. The receiving end applies the inverse algorithm and interprets the resulting plain text as if it were a PPP packet that had arrived directly on the interface.

Compare with *CHAP*. See also *authentication*, *DES*, *password*, *PPP*.

PAP-Token authentication—An extension of Password Authentication Protocol (PAP) authentication. In PAP-Token authentication, the user authenticates his or her identity by entering a password, called a *token*. The token is obtained from a hardware device, such as a hand-held token card. The TAOS unit prompts the user for the token, possibly along with a challenge key. The unit obtains the challenge key from a token-card server with which it communicates by means of RADIUS. The token travels in the clear, but because it is a one-time-only password, the security risk is usually not serious. To authenticate the base channel of the connection, the token-card server uses the token that the user sends in response to the challenge.

PAP-Token is appropriate for single-channel, dial-out calls. It is not practical for multichannel calls, because any time that bandwidth requirements result in adding another channel, the TAOS unit challenges the user for another token. Compare with *PAP, PAP-Token-CHAP authentication*. See also *RADIUS, token, token card, token-card authentication, token-card server*.

PAP-Token-CHAP authentication—An authentication method that uses PAP-Token to authenticate the base channel of a Multilink Protocol Plus (MP+) call, and then uses a Challenge Handshake Authentication Protocol (CHAP) password to authenticate additional channels. The advantage of a PAP-Token-CHAP call over a PAP-Token call is that you need to verify only the initial connection by means of a hand-held token card. In a PAP-Token-CHAP call, the TAOS unit uses CHAP to verify any additional channels. Compare with *CHAP, PAP, PAP-Token authentication*. See also *MP+, token, token card, token-card authentication, token-card server*.

parallel dialing—A way for a TAOS unit to add channels to an outgoing call in multiples, rather than one at a time.

parity—In 7-bit communication, a way for a device to determine whether it has received data exactly as the sending device transmitted it. The two communicating devices must agree upon whether they will use even parity, odd parity, or no parity.

The sending device counts the 1s in each string it sends and determines whether the sum is even or odd. Then, it adds an extra bit, called a *parity bit*, to the string. If even parity is in use, the parity bit makes the sum of the bits even. If odd parity is in use, the parity bit makes the sum of the bits odd. For example, if a device sends the binary number 1010101 under even parity, it adds a 0 (zero) to the end of the byte, because the sum of the 1s is already even. However, if it sends the same number under odd parity, it adds a 1 to the end of the byte in order to make the sum of the 1s an odd number.

The receiving device checks whether the sum of 1s in a character is even or odd. If the transmission is using even parity, the sum of 1s in a character should be even. With odd parity, the sums of bits in a character should be odd. If the sum of the bits does not equal the parity setting, an error has occurred during transmission of the data.

Special ASCII characters (128 through 256) require eight bits to represent the data. In eight-bit communication, no parity bit is used. See also *ASCII*.

pass count—A statistic that displays the number of background diagnostic tests that have passed without errors.

passive hub—A device that splits a transmission signal, enabling you to add more hubs to the network. Compare with *active hub*, *smart hub*. See also *hub*.

password—A text string that a user must enter during the login process. Entering the proper password identifies the user as a person authorized to access network resources. Compare with *token*.

password prompt—The prompt that the terminal server displays when asking the user for his or her password. See also *password*, *terminal server*.

path—On a SONET network, an end-to-end circuit. Path-terminating equipment multiplexes and demultiplexes the SONET payload, and can originate, modify, and terminate path overhead. Compare with *line*, *section.* See also *SONET*.

Path Selector Module—See *PSM*.

Payload—In an Asynchronous Transfer Mode (ATM) cell, a field that follows the Header Error Control (HEC) portion and contains 48 bytes of user data. See also *ATM, CLP, GFC, HEC, PT, VCI, See also ATM, VPI, VPL*..

payload—See *data bits*.

Payload Type—See *PT*.

P-bit Parity Errors—See *PERR*.

PBX—Private Branch Exchange. A PBX is an internal telephone network, such as one used in a large office, in which one incoming number directs calls to various extensions and from one office to another. The PBX routes calls both within an organization and to and from the outside telephone network. A PBX can be either analog or digital. Some digital PBX units can terminate analog as well as digital connections. PBX units work in conjunction with channel banks to distribute channels from the T1/E1 circuit for voice, video, fax, and data. In some cases, digital PBX units contain multiplexing components that distribute channels without a channel bank. See also *PRI-to-T1 conversion*.

PCG—Packetstar™ Connection Gateway. A Signaling System 7 (SS7) gateway that provides interface and connection management for toll and tandem data and voice links. See also *SS7*.

PCM—Pulse Coded Modulation. PCM is a sampling technique for encoding a digital stream so that it contains a digitized version of the analog waveform sent by a device attached to a modem. A TAOS unit can also convert outgoing data into analog waveforms, change these waveforms into a PCM-encoded digital stream, and send them to the network over a digital line. The network presents the data to the receiving modem in analog form over an analog line. The data looks exactly as it would appear if it had been sent by an analog-based modem.

There are two standards for coding the sample level. The U-Law standard is common in North America and Japan. Elsewhere, the A-Law standard is typically in use.

See also *A-Law*, *analog line*, *digital line*, *modem*, *U-Law*.

PCMCIA—Personal Computer Memory Card International Association. PCMCIA is a standard that supports devices on a credit-card-sized board. The 1990 PCMCIA version 1.0 specification supports Type I cards for RAM, ROM, or NVRAM. The 1991 PCMCIA version 2.01 specification supports Type II cards for network and fax/modem functionality, and Type III cards, which provide a miniature hard drive for wireless networks. See also *NVRAM*, *RAM*, *ROM*, *wireless technology*.

PCMCIA card code—Code written to make use of PCMCIA-card functionality. See also *PCMCIA*.

PCR—Peak Cell Rate. In an Asynchronous Transfer Mode (ATM) transmission, the PCR is the maximum rate at which cells can be transmitted. It represents the shortest time interval between two cells. Equivalent to Be for Frame Relay, PCR is measured in cells per second, and converted internally to bits per second. See also *ATM*, *Be*, *Frame Relay*.

PCS—Personal Communications Services. PCS is a wireless telephone service for mobile users, similar to cellular communication. It is also referred to as *digital cellular.* See also *cellular communication*, *wireless technology*.

PCS 1900—See *GSM 1900*.

PCT—Peripheral Control and Timing. A proprietary 5ESS interface used internally between a 5ESS time slot interchange unit and peripheral line and trunk units. A PCT link is an optical interface with two separate paths for the transmission and receipt of data. It operates at 65.536Mbps. Data is formatted into 32 blocks, each containing 32 bytes. The frame structure is repeated at a rate of 8kHz. Each block contains 2 overhead bytes, 24 DS0 bytes, and 6 signaling bytes. See also *PCTFI*.

PCTFI—Peripheral Control Timing Facility Interface. An interface that enables a Peripheral Control and Timing (PCT) link to be treated as an external trunk. Generally, the 5ESS device exercises extensive control and maintenance of devices attached to the PCT link. However, PCTFI peripherals do not receive a great deal of control and maintenance service from the 5ESS device. Instead, a minimal set of trunk maintenance operations are administered through the F signaling bits associated with each virtual channel. In addition the 5ESS device administers a minimal set of PCT link diagnostics and link maintenance for PCTFI peripherals. See also *PCT*.

PDC—Personal Digital Cellular. A Japanese standard operating in the 800MHz and 1500MHz bands. See also *WORM-ARQ*.

PDN—Public Data Network. A PDN is any government-owned or government-controlled commercial packet-switched network that offers WAN services for data transmission. See also *packet-switched network.*

PDU—Protocol Data Unit. A PDU is a packet created at any one of the OSI layers. It contains control information and a payload, and passes through the interfaces between one protocol layer and another. See also *OSI Reference Model*.

Peak Cell Rate—See *PCR*.

Peer Group Leader—See *PGL*.

peripheral—A device attached to a network, server, or workstation. Peripherals include CD-ROM drives, fax machines, hard drives, modems, optical drives, printers, and tape drives.

Peripheral Control and Timing—See *PCT*.

Peripheral Control Timing Facility Interface—See *PCTFI*.

Permanent Virtual Circuit—See *PVC*.

PERR—P-bit Parity Errors. PERR indicates the number of times that the P-bit parity check failed on the DS3 line. Compare with *CPERR*. See also *DS3 line*.

Personal Computer Memory Card International Association—See *PCMCIA*.

Personal Digital Cellular—See *PDC*.

Personal Handyphone System—See *PHS*.

Personal Internet Access Forum Standard—See *PIAFS*.

per-user accounting—A way for a network reseller to direct accounting information about specific users to a RADIUS server belonging to a particular ISP. A network reseller can serve many different ISPs, each with a different access policy. The reseller carries traffic for individual users, and must bill for usage according to the policies of the appropriate ISP. Per-user accounting facilitates this process. See also *accounting*, *ISP*, *RADIUS*.

per-user default route—The default route for IP packets coming from a particular user. A TAOS unit uses the per-user default under either of the following circumstances:

- The next-hop address in the TAOS unit's routing table is the default route for the system (destination 0.0.0.0).
- The normal routing logic fails to find a route and there is no systemwide default route.

The per-user default (or *direct*) route can be implemented on a WAN connection or an Ethernet connection. If the TAOS unit does not have a direct route, it drops the packets on the connection. The default value is 0.0.0.0. If you accept this value, the TAOS unit routes packets as the routing table specifies, using the systemwide default route if it cannot find a more specific route.

The per-user default route applies to all packets the TAOS unit receives for a given profile, regardless of the specific IP source address. Therefore, you can use this feature when the profile belongs to another router and all hosts behind that router use the default gateway. The TAOS unit handles packets from other users or from the Ethernet network in the usual fashion. The global routing table is not altered. Therefore, when you diagnose routing problems with a profile that implements a per-user default route, an error in a per-user gateway address is not apparent from inspection of the global routing table.

See also *default route*, *hop*, *IP address*, *IP route*, *IP routing table*.

PGL—Peer Group Leader. In a Private Network-to-Network Interface (PNNI) configuration, a system elected to perform a subset of the functions associated with a logical group node. See also *PNNI*, *PNNI peer group*.

PHS—Personal Handyphone System. PHS is a mobile telephone system available for users of Japanese Primary Rate Interface (PRI). In addition to providing voice service, PHS allows data communication at rates of up to 64Kbps, and can be used for Internet access. See also *PIAFS*.

Physical layer—The lowest layer in the OSI Reference Model. The Physical layer defines the electrical properties of the physical medium and converts the data into a series of 0s and 1s for digital transmission. See also *OSI Reference Model*.

Physical Layer Convergence Protocol—See *PLCP*.

PIAFS—Personal Internet Access Forum Standard. PIAFS is a protocol that handles connection negotiation, data transfer, and error correction for the Personal Handyphone System (PHS). See also *PHS*.

PID—Protocol Identifier. The PID is a group of bytes in the SNAP header of an IPX frame. The PID identifies the protocol in use for the transmission. See also *IPX frame*, *SNAP*.

Ping—A command that sends an Echo request to test whether a remote network device is accessible. If the remote device is properly connected, it receives the request and sends back an Echo reply. Certain versions of the Ping command can also determine the amount of time necessary to receive the Echo reply, and the number of replies lost in transmission. See also *Echo*.

Pipeline™—A family of remote-access products consisting of routers, bridges, and Terminal Adapters (TAs) that have the bandwidth, speed, protocol support, and security required for fast, reliable connections and safeguarded communications. See also *bridge*, *router*, *TA*.

Plain Old Telephone Service—See *POTS*.

PLCP—Physical Layer Convergence Protocol. A protocol that specifies how cells are formatted within a data stream over such transmission media as T1 or T3. PLCP is often used for data transmission over Asynchronous Transfer Mode (ATM) trunks. See also *ATM*.

PLP—Packet Layer Protocol. A protocol that specifies the rules for full-duplex data transmission between a sending device and a receiving device on an X.25 network. See also *full duplex*, *X.25*.

plug-and-play—See *PNP*.

PNNI—Private Network-to-Network Interface. A protocol that provides hierarchical routing and signaling between Asynchronous Transfer Mode (ATM) switches.

PNNI routing uses a standards-based dynamic hierarchical routing protocol for distributing link-state topology and ATM addressing information between ATM switches. Each switch can use the topology database to compute the best path to a given end system, taking into consideration bandwidth and Quality of Service (QoS) contracts. PNNI routing is largely self-configuring in networks in which the address structure reflects the topology. (For example, the members of a peer group use the same address prefix). In addition to supporting Permanent Virtual Circuits (PVCs), which require manual configuration in each switch along the path between two end systems, PNNI allows the switches to support Soft Permanent Virtual Circuits (SPVCs).

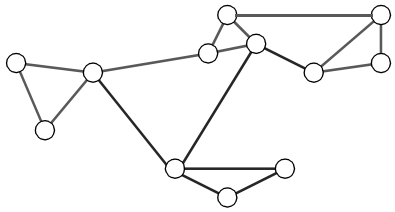
PNNI signaling uses a protocol that is based on ATM Forum UNI 4.0 signaling, with support for source routing and the ability to reroute a call on an alternative path in case of failure (*crankback*). This protocol is used to establish connections dynamically across the ATM network.

See also *ATM*, *PVC*, *QoS contract*, *SPVC*.

PNNI node ID—Private Network-to-Network Interface node ID. A 22-byte, 44-digit hexadecimal number used to identify the system as a logical node within a PNNI peer group. The first byte of the node ID is the node level—for example, 96 (0x60). The second byte is set to 160 (0xA0) by convention, and the remaining 20 bytes are set to the PNNI node ATM End System Address (AESA). See also *AESA format*, *PNNI*.

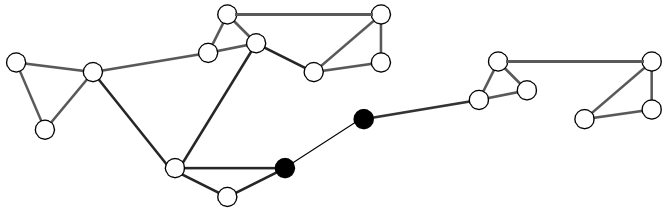
PNNI peer group—A set of logical nodes grouped together to create a routing hierarchy. At the lowest level of the hierarchy (a flat topology), nodes share topology and link-state information and maintain a synchronized topology database within a peer group. The database provides a continually updated view of available links, which enables the nodes to compute paths that fulfill Quality of Service (QoS) contracts. Figure 66 shows a peer group of lowest-level nodes.

Figure 66. Peer group of lowest-level nodes



At the next level of the hierarchy, a single node is elected to be the Peer Group Leader (PGL) and is responsible for communicating a summary of the database to other PGLs. In Figure 67, the PGL systems are shown in black. Each of the two peer groups has elected one node to be the PGL.

Figure 67. Two PGLs exchanging topology information



See also *PGL*, *PNNI*, *PNNI peer group ID*.

PNNI peer group ID—Private Network-to-Network Interface peer group ID. A 14-byte, 28-digit hexadecimal number used to group nodes into a PNNI peer group. (All members of the same PNNI peer group have the same peer group ID.) The first byte of the peer group ID is the node level—for example, 96 (0x60). The remaining 13 bytes are set to the PNNI node ATM End System Address (AESA) prefix. See also *AESA format*, *PNNI*, *PNNI peer group.*

PNNI Topology State Element—See *PTSE*.

PNNI Topology State Packet—See *PTSP*.

PNP—Plug-and-play. PNP describes the process of plugging a device into a computer and having the computer recognize it without user configuration.

PNS—PPTP Network Server. The device acting as the end point of a Point-to-Point Tunneling Protocol (PPTP) tunnel. See also *PPTP*.

Point of Presence—See *POP*.

point-to-point link—A connection that does not make any use of intervening devices. A point-to-point link can connect two hosts on the same network, or two networks across the WAN.

Point-to-Point Protocol—See *PPP*.

Point-to-Point Tunneling Protocol—See *PPTP*.

poison—Denotes a TAOS unit's ability to stop advertising (poison) IP dial-out routes if it temporarily loses the ability to dial out. See also *IP route*.

poison reverse—A policy for handling Routing Information Protocol (RIP) update packets that include routes received on the same interface on which the update was sent. Using a poison-reverse policy, a TAOS unit propagates routes back to the subnet from which they were received and assigns them a metric of 16. See also *metric*, *RIP*, *subnet*.

polling—An access-control method in which one master device queries other network devices, requesting them to transmit one at a time.

pool chaining—A configuration in which contiguous IP address pools are treated as one pool space with shared addresses. Pool chaining enables a caller to acquire an address from any pool within a chain. The pools within a chain must be defined in a contiguous sequence. When the system assigns an address to an end user, it begins searching for an available address in the first pool of the chain and stops when it either finds an available address or encounters a null pool definition. See also *IP address*, *IP address pool*.

pool summary—A configuration in which the router advertises a single route for the network you define in an address pool, rather than an individual host route for each address. By default, a TAOS unit adds dynamically assigned IP addresses to the routing table as individual host routes. To reduce the size of routing table advertisements, you can summarize the entire pool. The TAOS unit routes packets to a valid host address, and rejects packets with an invalid host address.

Because a TAOS unit creates a host route for every address assigned from the pools, and because host routes override subnet routes, the unit correctly routes packets whose destination matches an assigned IP address from the pool. However, because the unit advertises the entire pool as a route, and only knows privately which IP addresses in the pool are active, a remote network might improperly send the unit a packet with an inactive IP address.

When the TAOS unit receives a packet whose IP address matches an unused IP address in a pool, it either returns the packet to the sender, with an ICMP reject message, or simply discards the packet. To enable the router to handle packets with destinations to invalid hosts on the summarized network, you must specify one of the following internal interfaces as the router:

Interface	Description
Reject (rj0)	Has an IP address of 127.0.0.2. When you specify this address as the router to the destination pool network, the TAOS unit rejects packets to an invalid host on that network, appending an ICMP Host Unreachable message.
Blackhole (bh0)	Has an IP address of 127.0.0.3. When you specify this address as the router to the destination pool network, the TAOS unit silently discards packets to an invalid host on that network.

See also *network alignment*, *route*, *router*.

POP—Point of Presence. A POP is the location of an Internet Service Provider's (ISP's) equipment. See also *ISP*.

port—A TCP/IP interface that defines the logical location in which an application or process is running in a computer. When you define such a location, packets can reach an application from a remote system. There are certain well-known ports, such as port 21 used by FTP. Packet filters and firewalls make use of port addresses to restrict incoming and outgoing data and in order to secure an environment. The User Datagram Protocol (UDP) was developed to add the port address of an application or process to an IP packet, facilitating communication between applications over a network. See also *firewall*, *IP*, *packet filter*, *TCP/IP*, *UDP*.

port redirection—A configuration that enables a TAOS unit to redirect certain packet types to a specified server. For example, you can configure a Connection profile or RADIUS profile to redirect Hypertext Transfer Protocol (HTTP) traffic to a Web cache server on a local network. However, port redirection is not limited to HTTP traffic. You can use the feature to redirect any TCP or UDP packet on the basis of its protocol and port information. See also *HTTP*.

POST—Power-On Self Test. A POST is a diagnostic test a TAOS unit performs when it first starts or after it completes a system reset. During a POST, the unit checks system memory, configuration, installed cards, compression hardware, and T1 connections.

POTS—Plain Old Telephone Service. POTS denotes conventional analog voice transmission over telephone lines.

POTS splitter—A type of device that separates data from voice signals on the same telephone line. A POTS splitter resides at both the Central Office (CO) and the customer premises, enabling high-speed Digital Subscriber Line (DSL) data and ordinary telephone service to use the local loop simultaneously. At the end-user location, the POTS splitter supports one or more lines with one or more analog connectors for voice equipment. Typically, at the CO, multiline POTS splitters handle voice and data for multiple loops. A POTS splitter is also known as a *voice splitter*. See also *CO*, *DSL*.

Power-On Self Test—See *POST*.

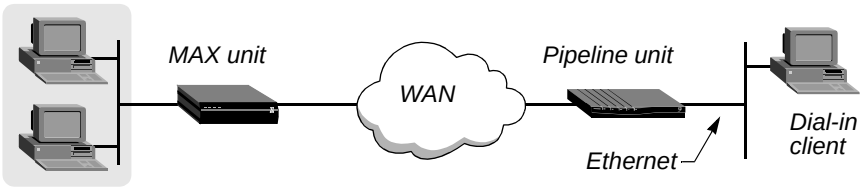
Power Spectral Density—See *PSD*.

PPD—Partial Packet Discard. PPD is an Asynchronous Transfer Mode (ATM) flow-control mechanism. If the global Cell Loss Priority (CLP) threshold for a port is reached, PPD is performed for circuits that are configured for Early Packet Discard (EPD). Unlike EPD, however, all of the remaining cells in the current packet are discarded. Note that the End of File (EOF) cell is discarded as well, resulting in the loss of the next packet, even if the packet is transmitted. See also *ATM*, *CLP*, *EPD*.

PPP—Point-to-Point Protocol. PPP provides a standard means of encapsulating data packets sent over a single-channel WAN link. It is the standard WAN encapsulation protocol for the interoperability of routers. PPP also allows direct dial-up access from a personal computer to a corporate LAN or Internet Service Provider (ISP). Using PPP ensures basic compatibility with non-TAOS devices. Both the dialing side and the answering side of the link must support PPP.

Figure 68 illustrates a single-channel PPP call.

Figure 68. PPP connection



Typically, a dial-in device (such as a modem) initiates a PPP session. The TAOS unit's terminal-server software handles the call. If the terminal server detects a PPP packet from the caller, it passes the call on to the router, which handles it as a regular PPP connection. The caller never sees the terminal-server interface.

However, a user whose dial-in software does not support PPP can still initiate a PPP session from within the terminal-server interface. To do so, the user can log in to the terminal server in terminal mode and use the PPP command. Or, the PPP command can be included in an expect-send script.

During establishment of a PPP data link, the dialing and answering units exchange Link Control Protocol (LCP) packets to establish communication and configure the link. When the link is established, PPP provides for an optional authentication step before exchanging Network Control Protocols (NCPs).

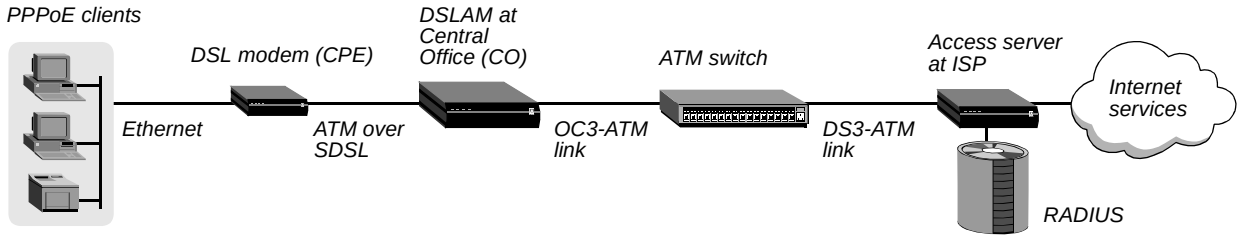
See also *expect-send script*, *ISP*, *LCP*, *NCP*, *router*, *terminal mode*, *terminal server*, *V.120 TA*.

PPPoE—PPP over Ethernet. PPPoE enables a PC to communicate with a broadband access server in order to gain access to a remote network. In general, PPPoE is appropriate for residential, telecommuter, and other small to middle-range customers who want to connect one or more PCs to multiple services at an ISP. To enable users to take advantage of Ethernet's multipoint support, PPPoE technology allows multiple devices on an Ethernet network to initiate PPP sessions with multiple destinations.

The links for the PPP connections are created by means of bridging modems. You can connect multiple PCs at a remote site to Customer Premises Equipment (CPE). The CPE can be an Asynchronous Transfer Mode (ATM) bridge that uses RFC-1483 encapsulation, or a Frame Relay bridge that uses RFC-1490 encapsulation. The CPE connects to the DSL Access Multiplexer (DSLAM) at the telephone company's Central Office (CO). The DSLAM then switches the cells or frames across the data network to the broadband access server, which terminates the bridged connection. Over this bridged connection, the PC and the server establish a PPP session, which looks like an ordinary dial-up connection to the user. The PC and the server can then exchange authentication, accounting, IP address, and other information.

In Figure 69, the PPPoE configuration uses an ATM link.

Figure 69. PPPoE configuration



The PPPoE client sends a packet through the DSL modem to the DSLAM. The CO sends the packet through an ATM switch to the server at the ISP. The ISP can then provide the services chosen by the end user.

PPPoE works in two basic phases: a Discovery phase and a PPP Session phase. During the Discovery phase, the following events take place:

1 A client that wants to establish a PPPoE session sends a broadcast, asking whether any PPPoE services are available.

2 The broadband access server responds with a packet containing the server's Ethernet MAC address, and verification that it supports PPPoE.

3 The client sends a session-request packet.

4 The server responds with a unique session ID. Together, the MAC address and session ID uniquely identify the PPPoE session.

During the PPP Session phase, the client and the server have sufficient information to create a connection over the Ethernet network. The client and the server allocate the resources for the connection, and the client sends PPP packets to the server, just as for an ordinary dial-in session.

See also *ATM*, *bridge*, *bridging*, *CO*, *CPE*, *DSLAM*, *Frame Relay*, *PPP*.

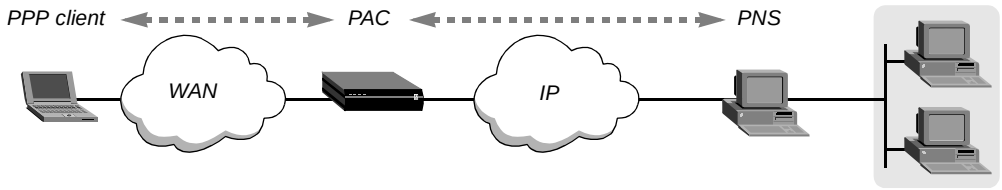
PPP over Ethernet—See *PPPoE*.

PPP Translation FRAD—Point-to-Point Protocol Translation Frame Relay Access Device. A PPP Translation FRAD configuration enables Data Terminal Equipment (DTE) configured for PPP to communicate with a DTE device configured for Frame Relay. The link uses RFC 1490 multiprotocol encapsulation. The network establishes a single circuit between the two devices. Lucent Technologies implements this feature by stripping the PPP header, translating the frame payload from PPP encapsulation to RFC 1490 encapsulation, and then applying an appropriate Frame Relay header. The Frame Relay Permanent Virtual Circuit (PVC) is completely transparent to the PPP devices. See also *Frame Relay*, *PPP*, *PVC*.

PPTP—Point-to-Point Tunneling Protocol. PPTP is a protocol that enables a PPP client to connect to a remote Windows NT server through a TAOS unit as if the connection were directly terminated at the server. PPTP tunneling occurs at OSI Layer 2, such as at the HDLC layer of a PPP connection. PPTP is a standard sponsored by Microsoft.

Figure 70 shows the basic elements of a PPTP tunnel. A PPP client dials in across an asynchronous or synchronous link, using any protocol that can be carried within a PPP connection. The TAOS unit answers the call and passes it to the PPTP Network Server (PNS) specified in the Point-to-Point Protocol (PPP) client's profile. If a PPTP Access Concentrator (PAC) has also been configured, PAC-to-PNS communication requires an IP connection.

Figure 70. PPTP tunnel



The connection from the PAC to the PNS is an IP link, which consists of a control link and zero or more data links. The control link runs over TCP, and the data links run over GRE-v2. The control link carries information used to query whether the PNS will accept the current call, and information used to establish a tunnel. PPTP implements a Hello mechanism by which the PAC and PNS verify that the other is still operational. If the Hello message does not arrive for several minutes, the tunnel and all the tunneled connections are dismantled.

Data links carry the client data, which consists of PPP frames. There is one data link per tunneled client connection. See also *PAC*, *PNS*, *PPP*.

PPTP Access Concentrator—See *PAC*.

PPTP client—Point-to-Point Tunneling Protocol client. A PPTP client is a Point-to-Point Protocol (PPP) connection that brings up a PPTP tunnel to a specified PPTP Network Server (PNS). A PPP profile can initiate a PPTP tunnel on the basis of Dialed Number Information Service (DNIS) or Calling-Line ID (CLID) information, or after PPP authentication. See also *CLID*, *DNIS*, *PNS*.

PPTP Network Server—See *PNS*.

PPP Translation Frame Relay Access Device—See *PPP Translation FRAD*.

precedence—In a Type of Service (TOS) policy or filter specification, the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set the precedence for priority queuing. See also *TOS*, *TOS filter*.

preference—A way for a TAOS unit to decide which route has highest priority. As a distance-vector protocol, Routing Information Protocol (RIP) uses a hop count to select the shortest route to a destination network. Open Shortest Path First (OSPF) is a link-state protocol, which can take into account a variety of link conditions (such as the reliability or speed of the link) when determining the best path to a destination network. Because the metrics used by the two protocols are incompatible, TAOS units support route preferences.

By default, static routes and RIP routes have the same preference, so they compete equally. Internet Control Message Protocol (ICMP) Redirect packets take precedence over both, and OSPF takes precedence over everything. If a dynamic route's preference is lower than that of the static route, the dynamic route can temporarily hide a static route to the same network. However, dynamic routes age, and if no updates are received, they eventually expire. In that case, the hidden static route reappears in the routing table.

See also *dynamic route*, *hop count*, *ICMP*, *metric*, *OSPF*, *RIP*, *route*, *static IP route*.

Presentation layer—The second highest layer in the OSI Reference Model. The Presentation layer is used for presenting information in a format understandable to users and their applications. Data conversion, special graphics, compression, and encryption are some of the functions implemented at the Presentation layer. See also *OSI Reference Model*.

primary add-on number—A number that enables a calling TAOS unit to build multichannel calls. A multichannel call begins as a single-channel connection to one telephone number. The calling unit then requests additional numbers it can dial to connect additional channels. When it receives the additional (add-on) numbers from the answering unit, the calling unit stores them, making them available to provide additional bandwidth.

When a TAOS unit receives a multichannel AIM, BONDING, MP, or MP+ call, it reports its primary add-on number and the secondary add-on number to the calling party. To add channels to the call, the calling unit must integrate the add-on numbers with the telephone number it dialed initially. If you do not specify an add-on number, and the calling TAOS unit needs to add more channels, it redials the telephone number it used to make the first connection. See also *AIM*, *BONDING*, *MP*, *MP+*, *secondary add-on number*.

primary CM—Primary Control Module. On a Stinger unit, the primary CM manages the Line Interface Modules (LIMs) and assumes all the normal controller responsibilities of managing the unit, including the call-control and circuit-management functions. The status lights (LEDs) on the CM front panel indicate which of the modules is the primary CM. All configuration takes place on the primary CM. Compare with *secondary CM*. See also *CM*.

primary Control Module—See *primary CM*.

primary DNS server—The first server that a TAOS unit attempts to access in order to perform name-address resolution on an IP network. If the primary DNS server is unavailable, the TAOS unit attempts to use the secondary DNS server. See also *DNS*, *IP network*, *secondary DNS server*.

primary group—The main group to which associated users belong. The system identifies the primary group by the `group` field in the user account (stored in the `/etc/password` file) and by the group ID associated with a new file.

Primary Rate Interface line—See *E1 PRI line*, *T1 PRI line*.

primary WINS server—The first server that a TAOS unit attempts to access for Windows Internet Name Service (WINS) name-address resolution. The link must be a Telnet or raw TCP connection running under the TAOS unit's terminal-server interface. See also *secondary WINS server*, *WINS*.

PRI-to-T1 conversion—A feature that enables a single T1 PRI line to carry both data and voice traffic. A T1 PRI line offers reduced call-setup times, unrestricted 64Kbps channels, call-by-call service selection, and enhanced data services such as Switched-384, Switched-1536, and MultiRate. With PRI-to-T1 conversion, any standard T1-based PBX can access voice circuits on the T1 PRI line, and LAN traffic can access both dedicated and switched data circuits on the T1 PRI line. See also *D channel*, *dedicated circuit*, *MultiRate*, *PBX*, *PCM*, *Switched-384*, *Switched-1536*, *switched circuit*, *T1 line*, *T1 PRI line*.

privacy—A Simple Network Management Protocol Version 3 (SNMPv3) User-Based Security Model (USM) feature that enables you to prevent data present in a Protocol Data Unit (PDU) from being copied or interpreted by unauthorized listeners on the wire. See also *PDU*, *SNMP*, *SNMPv3 USM*.

privacy key—A value that an Simple Network Management Protocol Version 3 (SNMPv3) User-Based Security Model (USM) device uses to communicate with an SNMP manager. See also *SNMP*, *SNMPv3 USM*.

private circuit—See *dedicated circuit*.

private-key encryption—An encryption method that uses a single key, which only the sender and receiver know, and a public encryption algorithm. Compare with *public-key encryption*. See also *encryption*.

private network—A network particular to an organization, and not connected to a Public Data Network (PDN). See also *PDN*.

Private Network-to-Network Interface—See *PNNI*.

Private Network-to-Network Interface node ID—See *PNNI node ID*.

Private Network-to-Network Interface peer group—See *PNNI peer group*.

Private Network-to-Network Interface peer group ID—See *PNNI peer group ID*.

private routing table—An IP routing table used only by Connection or RADIUS profiles that refer to it. A private routing table can be configured locally or in RADIUS. Externally defined private routing tables are cached locally for a configurable interval. See also *IP routing table*.

private static route—In a RADIUS user profile, an IP route that affects only packets received from the connection. The route is not added to the global routing table. If a destination is not found in the list of private routes and there is no default private route, the global routing table is consulted for a decision on routing the packets. Otherwise, only the private routing table is consulted. See also *static IP route*.

profile—A collection of settings that enable you to configure various aspects of a TAOS unit. See also *pseudo-user profile*, *user profile*.

Programmable Read-Only Memory—See *PROM*.

PROM—Programmable Read-Only Memory. PROM is a memory chip on which a device can write data only once. A PROM chip retains its contents across power cycles and system resets. See also *EEPROM*.

promiscuous mode—A bridging mode in which the TAOS unit's Ethernet controller accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. Promiscuous mode is appropriate if you are using the TAOS unit as a bridge. See also *bridge*.

protective ground—On a DB-25 pin connector, the chassis ground connection between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE). See also *DB-25 pin connector*, *DCE*, *DTE*.

protocol—A set of rules governing message exchange over a network or internetwork. Examples of commonly used protocols are Transmission Control Protocol/Internet Protocol (TCP/IP), Point-to-Point Protocol (PPP), and Internetwork Packet Exchange (IPX). See also *internetwork*, *IPX*, *network*, *PPP*, *TCP/IP*.

Protocol Data Unit—See *PDU*.

Protocol Identifier—See *PID*.

provisioning—The process of supplying telecommunications service and equipment to a user. In ISDN provisioning, for example, a telephone service provider configures its own switch that connects via an ISDN line to the user's ISDN hardware. Because switch configuration varies according to hardware, telephone company, switch, and available ISDN line, the user and provider must work together to establish the correct settings.

proxy ARP—Proxy Address Resolution Protocol. Proxy ARP denotes a configuration in which one unit handles address resolution requests for another device. In an ARP request, a device asks a host to provide the host's physical address so that a connection can take place. ARP requests are broadcast only on the local network. If a TAOS unit is the default router on a network and is configured in proxy mode, incoming packets destined for any of the hosts on the network go to the TAOS unit. If an ARP request requires a response from a remote host, the TAOS unit can respond on behalf of the remote host. See also *ARP*, *proxy mode*, *router*.

proxy authentication—A feature that enables an L2TP Access Concentrator (LAC) to forward a caller's name and password to an L2TP Network Server (LNS) on behalf of a dial-in Point-to-Point Protocol (PPP) client. Along with proxy LCP, proxy authentication enables a client's connection to be established quickly.

If a PPP client's profile is configured to initiate an L2TP tunnel, a TAOS unit operating as a LAC attempts to open a tunnel or reuse an existing tunnel after initial authentication of the connection. If the LAC preauthenticates the client's dial-in call by means of Calling-Line ID (CLID) or Dialed Number Information Service (DNIS), it initiates a tunnel to the LNS. The LNS then begins Link Control Protocol (LCP) negotiation with the mobile client.

If the LAC authenticates the PPP client's dial-in call by means of a name and password, it negotiates LCP with the client and then opens the PPP Auth state. If the information obtained from authentication on the LAC were not forwarded to the LNS, the LNS would have to restart negotiation with the client, slowing down link establishment.

With proxy authentication, the LAC completes PPP authentication of the dial-in call and then sends the caller's name and password to the LNS in the appropriate L2TP attribute-value pairs. Proxy authentication occurs for digital calls that are authenticated through any PPP authentication protocol (such as PAP, CHAP, or MS-CHAP) but not for analog PPP connections authenticated by a terminal-server login. For security reasons, the terminal server erases the caller's name and password immediately after authenticating the user.

See also *CHAP*, *CLID*, *DNIS*, *L2TP*, *LAC*, *LNS*, *MS-CHAP*, *PAP*, *PPP*, *proxy LCP*.

proxy Link Control Protocol (LCP)—See *proxy LCP*.

proxy LCP—Proxy Link Control Protocol (LCP). A feature that enables an L2TP Access Concentrator (LAC) to forward LCP information to an L2TP Network Server (LNS) on behalf of a dial-in Point-to-Point Protocol (PPP) client. Along with proxy authentication, proxy LCP enables a client's connection to be established quickly.

If a PPP client's profile is configured to initiate a Layer 2 Tunneling Protocol (L2TP) tunnel, a TAOS unit operating as a LAC attempts to open a tunnel or reuse an existing tunnel after initial authentication of the connection. If the LAC preauthenticates the client's dial-in call by means of Calling-Line ID (CLID) or Dialed Number Information Service (DNIS), it initiates a tunnel to the LNS. The LNS then begins LCP negotiation with the mobile client.

If the information obtained from LCP negotiation on the LAC were not forwarded, the LNS would have to restart negotiation with the client, slowing down link establishment. By means of proxy LCP, the LAC forwards relevant LCP information. Instead of sending an empty LCP Config Request packet in the data stream to the LNS, the LAC sends the LNS the following information:

- The first LCP Config Request packet received from the client
- The last LCP Config Request packet received from the client
- The last LCP Config Request packet the LAC sent to the client

Proxy LCP occurs for digital calls that are authenticated through any PPP authentication protocol (such as PAP, CHAP, or MS-CHAP) but not for analog PPP connections authenticated by a terminal-server login.

See also *CHAP*, *CLID*, *DNIS*, *L2TP*, *LAC*, *LCP*, *LNS*, *MS-CHAP*, *PAP*, *PPP*, *proxy authentication*.

proxy mode—A mode in which a profile assigns a local IP address to a remote host. Local hosts see the remote host as though it were on the local network. When calls are made to the remote host, the TAOS unit acts on its behalf, replying to requests and forwarding packets. See also *proxy ARP*.

proxy service—A management service provided for one or more devices by another unit.

PSD—Power Spectral Density. PSD is the power of bandwidth divided by the bandwidth, expressed in dBm/Hz. A lower value means that the line consumes less power and has a lower capacity. A higher value means that the line consumes more power and has a higher capacity.

PSDN—Packet-Switched Data Network. A PSDN is a network in which no connection is required end to end. This type of network is very efficient for data transfer, and provides redundancy. Other circuits are automatically available if a line goes down. See also *packet-switched network, packet switching*.

pseudo-user profile—A RADIUS entry containing information that a TAOS unit can query. Unlike a RADIUS user profile, a pseudo-user profile does not exist for the purpose of authenticating a user. Rather, it enables you to set up static routes, Frame Relay systems, and other types of configurations. See also *user profile*.

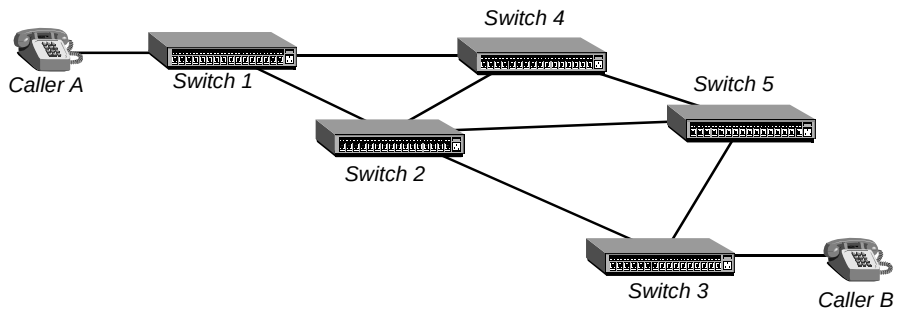
PSM—Path Selector Module. A Stinger module that provides redundancy and test functionality. A PSM contains the necessary circuitry to connect a failed Line Interface Module (LIM) or LIM port to a spare LIM or LIM port. When used for this purpose, a PSM is installed behind or next to the spare LIM in place of a Line Protection Module (LPM). A PSM can also replace an older interface redundancy module and provide access to individual copper loops for technical tests that use an external test head. See also *LIM*, *LPM*.

PSPDN—Packet-Switched Public Data Network. A PSPDN is an X.25 network. See also *X.25*.

PSTN—Public Switched Telephone Network. A PTSN is a public circuit-switched network for telephone users. Typically, real-time voice information is sent over the PSTN. Circuit-switched technology provides every call with dedicated bandwidth, usually 64Kbps. End-to-end calls are established on the basis of a sequence of dialed digits, and the PSTN dedicates a physical path between callers. Because the telephone equipment establishes the call path at the beginning of the call, the path can change between calls, but never while a call is active.

Figure 71 illustrates an example of a PSTN network. Caller A dials Caller B's telephone number. As Caller A dials the number, the network might route the call from Switch 1 to Switch 2 to Switch 3, which connects to Caller B. Once the PSTN establishes the call, communication travels only through Switch 1, Switch 2, and Switch 3.

Figure 71. Example of call routing over circuit-switched PSTN



If Caller A dials Caller B again, the PSTN might establish the call by routing it from Switch 1 to Switch 4 to Switch 5 to Switch 3 before finally connecting Caller A to Caller B. Again, the path can change between calls, but not during any specific call.

Compare with *IP network*. See also *circuit switching.*

PT—Payload Type. A 3-bit field in an Asynchronous Transfer Mode (ATM) cell header, the PT indicates whether the cell contains management information or user information. The network or terminating equipment uses this field to provide various traffic-handling mechanisms. See also *ATM*.

PTSE—PNNI Topology State Element. Private Network-to-Network Interface (PNNI) topology information distributed to all logical nodes in a peer group. When the PNNI link in a TAOS unit initializes, it sends a Hello packet on a Routing Control Channel (RCC). The Hello packet contains state and nodal information such as link status and peer group ID. After the node is established within its peer group, it periodically updates the information in PTSEs. The updated PTSEs are flooded among the nodes of the peer group by means of PNNI Topology State Packets (PTSPs), so that the topology database is synchronized for all nodes in the group. See also *PNNI*, *PNNI peer group*.

PTSP—PNNI Topology State Packet. A type of Private Network-to-Network Interface (PNNI) routing packet used for distributing PNNI Topology State Elements (PTSEs) to all logical nodes in a peer group. See also *PNNI*, *PNNI peer group*, *PTSE*.

Public Data Network—See *PDN*.

public-key encryption—An encryption method that bases an encryption algorithm on the two halves of a long bit string. Each half of the bit sequence corresponds to a key. One key resides in a public-key library. Only a single party knows the other key. You can use either key to encrypt the data, but both keys are required to decrypt it. The sender can encrypt the data with the receiver's public key, and the receiver can decrypt it with the private key. Or, the sender can use the private key to encrypt the message, and the receiver can use the public key to decrypt it. Compare with *private-key encryption*. See also *encryption*.

Public Switched Telephone Network—See *PSTN*.

Pulse Coded Modulation—See *PCM*.

pulse dialing—A method of dialing in which the modem sends a certain number of pulses (which you hear as clicks) to represent each digit of a telephone number. Pulse dialing is generally associated with rotary-dial telephones.

PVC—Permanent Virtual Circuit. A PVC is a path maintained by two stations. The path can include a number of hops. The circuit is through the packet-switched network, but stays up all the time, regardless of whether or not data is on the line. Because the circuit is always up, there is no circuit setup time. A PVC can be a virtual link that terminates in the TAOS unit or a virtual link that is cross-connected to another virtual link on a different interface. Compare with *Frame Relay SVC*, *SVC*. See also *multinetwork PVC*, *packet-switched network*, *packet switching*.

Q

Q.850—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that specifies the format, encoding, and semantics of cause information elements and parameters and the usage of the location field in the Signaling System 7 (SS7) ISDN User Part. See also *SS7*.

Q.93B—An International Telecommunication Union (ITU) recommendation detailing the signaling protocol for establishing and maintaining Switched Virtual Channels (SVCs) in an Asynchronous Transfer Mode (ATM) configuration.

Q.931—An International Telecommunication Union (ITU) recommendation for a signaling standard that supports Switched Virtual Circuits (SVCs) over ISDN. Q.931 is the basis of the Asynchronous Transfer Mode (ATM) and Frame Relay signaling standards. See also *ATM*, *Frame Relay*.

Q.931+—An International Telecommunication Union (ITU) recommendation based on Q.931. Q.931+ provides additional functions required for the Signaling System 7 (SS7) signaling gateway interface. See also *Q.931*, *SS7*.

Q.931 en-bloc dialing—The process of sending all dialed digits to a TAOS unit in one block. Q.931 en-bloc dialing is also known as *senderized digit transmission.* See also *Q.931*.

Q.931 Layer 3 SETUP_ACK timer.—See *T302 timer*.

Q.931W GloBanD—See *GloBanD*.

QoS—Quality of Service. QoS denotes the process by which one can measure, improve, and predict data rates, error rates, and other facets of network transmission. QoS is particularly important for the transmission of high-bandwidth video and multimedia data. When you use the Resource Reservation Protocol (RSVP), you can use criteria prepared in advance to expedite packets going through a gateway. Asynchronous Transfer Mode (ATM) enables you to specify QoS by means of the following values: Cell Loss Ratio, Cell Transfer Delay, and Cell Delay Variation. See also *ATM*, *RSVP*.

QoS contract—Quality of Service contract. A QoS contract defines an Asynchronous Transfer Mode (ATM) service category and related traffic characteristics. An ATM Permanent Virtual Circuit (PVC) is typically assigned a QoS contract for each direction of the connection. The ATM switches that reside between the source and destination agree to meet a requested QoS as long as the end nodes comply with the negotiated QoS contract. The ATM network can make use of traffic-management capabilities, such as altering the characteristics of a cell stream, to meet the QoS objectives and ensure that the contract is enforced. See also *ATM*, *PVC*, *QoS*.

Q.SAAL—An ATM Adaptation Layer (AAL) protocol that defines the reliable transmission and reception of signaling data between Asynchronous Transfer Mode (ATM) end points. See also *AAL*, *ATM*.

QTP—Quick Transaction Protocol. QTP is a symmetrical protocol that operates over User Datagram Protocol (UDP) in both directions between a TAOS unit and transaction servers on a Short-Duration Transaction Network (SDTN). QTP establishes and releases the virtual connection between systems, transports transaction traffic, and exchanges periodic Status Report messages. See also *SDTN*.

QTP Status Report message—Quick Transaction Protocol Status Report message. On a Short-Duration Transaction Network (SDTN), a QTP Status Report message enables the system to keep its transaction server selection table up-to-date. A QTP Status Report message from a transaction server can contain the following flow control attributes, indicating how busy the server is:

- Available (0x01)
- Partly Congested (0x02)
- Congested (0x03)
- Shut down (0x04)

A QTP Status Report message can also contain the Primary Station (0x01) or Secondary Station (0x02) status attribute, indicating whether the server is on the primary or secondary selection list. See also *QTP*, *SDTN*.

Quality of Service—See *QoS*.

Quality of Service contract—See *QoS contract*.

queue—A set of items arranged in a defined sequence.

queue depth—The maximum number of unprocessed requests that a TAOS unit saves.

Quick Transaction Protocol—See *QTP*.

Quick Transaction Protocol Status Report message—See *QTP Status Report message*.

quiesce—To take a line or modem out of service without disconnecting any current users.

R

R1 signaling—A multifrequency inband signaling system that uses a set of register signals, known as MFR1 tones, for call-addressing purposes. Each telephone number is preceded by a KP pulse, and followed by an ST pulse denoting the end of addressing. You can use R1 signaling with Automatic Number Identification (ANI), which is similar to Caller ID (CLID). When ANI is in use, you can specify whether to send an Automatic Number ID Request (ANIR) to the switch. If you specify that the unit should send an ANIR to the switch, you can also specify how long it waits before sending the request and how long the ANIR signal lasts. R1 signaling is supported on both E1 and T1 lines. See also *ANI*, *CLID*, *E1 line*, *T1 line*.

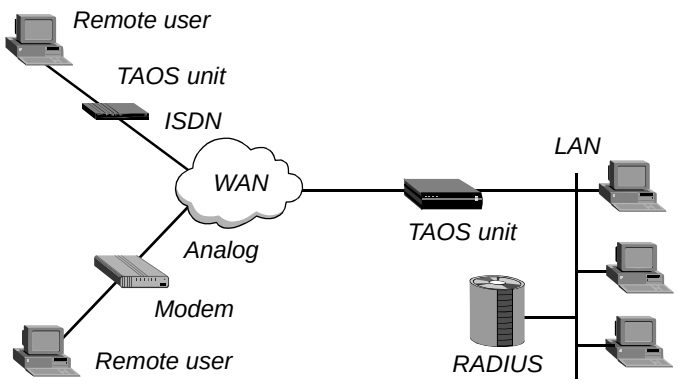
R2 signaling—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) signaling protocol for establishing and clearing 64Kbps switched circuits on E1 digital trunks. Signaling is performed through a combination of A/B bit manipulation in channel 16 of the E1 frame, and inband MF tone generation and detection. The relevant specifications are found in ITU-T recommendations Q.400 through Q.490. R2 signaling is widely implemented in international markets in which ISDN PRI signaling is not yet available. See also *E1 line*, *ITU-T*.

RACP—Receive ATM Cell Processor. An RACP is a processor that delineates received Asynchronous Transfer Mode (ATM) cells; filters received cells on the basis of their idle status, unassigned status, or associated Header Check Sequence (HCS) errors; and descrambles the received cell's payload. Compare with *TACP*. See also *ATM*, *HCS*.

RADIPAD—RADIUS IP Address Daemon. RADIPAD is a program that works with RADIUS to manage IP address pools centrally, so that all connections can acquire an address from a global pool, regardless of which system answers the call. RADIPAD runs on one RADIUS server on the network. A TAOS unit sends an authentication request to RADIUS, and if the user profile contains an attribute specifying allocation of an IP address from the global pool, RADIUS sends a request to RADIPAD to acquire the address. See also *global IP address pool*, *IP address pool*, *RADIUS*, *RADIUS server*.

RADIUS—Remote Authentication Dial-In User Service. When you install and configure RADIUS, end users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, callback, Serial Line Internet Protocol (SLIP), and Point-to-Point Protocol (PPP). It also enables you to set up accounting. You can keep records of the number of packets the TAOS unit transmits and receives, the protocol in use, the username and IP address of the client, and other system information. In Figure 72, the RADIUS server performs both authentication and accounting.

Figure 72. RADIUS authentication and accounting



In a RADIUS query, a TAOS unit provides a user ID and password to the server. The server sends back a complete profile, which specifies routing, packet filtering, and restrictions specific to the user. In addition, the TAOS unit can use the data in the RADIUS database to create and advertise static routes and to place outgoing calls.

The communications channel between a RADIUS client and server is provided by UDP/IP, with messages acknowledged. The primary advantage in using RADIUS to authenticate incoming calls is that you can maintain all user information offline on a separate UNIX-based server. The server can accept authentication requests from many machines, which makes swapping out one dial-in network server for another much easier.

See also *accounting*, *authentication*, *packet filter*, *pseudo-user profile*, *routing*, *static IP route*, *user profile*.

RADIUS accounting—See *accounting*.

RADIUS daemon—The daemon that provides users with RADIUS authentication and accounting.

RADIUS IP Address Daemon—See *RADIPAD*.

RADIUS server—The machine on which the RADIUS daemon is running. A single RADIUS server can administer multiple security systems, maintaining profiles for thousands of users. See also *RADIUS, RADIUS daemon*.

RADIUS timeout—The number of seconds between retries to the RADIUS server. If a TAOS unit is acting as a RADIUS client, it waits the specified number of seconds for a response to an authentication request. If it does not receive a response within that time, it times out and sends the authentication request to the next authentication server. See also *authentication server*, *RADIUS*.

RADSL—Rate-Adaptive Digital Subscriber Line. RADSL uses either Carrierless Amplitude Phase (CAP) modulation or Discrete MultiTone (DMT) modulation, two line-encoding techniques that optimize data-transmission rates. To optimize performance, RADSL also adjusts the transmission to the quality of the telephone line. Compare with *ADSL*, *HDSL*, *IDSL*, *SDSL*, *VDSL*. See also *CAP*, *DMT*, *DSL*, *rate adaptation*.

RAI—Remote Alarm Indicator. An RAI indicates that a device on the T1 line, DS3 line, or DS2 stream is detecting framing-error conditions in the signal it receives. An RAI is also called a *Yellow Alarm signal*. Compare with *Blue Alarm signal*, *Red Alarm signal*. See also *DS3 line*, *T1 line*.

RAM—Random Access Memory. RAM is computer memory that holds data temporarily. See also *DRAM*, *NVRAM*.

Random Access Memory—See *RAM*.

random vector attribute-value pair—See *random vector AVP*.

random vector AVP—Random vector attribute-value pair. An AVP used to hide other AVPs in a Layer 2 Tunneling Protocol (L2TP) configuration. See also *AVP*.

RARP—Reverse Address Resolution Protocol. RARP is a TCP/IP protocol that learns a workstation's hardware address and maps it to an IP address. See also *ARP*.

RAS—(1) Registration, Admission, and Status. Used in a MultiVoice environment, RAS is a protocol that handles registration, admission, bandwidth allocation, system status, and disengagement procedures between the MultiVoice gateway and the MultiVoice gatekeeper. See also *MultiVoice™*.

(2) Remote Access Server. A network unit that enables branch offices, telecommuters, and traveling computer users to gain access to the corporate LAN backbone over dedicated or dialed, digital or analog lines. See also *APX 8000™*.

rate adaptation—A capability that enables a Rate-Adaptive Digital Subscriber Line (RADSL) signal to continue to transmit data even if noise is blocking some frequencies. Single, unshielded twisted-copper cable is subject to noise from external sources and nearby cables. Without rate adaptation, Digital Subscriber Line (DSL) equipment cannot adjust to noise on the line and is forced to drop the signal. Rate adaptation bypasses impaired frequencies, and the transmission continues. The system resumes the use of the bypassed frequencies as soon as the line is clear. See also *DSL*, *RADSL*.

rate adaption—A data-transmission method that enables a TAOS unit to send and receive data moving at a rate of 56Kbps over a 64Kbps channel. For incoming calls, the unit automatically adapts the data received at 56Kbps to the 64Kbps channel. For outgoing calls, the unit sets the data rate to either 64Kbps or 56Kbps. V.120 is a rate-adaption standard. See also *RADSL*, *V.120*.

Rate-Adaptive Digital Subscriber Line—See *RADSL*.

rate enforcement—A process in which a network measures the actual traffic flow across a given connection and then compares it to the total admissible traffic flow. If congestion develops, traffic in excess of the acceptable level can be tagged and discarded on the way to its destination. Asynchronous Transfer Mode (ATM) and Frame Relay use rate enforcement. See also *ATM*, *Frame Relay*.

rate limit—See *multicast rate limit*.

rate monitoring—A set of rules that describes traffic flow. The sender has a mechanism to ensure that the transmission of its guaranteed packets functions in a certain way. The network knows what kind of traffic to expect and monitors the behavior of the traffic. The standard rate-monitoring definitions for Frame Relay are as follows:

- Committed Information Rate (CIR)
- Committed Burst (Bc)
- Excess Burst (Be)
- Discard Eligibility (DE)
- Committed Rate Measurement Interval (Tc)

See also *Bc*, *Be*, *CIR*, *DE*, *Frame Relay*, *Tc*.

Raw 802.3—See *802.3*.

Raw TCP—Raw Transmission Control Protocol. Raw TCP is a method of supporting encapsulation performed by an application that runs on top of TCP. Raw TCP must be understood by both the login host and the caller. As soon as the connection is authenticated, the TAOS unit establishes a TCP connection to the host. Raw TCP is also known as *TCP-Clear*. See also *TCP*, *V.120*.

Raw Transmission Control Protocol—See *Raw TCP*.

RBOC—Regional Bell Operating Company. An RBOC is one of six companies created after the breakup of AT&T. The RBOCs are Ameritech, Bell Atlantic, Bell South, Pacific Telesis, Southwestern Bell, and U.S. West.

RC4—A proprietary stream cipher from RSA Data Security, Inc. See also *authentication*, *encryption*.

RCC—Routing Control Channel. A Virtual Channel Connection (VCC) over which Private Network-to-Network Interface (PNNI) routing protocol messages are exchanged. When the PNNI link in a TAOS unit initializes, it sends a Hello packet on an RCC. The Hello packet contains state and nodal information such as link status and peer group ID. See also *PNNI*, *VCC*.

RCCP message—Request Packet Pass-Through Call message. A call-request message sent by a Signaling System 7 (SS7) signaling gateway to a TAOS unit. An RCCP message contains the call-setup information that a TAOS unit needs for routing a call to its destination, including all Internet Protocol (IP) addressing, Real-Time Transport Protocol (RTP) port setup, codec, and packet-loading information. Compare with *ACCP message*. See also *RTP*, *signaling gateway*, *SS7*.

RCF—Registration Confirmation. A MultiVoice Access Manager (MVAM) device sends a TAOS unit an RCF packet to inform the device that its Registration Request (RRQ) has been accepted. Compare with *RRJ*, *RRQ*. See also *MultiVoice*™, *MVAM*.

RCR message—Release Channel Request message. An Internet Protocol Device Control (IPDC) call-control message sent between the Remote Access Server (RAS) and the signaling gateway, requesting that the call channel be closed because a caller has been disconnected. At a minimum, this message reports the cause code that identifies how the call was terminated, and the source port type, source module number, source line number, and source channel number assigned to that call. The port information corresponds to the Public Switched Telephone Network (PSTN) port associated with the connection. For pass-through calls, the identified channel is opened by the source RAS. Compare with *ACR message*. See also *IPDC*, *PSTN*, *RAS*, *signaling gateway*.

RD—Receive Data. RD is a signal that indicates that the modem is receiving data from a remote device. See also *DB-25 pin connector*.

RDI—Restricted Digital Information. A category of data transfer in which the eighth bit of each byte is always set to 1. Compare with *UDI*.

RDP—Reliable Data Protocol. RDP provides a reliable data transport service for packet-based applications. It is simple to implement, and works efficiently in environments that have long transmission delays and nonsequential delivery of message segments.

reachable address—An Asynchronous Transfer Mode (ATM) address that either is directly reachable through one of the TAOS unit's interfaces or is reachable through an advertising node that the unit can reach. See also *ATM*.

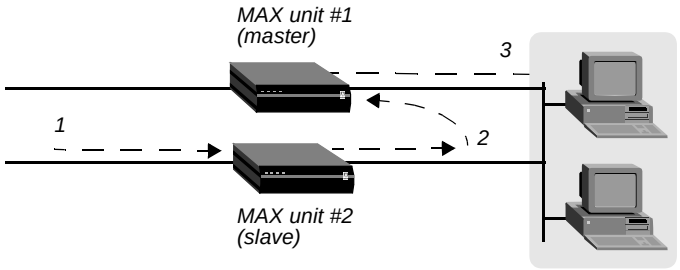
reachable address prefix—A prefix that enables a TAOS unit to reach all end systems and other nodes whose Asynchronous Transfer Mode (ATM) addresses match the prefix. See also *ATM*.

Read-Only Memory—See *ROM*.

real channels—Channels that connect directly to the TAOS unit that owns the bundle in a stacked configuration.

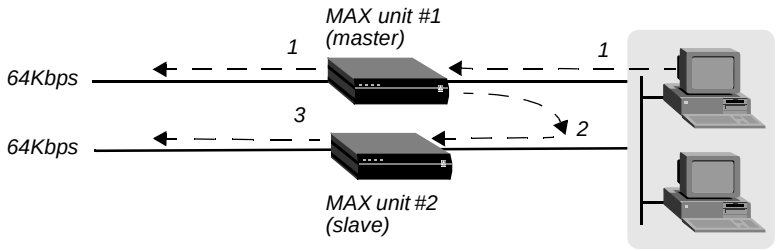
For example, assume that the initial call of an MP/MP+ bundle connects to MAX unit #1. This connection is a *real* channel. MAX unit #1 is the bundle owner, and it manages the traffic for both channels of the bundle. Next, as shown in Figure 73, the second call of the bundle connects to MAX unit #2. This connection is a *stacked* channel. MAX unit #2 forwards any traffic from the WAN to MAX unit #1, which sends it to its destination.

Figure 73. Packet flow from the slave channel to the Ethernet network



Likewise, as shown in Figure 74, MAX unit #1 receives all Ethernet traffic destined for the bundle, and disperses the packets between itself and MAX unit #2.

Figure 74. Packet flow from the Ethernet network



MAX unit #1 forwards some of the packets across the WAN through a real channel. MAX unit #2 sends the rest of them through a stacked channel.

Compare with *stacked channels*. See also *bundle*, *bundle owner*, *stack*.

real-time fax over IP—In a MultiVoice environment, an implementation of the ITU-T T.38 standard for fax transmission across IP networks. The system uses the Voice over IP (VoIP) framework for call establishment, fax initiation, and detection of an incoming fax call. Real-time fax communications require guaranteed Quality of Service (QoS) between the two fax-capable MultiVoice gateways. The packet loss on the network must be less than 1%.

If a TAOS unit has been licensed for real-time fax, users can run either a high-speed modem, with speeds greater than 2400bps, or a fax terminal in the VoIP channel. This capability provides a fallback for real-time fax transmissions. Both fax terminals and high-speed modems transmit a single tone when they answer a call, but they do not use the same tone. The TAOS unit can therefore detect the type of equipment answering the call and send the appropriate H.245 request-mode message. For a transparent modem, the message requests a switchover from the current audio codec to G.711 with no echo canceler. For real-time fax, the request is to switch to T.38 data mode.

See also *MultiVoice™*, *QoS*, *T.38*, *VoIP*.

Real-Time Streaming Protocol—See *RTSP*.

Real-Time Transport Control Protocol—See *RTCP*.

Real-Time Transport Protocol—See *RTP*.

reboot—To restart the computer and reload the operating system.

Receive ATM Cell Processor—See *RACP*.

Receive Data—See *RD*.

receive data rate—The rate of data received by a TAOS unit. Compare with *transmit data rate*.

Receive Line Overhead Processor—See *RLOP*.

receiver/transmitter echo—The acoustic echo generated at the calling end point of a connection. See also *echo cancellation, echo tail*.

Receive Section Overhead Processor—see *RSOP*.

Recognized Private Operating Agency—See *RPOA*.

Red Alarm signal—A signal indicating that an out-of-frame condition has lasted for more than 2.23ms on the T1 or DS3 line, or more than 9.9ms on the DS2 stream. Compare with *Blue Alarm signal*, *RAI*. See also *DS3 line*, *out-of-frame condition*, *T1 line*.

red frame—A type of frame forwarded with the Discard Eligibility (DE) bit if the graceful discard feature is enabled on the Frame Relay switch. If the number of bits received during the current time interval, including the current frame, is greater than the Excess Burst (Be) size, the frame is designated as a red frame. (If the graceful discard feature is disabled, the frame is simply discarded.)

Congested nodes that must discard packets use the color designations to determine which frames to discard. Red frames are discarded first, followed by amber frames, and then by green frames. Compare with *amber frame*, *green frame*. See also *Be*, *DE*, *Frame Relay*, *graceful discard*, *Tc*.

redialer—A hardware device connected to a fax machine. The redialer intercepts the number dialed on the fax machine and initiates a call to the TAOS unit, which transfers the transmission to the Internet. The transfer to the Internet is transparent to the person sending a fax. See also *IP fax*.

Reduced-Instruction-Set Computing—See *RISC*.

redundancy—A method of safeguarding against line and equipment failure during a transmission. Each method for transmitting signals has inherent error rates, and all physical media is subject to damage. In the event of hardware failure, a redundant line or unit can take over at any time. You should always have a redundant (backup) module for multiplexers and other critical equipment.

redundant packet data—The last *n* packets transmitted on the connection and appended by the TAOS unit to the current packet of a real-time fax transmission. Appending previously sent packets onto the current packet improves the reliability of real-time fax transmissions on a network experiencing measurable packet loss. See also *real-time fax over IP*.

registration—A process whereby a TAOS unit informs the unit running MultiVoice Access Manager (MVAM) of its identity and availability for processing Voice over IP (VoIP) calls. The TAOS unit sends its transport and alias addresses across the Registration, Admission, and Status (RAS) channel to the MVAM unit, along with a Registration Request (RRQ). MVAM responds with either a Registration Confirmation (RCF) or a Registration Reject (RRJ) message. See also *MultiVoice™*, *MVAM*, *RAS*, *RCF*, *RRJ*, *RRQ*, *VoIP*.

Registration, Admission, and Status—See *RAS*.

Registration Confirmation—See *RCF*.

Registration Reject—See *RRJ*.

Registration Request—See *RRQ*.

reject interface—An interface that enables a router to handle packets whose IP address matches an unused IP address in a summarized address pool. The reject interface has an IP address of 127.0.0.2. When you specify this address as the router to the destination pool network, the TAOS unit rejects packets to an invalid host on that network, appending an ICMP Host Unreachable message. See also *pool summary*.

relative transit time—The difference between a packet's Real-Time Transport Protocol (RTP) timestamp at the sender and the receiver's clock at the time of arrival. See also *RTP*.

Release Channel Completed message—See *ACR message*.

Release Channel Request message—See *RCR message*.

release indication timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum amount of time that can elapse between the transmission of a Release message and the receipt of a Release or Release Complete message. The release indication timer is also called the *T308 timer*. See also *ATM*.

Reliable Data Protocol—See *RDP*.

remote access—See *remote LAN access*.

Remote Access Server—See *RAS*.

Remote Alarm Indicator—See *RAI*.

Remote Authentication Dial-In User Service—See *RADIUS*.

remote connection—A workstation-to-network connection that uses a modem and a telephone line. The remote link enables you to send or receive data over greater distances than a connection that uses conventional cabling.

remote device—A unit that resides across the WAN.

remote LAN access—The process of enabling branch offices, telecommuters, and traveling computer users to gain access to the corporate LAN backbone over digital or analog lines. The lines can be switched or dedicated. See also *analog line*, *dedicated line*, *digital line*, *switched line*.

remote loopback—A procedure that tests the entire connection from host interface to host interface, enabling the TAOS unit to place a call to itself over the WAN and to send a user-specified number of packets over the connection. The data loops at the serial port interface of the remote TAOS unit, and comes back to the local TAOS unit. The remote loopback tests the local unit's ability to initiate and receive calls, and diagnoses whether the connection over the digital access line and the WAN is sound. Compare with *local loopback*. See also *analog loopback*, *digital loopback*, *loopback*.

remote management—A management feature that uses bandwidth between sites over a management subchannel. Any TAOS unit can control, configure, and obtain statistical and diagnostic information about any other TAOS unit. Multilevel security assures that unauthorized personnel do not have access to remote-management functions.

remote network—A network to which a local TAOS unit connects over the WAN.

Remote Procedure Call—See *RPC*.

remote profile—A user profile configured in RADIUS, TACACS, or TACACS+, as opposed to a profile configured on the TAOS unit. See also *user profile*.

remote user—A user at a device not connected directly to the TAOS unit and not residing on the local Ethernet network—in other words, a user across the WAN.

REN—Ringer Equivalency Number. A REN indicates the total loading effect of the subscriber's equipment on the ringing current generator at the Central Office (CO). A REN of 1 indicates the equivalent of a single traditional telephone circuit. A modem can be associated with a REN lower than 1. Your telephone company can set a limit for the total REN of a subscriber's loop. If some of the individual RENs are less than 1, the number of devices on the loop can be greater than the REN limit.

repeater—A device that receives data on one communications link and transmits it, one bit at a time, onto another link. The repeater uses no buffering, but transmits the data as soon as it receives it.

replay attack—A strategy for gaining illegal access to a system. During a replay attack, an unauthorized user records valid authentication information exchanged between systems, and then replays it later to gain entry. Token-card authentication protects your system against replay attacks. Because the token is a one-time-only password, replay is impossible. See also *token-card authentication*.

replay protection—An Internet Protocol Security (IPSec) feature that enables you to counter Denial of Service (DoS) attacks. The receiving system uses a sequence number to detect the arrival of duplicate packets within a constrained window. See also *DoS attack*, *IPSec*.

reply item—One or more components of a RADIUS user profile that the RADIUS server sends to the Network Access Server (NAS) to specify a user's connection when all check items in the profile have been satisfied by the Access-Request packet. See also *Access-Request packet*, *check item*, *NAS*, *RADIUS*.

Request For Comments—See *RFC*.

Request Packet Pass-Through Call message—See *RCCP message*.

Request Test Echo—See *RTE*.

Request To Send—See *RTS*.

Reservation Protocol—See *RSVP*.

Reset-Confirmation packet—On an X.25 connection, a packet sent in response to a Reset-Request packet. Once the sending device receives a Reset-Confirmation packet, it can send data on the logical channel. See also *logical channel*, *Reset-Request packet*, *X.25*.

Reset-Request packet—At the packet layer of an X.25 network, a packet that resets the packet-sequence number for the logical channel to 0 (zero) and removes any outstanding data and Interrupt packets from the Virtual Circuit (VC). See also *VC*, *X.25*.

Reset-Request timer—A value that specifies the number of 10-second ticks that a TAOS unit waits before retransmitting a Reset-Request packet on an X.25 network. See also *Reset-Request packet*, *X.25*.

Reset Retries—The number of times a TAOS unit retransmits a Reset-Request packet on an X.25 network before clearing a call. See also *Reset-Request packet*, *X.25*.

Resource Management cell—See *RM cell*.

Resource Reservation Protocol—See *RSVP*.

Response timer—On an X.25/T3POS connection, a value that specifies the amount of time the Packet Assembler/Disassembler (PAD) waits for a SYN signal from the Data Terminal Equipment (DTE). The SYN signal indicates that the response from the DTE is being delayed and that the link is still alive. See also *DTE, PAD*.

Restart-Confirmation packet—On an X.25 network, a packet that signals a sending device that it can again issue a call to establish a Virtual Circuit (VC). See also *VC, X.25*.

Restart-Request packet—At the packet layer of an X.25 network, a packet that clears all Virtual Circuits (VCs). See also *Restart Retries, Restart timer, X.25*.

restart request timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum amount of time that can elapse between the transmission of a Restart message and the receipt of a Restart Acknowledge message. The restart request timer is also called the *T316 timer.* Compare with *connect request timer*. See also *ATM*.

Restart Retries—The number of times that a TAOS unit transmits a Restart-Request packet before waiting indefinitely for a response. See also *Restart-Request packet, X.25*.

Restart timer—On an X.25 network, a value that specifies the number of 10-second ticks a TAOS unit waits before retransmitting a Restart-Request packet. See also *Restart-Request packet, X.25*.

Restricted Digital Information—See *RDI*.

retry limit—The maximum number of times that a TAOS unit sends a packet or frame, or attempts to connect to another device, before giving up and clearing the connection. See also *retry timeout*.

retry timeout— The number of seconds between retries. See also *retry limit*.

Reverse Address Resolution Protocol—See *RARP*.

RFC—Request for Comments. RFC denotes the document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs. The RFC series of documents is unusual in that the proposed protocols are distributed by the Internet research and development community, acting on its own behalf. The protocols do not go through the formal review and standardization process promoted by organizations such as ANSI. A complete list of RFCs resides at `http://www.internic.net/rfc/`.

RI—Ring Indicate. RI is a signal that indicates that a call is coming into a unit.

ring lead—The end of a ring wire. Compare with *tip lead*. See also *CO*.

ring wire—The negative (-) wire in a telephone circuit. Compare with *tip wire*.

ringback tone—A tone that a TAOS unit generates when it answers an analog modem call. When the calling modem hears the ringback tone, it begins establishing the modem protocol. See also *early ringback*, *modem*.

Ringer Equivalency Number—See *REN*.

Ring Indicate—See *RI*.

RIP—Routing Information Protocol. RIP is a distance-vector protocol found in both the NetWare and TCP/IP protocol suites. The protocol keeps a database of routing information that it gathers from periodic broadcasts by each router on a network. See also *IPX*, *router*, *routing*, *TCP/IP*.

RIP queue—A queue containing unprocessed Routing Information Protocol (RIP) requests. Compare with *backoff queue*, *SNMP queue*, *UDP queue*. See also *queue*.

RIP triggering—A process that enables an IP router to tag routes that have been updated in its routing table and send updates that include only the changed routes. The result is reduced processing overhead for both the TAOS unit's router and its neighbors. Changes occur when a call arrives or disconnects, RIP or OSPF learns a route from another router, or the administrator modifies a route-related profile. The router broadcasts updates 5 to 8 seconds after the first change in the routing table is detected. The delay helps to prevent constant updates during peak traffic conditions. See also *IP router*, *OSPF*, *RIP*.

RISC—Reduced-Instruction-Set Computing. RISC is a microprocessor architecture designed for decoding and executing a small set of instructions, thereby optimizing performance.

Rlogin—An Application-layer, remote-login service provided by Berkeley UNIX. On a TAOS unit, Rlogin is available only from an asynchronous dial-in session to the terminal server. See also *Application layer*.

RLOP—Receive Line Overhead Processor. An RLOP is a processor responsible for line-level alarms and performance monitoring. Compare with *RPOP*, *RSOP*.

RM cell—Resource Management cell. A type of Asynchronous Transfer Mode (ATM) control cell used by the Explicit Forward Congestion Indication (EFCI) and Explicit Rate marking flow-control methods. An RM cell informs other switches in the network about bandwidth availability and network congestion. See also *ATM*, *EFCI*, *Explicit Rate marking*.

RMCP message—Request Modify Packet Pass-Through Call message. On a MultiVoice network, an RMCP message is sent by a Signaling System 7 (SS7) signaling gateway to a TAOS unit and specifies a request to modify one or more of the following values for a Voice over IP (VoIP) call:

- VoIP encoding type
- Packet loading rate in frames per packet
- Source port type
- Destination port type
- Listen Internet Protocol (IP) address
- Listen Real-Time Transport Protocol (RTP) port number
- Send IP address
- Send RTP port number

Compare with *AMCP message*. See also *MultiVoice™*, *SS7*.

robbed-bit signaling—See *inband signaling*.

ROM—Read-Only Memory. ROM is computer memory whose contents can be read and executed, but not modified. See also *EEPROM*, *PROM*.

root—See *superuser*.

rotary—A type of hunt group in which the incoming call hunts on a rotating basis for an available channel to ring and answer the call. See also *hunt group*.

route—The path that data takes from its source network to its destination network. See also *IP route*, *IPX route*.

route filter—A type of filter containing rules for the action to take on routes in Routing Information Protocol (RIP) update packets. When you apply a route filter to an IP interface, the TAOS unit monitors RIP packets on the interface and takes one of the following actions when a route matches the filter rules:

- No action (the default).
- Accept the route by allowing it to affect the routing table.
- Deny the route by not allowing it to affect the routing table.
- Add the specified value to the route metric and accept the route.

The filter can apply to incoming packets, outgoing packets, or both. When you apply a route filter to an interface, the TAOS unit applies all defined input and output filters to RIP update packets until it finds a match. If it does not find a match for a route, the default action is to deny the route. RADIUS does not support route filters. Compare with *packet filter*. See also *IP route*, *IP routing table*, *RIP*.

router—A device that determines a path from a host on one network to a host on another. The networks can be in close proximity, or can be separated by long distances. A router has access to the three lowest OSI layers, and generally operates at the Network layer. To route a packet, a router uses the logical address specified as the packet's destination field and determines the next router (if any) to which the packet must travel to reach its destination. All routers share information about the current topology and state of the network, and they maintain routing tables that reflect the latest information. See also *IP router*.

route recovery—An Open Shortest Path First (OSPF) routing function. When a tandem node or trunk becomes inoperative, the switch immediately recalculates new shortest-path routes for the affected Permanent Virtual Circuits (PVCs), and reroutes the circuits. Recovery time is typically less than four seconds. The network reports PVC rerouting as an event/alarm. See also *OSPF*.

router Home Agent—In an Ascend Tunnel Management Protocol (ATMP) configuration, a Home Agent whose routing module forwards packets it receives from the Foreign Agent onto the local network. The network can be the home network, or it can support another router that can connect to the home network. In either case, packet delivery relies on a routing mechanism, such as a static or dynamic route, and not on a WAN connection. Compare with *gateway Home Agent*. See also *ATMP*, *dynamic route*, *Foreign Agent*, *Home Agent*, *home network*, *static IP route*, *static IPX route*.

routing—A method of determining how to forward a data packet to its proper destination. See also *IP routing*, *IPX routing*, *OSPF*, *RIP*, *route*, *router*.

Routing Control Channel—See *RCC*.

Routing Information Protocol—See *RIP*.

routing protocol—A protocol that implements routing by means of a specific routing algorithm. Routing protocols include Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). See also *OSPF*, *RIP*.

routing table—See *IP routing table*.

Routing Table Maintenance Protocol—See *RTMP*.

RPC—Remote Procedure Call. An RPC is a method in which a program on one device can transparently use a procedure on another device. RPCs are often used in client/server architectures.

RPOA—Recognized Private Operating Agency. An RPOA is an agency that runs a telecommunications service.

RPOP—Receive Path Overhead Processor. An RPOP is a processor that interprets pointers, extracts both path overhead and the synchronous payload envelope, sends path-level alarms, and monitors performance. Compare with *RLOP*, *RSOP*.

RRJ—Registration Reject. A unit running MultiVoice Access Manager (MVAM) sends a TAOS unit an RRJ packet in response to a Registration Request (RRQ) packet if MVAM does not grant the request to be registered. Compare with *RCF*, *RRQ*. See also *MultiVoice™*, *MVAM*.

RRQ—Registration Request. A TAOS unit sends an RRQ packet to inform MultiVoice Access Manager (MVAM) of its identity and availability for processing Voice over IP (VoIP) calls. Compare with *RCF*, *RRJ*. See also *MultiVoice™*, *MVAM*, *VoIP*.

RS-232—An EIA standard that specifies various electrical and mechanical characteristics for interfaces between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) devices. The standard applies to both synchronous and asynchronous binary data transmission at rates below 64Kbps. RS-232 is also known as *EIA/TIA-232*. Compare with *RS-422*, *RS-423*. See also *asynchronous transmission*, *DCE*, *DTE*, *synchronous transmission*.

RS-232C—The latest version of the RS-232 standard. See also *RS-232*.

RS-366—An EIA standard that specifies commands for dialing in to network-access equipment. Although RS-366 uses RS-232 electrical specifications, it specifies different pinouts and signal functions. See also *RS-232*.

RS-422—A standard EIA interface for connecting serial devices. Along with RS-423, RS-422 replaces the RS-232 standard. RS-422 supports higher data rates than RS-232 and offers greater protection against electrical interference. All Apple Macintosh computers contain an RS-422 port that you can use for RS-232 as well as RS-422 communication. RS-422 supports multipoint connections, while RS-423 does not. RS-422 and RS-423 are often referred to collectively as *EIA-530*. Compare with *RS-232*, *RS-423*. See also *EIA*, *multipoint link*.

RS-423—A standard EIA interface for connecting serial devices. Along with RS-422, RS-423 replaces the RS-232 standard. RS-423 supports higher data rates than RS-232 and offers greater protection against electrical interference. All Apple Macintosh computers contain an RS-423 port that you can use for RS-232 as well as RS-423 communication. Unlike RS-422, RS-423 supports only point-to-point connections. RS-422 and RS-423 are often referred to collectively as *EIA-530*. Compare with *RS-232*, *RS-422*. See also *EIA*, *point-to-point link*.

RS-442—An EIA standard that specifies the electrical characteristics of balanced-voltage digital circuits. RS-442 applies to high-speed, synchronous links between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE). Compare with *RS-443*. See also *DCE*, *DTE*.

RS-443—An EIA standard that specifies the electrical characteristics of unbalanced-voltage digital circuits. RS-443 applies to high-speed, synchronous links between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE). Compare with *RS-442*. See also *DCE*, *DTE*.

RS-449—A standard EIA Physical-layer interface. RS-449 is a faster version of RS-232 and allows longer cable extension. RS-449 can run at speeds of up to 2Mbps. It is also known as *EIA/TIA-449*. Compare with *RS-232*.

RSOP—Receive Section Overhead Processor. On an OC3-ATM interface, an RSOP is a processor that synchronizes and descrambles frames, provides section-level alarms, and monitors performance. Compare with *RLOP*, *RPOP*.

RSVP—Reservation Protocol. RSVP enables a router to reserve bandwidth for time-sensitive data transmissions, resulting in smooth reception of voice and video data. A client can use RSVP to request that a router set aside a certain amount of bandwidth to handle the incoming call. If sufficient bandwidth does not exist, the request enters a queue and remains there until the appropriate amount of bandwidth becomes available.

RT-24 codec—A Lucent Technologies proprietary audio codec that compresses speech samples from 64Kbps Pulse Code Modulation (PCM) to 2.4Kbps, reducing the effective bandwidth required for transmission across the Internet Protocol (IP) network. This codec uses a 22.5ms audio frame, and encapsulates audio at 8 bytes per frame. The decoder produces 180 samples of audio from the 8-byte encoder output. The RT-24 codec is available for both H.323 Voice over IP (VoIP) calls and Signaling System 7 (SS7) VoIP calls. See also *audio codec*, *codec*, *H.323*, *IP network*, *PCM*, *SS7*, *VoIP*.

RTCP—Real-Time Transport Control Protocol. RTCP enables a system to monitor the Quality of Service (QoS) and to transmit information about the participants involved in a real-time audio or video session. See also *QoS*, *RTP*.

RTE—Request Test Echo. An Internet Protocol Device Control (IPDC) heartbeat message sent from a TAOS unit to a signaling gateway. If the signaling gateway is a Lucent Softswitch and the RTE message contains a congestion indicator, the gateway can respond to the congestion indication by slowing down the rate at which it forwards calls. For any other type of signaling gateway, the RTE message is used only as a signaling heartbeat message.

If congestion control is enabled (as it is by default), the TAOS unit monitors the depth of the Layer-3 queue as a measure of call congestion. The queue contains messages for the IPDC layer, including call control and other network messages, as well as messages from IPDC itself.

If the number of messages in the queue exceeds congestion level 1, the unit can either ignore the congestion level or send an RTE message with a congestion level indicator showing that level 1 has been exceeded (the default). If the number of messages drops below the specified congestion level 1, the unit sends an RTE message indicating congestion level 0 (no congestion). If the number of messages in the queue exceeds congestion level 2, the unit can ignore the congestion, send the signaling gateway an RTE message indicating that congestion level 2 has been exceeded, or send the message and reject new calls (the default).

See also *ARTE*, *IPDC*, *Softswitch*.

RTMP—Routing Table Maintenance Protocol. RTMP is Apple Computer's proprietary routing protocol.

RTP—Real-Time Transport Protocol. RTP provides end-to-end delivery services for real-time data (for example, interactive video and audio). RTP identifies the type of data being transmitted and provides packet sequencing, timestamping, and monitoring services. With RTP, a unit can use multicast services to transmit data if the network provides them. RTP does not provide Quality of Service (QoS) guarantees, nor does it ensure reliable delivery of all packets in the proper sequence. See also *QoS*, *RTCP*.

RTS—Request To Send. A transmitter sends an RTS signal to a receiver when ready to begin sending data. If the receiver is ready for the transmission, it responds with a Clear To Send (CTS) signal. See also *CTS*.

RTSP—Real-Time Streaming Protocol. An Application-level protocol for control over the on-demand delivery of real-time data, such as audio and video from live data feeds and stored clips. You can use RTSP to control multiple data-delivery sessions and to choose such delivery methods as User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Real-Time Transport Protocol (RTP). See also *RTP*, *TCP*, *UDP*.

rubber bandwidth—Bandwidth that can be increased or decreased without terminating and reestablishing the link. See also *bandwidth*.

S

SA—Security Association. An SA specifies how two or more devices use security services with the Authentication Header (AH) or Encapsulating Security Payload (ESP) protocol in an Internet Protocol Security (IPSec) environment. See also *AH*, *ESP*, *IPSec*, *SPI*.

SAAL—Signaling ATM Adaptation Layer. The SAAL is a mechanism for ensuring that signaling messages are reliably transported between network peers. It resides between the Asynchronous Transfer Mode (ATM) Layer and Q.2931 processing in the user's equipment. The purpose of the SAAL is to provide reliable transport of Q.2931 messages between peer Q.2931 entities, such as an ATM switch and a host, over the ATM Layer. The SAAL is subdivided into the Common Part (CP) and the Service-Specific Part (SSP). See also *ATM*, *CP*, *SSP*.

SafeWord authentication—A form of token-card authentication in which RADIUS forwards a connection request to an Enigma Logic SafeWord server. The SafeWord server sends an Access-Challenge packet back through the RADIUS server and the TAOS unit to the user dialing in. The user sees the challenge message, obtains the current password from his or her token card, and enters the current password (called a *token*).

The token travels back through the TAOS unit and the RADIUS server to the SafeWord server. The SafeWord server sends a response to the RADIUS server, specifying whether the user has entered the proper username and token. If the user enters an incorrect token, the SafeWord server returns another challenge, and the user can attempt to enter the correct token. The server sends up to three challenges. After three incorrect entries, the TAOS unit terminates the call. See also *authentication*, *authentication server*, *RADIUS server*, *SafeWord token*, *token-card authentication*, *token-card server*.

SafeWord token—A randomly generated access code that a user obtains from a token card when using a SafeWord authentication server. See also *SafeWord authentication*.

SAP—Service Access Point. A SAP is a defined location through which a procedure at one OSI layer can provide services to the layer above it. Each SAP has a unique address in hexadecimal format. See also *DSAP*, *OSI Reference Model*.

SAP—Service Advertising Protocol. SAP is a NetWare protocol that operates at the Transport layer and enables servers to inform other devices about the services they have available. Each server uses a SAP packet to advertise its services. Each router on the network retrieves the SAP packets and builds a database of all the servers it knows about. Each router then broadcasts this information to other routers, either at a set interval or whenever the database changes.

A TAOS unit follows standard SAP behavior for routers when connecting to non-TAOS units across the WAN. However, when it connects to another TAOS unit configured for IPX routing, both ends of the connection exchange their entire SAP tables, so that all remote services are immediately added to the TAOS unit's SAP table.

When a NetWare client sends a SAP request to locate a service, the TAOS unit consults its SAP table and replies with its own hardware address and the internal network address of the requested server. This behavior is analogous to the use of proxy ARP in an IP environment. The client can then transmit packets whose destination address is the internal address of the server. When the TAOS unit receives those packets, it consults its Routing Information Protocol (RIP) table. If it finds an entry for that destination address, it establishes the connection (unless it is already established) and forwards the packet. See also *IPX router*, *IPX server*, *proxy ARP*, *RIP*.

SAP filter—Service Advertising Protocol filter. A SAP filter determines which SAP advertisements a TAOS unit forwards or drops.

The TAOS unit examines incoming and outgoing SAP packets to determine whether certain fields in the packet match the filter. The unit then applies input filters to all SAP packets it receives. Input filters screen advertised services and exclude them from (or include them in) the unit's service table. The unit applies output filters to SAP response packets it transmits. If it receives a SAP request packet, the unit applies output filters before transmitting the SAP response, and excludes services from (or includes them in) the response packet.

A SAP filter enables you to control the size of resident SAP tables and reduce bandwidth usage. You can also use a SAP filter to restrict a user's view of services on the network. By turning off IPX SAP, you can prevent the TAOS unit from sending its SAP table or from receiving a remote site's SAP table.

See also *SAP*.

SAP home server proxy—Service Advertising Protocol home server proxy. SAP home server proxy is a feature that enables you to give remote users access to the same resources as local users. Rather than relying on the built-in functionality of SAP, you can configure a TAOS unit to direct SAP broadcasts to specified networks. The SAP responses come from servers on those networks, rather than from servers near the TAOS unit. See also *SAP*.

SAR—Segmentation and Reassembly. SAR is a sublayer of the ATM Adaptation Layer (AAL). The SAR sublayer is responsible for fragmenting the packets passed from the Convergence Sublayer (CS) in cells. See also *AAL*, *ATM*, *CS*.

SCCRQ—Start Control Connection Request. In a Layer 2 Tunneling Protocol (L2TP) configuration, a message sent by an L2TP Access Concentrator (LAC) to an L2TP Network Server (LNS), requesting L2TP tunnel negotiation. See also *L2TP*, *LAC*, *LNS*.

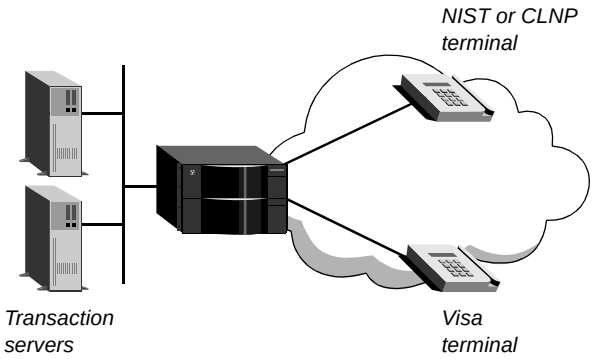
SCR—Sustainable Cell Rate. In an Asynchronous Transfer Mode (ATM) transmission, SCR is the average cell-transmission rate. Equivalent to Committed Information Rate (CIR) in Frame Relay, SCR is measured in cells per second and converted internally to bits per second. In general, SCR is a fraction of the Peak Cell Rate (PCR). Cells are sent at this rate if there is no credit. See also *ATM*, *CIR*, *Frame Relay*, *PCR*.

SDH—Synchronous Digital Hierarchy. SDH is an international standard for synchronous data transmission at a rate of 155.52Mbps over fiberoptic media. Compare with *NADH*.

SDSL—Symmetric Digital Subscriber Line. SDSL is a technology that transmits data at rates of up to 1.5Mbps over a single telephone line. The downstream transmission rate and the upstream transmission rate are the same. Compare with *ADSL*, *HDSL*, *IDSL*, *RADSL*, *VDSL*. See also *DSL*.

SDTN—Short-Duration Transaction Network. As a forwarding device on an SDTN, a TAOS unit receives calls from transaction client applications and transparently forwards them to a transaction server. Figure 75 shows a sample SDTN setup, with transaction servers on a local 100Mb Ethernet interface.

Figure 75. Sample SDTN setup



The TAOS unit recognizes High-Level Data Link Control–Normal Response Mode (HDLC-NRM) and Visa-II dial-in connections for transaction processing. Transaction data calls come in from National Institute of Standards and Technology (NIST), Connectionless Network Protocol (CLNP), or Visa terminals. The TAOS unit answers the calls and forwards them to the transaction server by means of Quick Transaction Protocol (QTP).

To determine which server to use for a particular transaction processing request, the TAOS unit uses a selection table. The table contains a primary and secondary list of transaction servers that have been entered by means of QTP. The TAOS unit uses only the primary list unless no available servers are left in the primary list, in which case it begins using the secondary list.

Each list entry specifies a transaction server's IP address, the User Datagram Protocol (UDP) port used by QTP on that server, and a metric that indicates the server's availability to the TAOS unit. The TAOS unit searches the list in cyclic order and chooses the first available server. The system keeps the table up-to-date on server availability and status by applying configurable metrics to information obtained from QTP Status Report messages and from real-time events, such as failure to receive a response to a call request.

See also *CLNP*, *HDLC-NRM*, *NIST*, *QTP*, *QTP Status Report message*, *UDP*.

sealing—The ability of an IDSL card to send a current (40V) on the line. You typically use this feature to keep the physical connection from corroding. Corrosion can occur when no activity occurs on the line.

secondary add-on number—For an ISDN BRI line, an alternative number that enables the calling TAOS unit to build multichannel calls. See also *AIM*, *BONDING*, *MP*, *MP+*, *primary add-on number*.

secondary CM—Secondary Control Module. On a Stinger unit, the secondary CM carries out the following tasks:

- Monitors the primary CM, using a heartbeat protocol
- Updates its own repositories of code and configuration settings whenever the primary CM is updated
- Immediately takes over operations if the primary CM fails

Compare with *primary CM*. See also *CM*.

secondary Control Module—See *secondary CM*.

secondary DNS server—The second server to which a TAOS unit attempts to gain access in order to perform name-address resolution on an IP network. See also *DNS*, *IP network*, *primary DNS server*.

secondary WINS server—The second server that a TAOS unit attempts to access for Windows Internet Name Service (WINS) name-address resolution on a Telnet or raw TCP connection running under the TAOS unit's terminal-server interface. See also *primary WINS server*, *WINS*.

section—On a SONET network, a single run of cable. Section-terminating equipment consists of any adjacent pair of switches. Compare with *line*, *path*. See also *SONET*.

Secure Hash Algorithm 1—See *SHA1*.

Secure Hash Algorithm 1–Keyed-Hashing for Message Authentication—See *SHA1-HMAC*.

SecurID—A brand of token card used with a Security Dynamics ACE/Server. The server generates a code based on a user's ID, a password, and specific information encoded in the card. When the user attempts to log in to a secure network, the token-card server requests a code generated within the previous 60 seconds. The server interprets the code. If the code is genuine, the server grants access to the user. See also *ACE authentication*, *ACE token*, *authentication*, *authentication server*, *Security Dynamics ACE/Server*, *token card*, *token-card authentication*, *token-card server*.

SecurID authentication—See *ACE authentication*.

SecurID ACE/Server—See *Security Dynamics ACE/Server*.

Security Association—See *SA*.

security card—See *token card*.

security-card authentication—See *token-card authentication.*

security-card server—See *token-card server.*

Security Dynamics ACE/Server—A type of authentication server that performs token-card authentication. See also *ACE authentication*, *ACE token*, *authentication*, *authentication server*, *SecurID*, *token card*, *token-card authentication*, *token-card server*.

Security Parameter Index—See *SPI*.

seed router—An IPX or AppleTalk router from which other routers learn their network configurations. Compare with *nonseed router*. See also *AppleTalk routing*, *IPX router*.

Segmentation and Reassembly—See *SAR*.

SEL subfield—Selector subfield. A subfield of the Domain-Specific Part (DSP) of an ATM End System Address (AESA). The SEL subfield is a hexadecimal number that is not used for routing but can be used by the end system. Compare with *ESI*, *HO-DSP*. See also *AESA format*, *DSP*.

Selective Discard—An Asynchronous Transfer Mode (ATM) flow-control mechanism. Selective Discard can be provisioned for Unspecified Bit Rate (UBR), Available Bit Rate (ABR), and Variable Bit Rate-Non Real Time (VBR-NRT) Virtual Channels (VCs). If the current cell causes the queue for a VC to exceed the discard thresholds, and the cell has Cell Loss Priority (CLP) set to 1, the cell is discarded. Note that Early Packet Discard (EPD) is not performed in this case. Compare with *EPD*. See also *ABR*, *ATM*, *CLP*, *UBR*, *VBR-NRT*, *VC*.

senderized digit transmission—See *Q.931W GloBanD*.

Send Tones message—See *STN message*.

Sequenced Packet Exchange—See *SPX*.

serial communication—Communication through the serial port of a device. See also *serial port*, *serial transmission*.

serial connection—A link between the serial ports of two devices. See also *serial communication*, *serial port*, *serial transmission*.

serial host—A device (such as a videoconferencing codec) that is connected to a serial WAN port communicating over a point-to-point link. To a serial host, the TAOS unit appears to be a cable or Data Circuit-terminating Equipment (DCE) device. See also *codec*, *DCE*, *point-to-point link*, *serial WAN port*.

Serial Line Internet Protocol—See *SLIP*.

serial port—A port that transmits and receives asynchronous or synchronous serial data. See also *asynchronous transmission*, *serial transmission*, *synchronous transmission.*

serial transmission—A form of data transmission in which only one line carries all eight bits of a byte. In serial transmission, one bit follows another (as opposed to parallel transmission, in which the bits travel simultaneously, each on a different wire). Serial transmission can be either synchronous or asynchronous. Synchronous communication requires additional lines for transmitting handshake or timing signals. In asynchronous communication, the data itself contains synchronization information, so neither handshaking nor clock signals are necessary. See also *asynchronous transmission*, *synchronous transmission*.

serial V.35 DTE port—See *serial WAN port.*

serial WAN port—A port that provides a V.35/RS-449/X.21 WAN interface, typically used to connect the TAOS unit to a Frame Relay switch.The clock speed received from the link determines the serial WAN data rate. The maximum acceptable clock speed is 8Mbps. The clock speed at the serial WAN port has no effect on the bandwidth of other WAN interfaces in the TAOS unit. See also *serial transmission.*

server—A device or program that provides services to hosts on a network.

server key—A RADIUS key used to validate the authenticator field on requests and generate the authenticator on responses. See also *authenticator field, RADIUS*.

Service Access Point—See *SAP*.

Service Advertising Protocol—See *SAP*.

Service Profile Identifier—See *SPID*.

Service-Specific Part—See *SSP*.

session—The state a connection has reached when two parties can communicate with each other.

session ID—A unique ID that denotes a particular session. A TAOS unit can pass a session ID to SNMP, RADIUS, or other external entities. See also *session, session ID base*.

session ID base—The base number for calculating a session ID. If the value of the session ID base is nonzero, the TAOS unit uses it as the initial base for calculating session IDs. The system increments the ID for each subsequent session by 1. If the session ID base is zero, the TAOS unit sets the initial base for session IDs to the absolute clock. For example, if the clock is 0x11CF4959, the subsequent session IDs uses 0x11CF4959 as a base. However, if the clock changes and the system reboots or clears NVRAM, session IDs can be duplicated. See also *session, session ID*.

session key—In RADIUS, a key that associates a client request with the user session. See also *RADIUS.*

Session layer—The third highest layer in the OSI Reference Model. The Session layer synchronizes the data in a network connection, maintains the link until the transmission is complete, handles security, and makes sure that the data arrives in the proper sequence. Gateway communications are implemented at the Session layer. See also *OSI Reference Model*.

Set Normal Response Mode—See *SNRM*.

Setup Ack timer—See *T302 timer*.

Setup message—See *ISDN Call Setup message*.

severe congestion—In Frame Relay, a condition that occurs when the queue size is greater than a predetermined threshold. In this state, the continued forwarding of amber and red frames compromises the delivery of green frames. When the link is severely congested, the following events occur:

- All incoming red frames are discarded.
- All incoming amber frames are discarded.
- The Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) bits are set.

Compare with *absolute congestion*, *mild congestion*. See also *amber frame*, *BECN*, *congestion*, *FECN*, *Frame Relay*, *red frame*.

Severely Errored Frame—On a SONET network, a defect that begins when four contiguous words are detected with an error in frame alignment, and ends when two contiguous words occur with error-free frame alignment. Compare with *Severely Errored Framing Second*, *Severely Errored Second*. See also *SONET*.

Severely Errored Framing Second—On a SONET network, a second in which one or more Severely Errored Frame defects occur. Compare with *Errored Second*, *Severely Errored Second*. See also *SONET*.

Severely Errored Second—On a SONET network, a second in which more than a certain number of coding violations or incoming errors have occurred. The number is based on the line rate and Bit Error Rate (BER). Compare with *Errored Second*, *Severely Errored Frame*, *Severely Errored Framing Second*. See also *SONET*.

SG—Signal Ground. A connection to which the system refers all electrical signals on an interface. See also *DB-25 pin connector*.

SHA1—Secure Hash Algorithm 1. SHA1 is a cryptographic algorithm that produces a 160-bit message digest. See also *hash value*, *IPSec*, *MD5*.

SHA1-HMAC—Secure Hash Algorithm 1–Keyed-Hashing for Message Authentication. SHA1-HMAC represents version 2 of the SHA1 algorithm. See also *hash value*, *IPSec*, *SHA1*.

shared secret—A password shared between a TAOS unit and a RADIUS server, or between tunnel end points in a Layer 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP) configuration. Compare with *distinct secret*. See also *L2F*, *L2TP*, *RADIUS server*.

Shielded Twisted Pair cable—See *STP cable*.

Short-Duration Transaction Network—See *SDTN*.

shortest path routing—An Open Shortest Path First (OSPF) routing algorithm that calculates the path distance to all network destinations. A cost assigned to each link determines the shortest path. See also *OSPF*.

SIG— SMDS Interest Group. SIG is a consortium of vendors and consultants committed to advancing Switched Multimegabit Data Service (SMDS) as an open solution for high-performance data connectivity. See also *SMDS*.

Signal Ground—See *SG*.

Signaling ATM Adaptation Layer—See *SAAL*.

signaling gateway—A device that initiates and manages call setup and release, and executes call routing in a Signaling System 7 (SS7) configuration. A signaling gateway uses an Access SS7 Gateway Control Protocol-Q.931+ (ASGCP-Q.931+) license, an Internet Protocol Device Control (IPDC) license, or a Q.931+ license. TCP/IP is the transport service used to carry control messages between a signaling gateway and the TAOS unit.

See also *ASGCP*, *DDL*, *IPDC*, *PSTN*, *SS7*, *SS7 network*, *TCP/IP*.

Signaling Point—See *SP*.

signaling protocol—A protocol that enables an Asynchronous Transfer Mode (ATM) system to transfer service-related information between the user and the network, and among network elements. Signaling takes place between the user and the network over the User-to-Network Interface (UNI). Signaling takes place between network elements over the Network-to-Network Interface (NNI). The signaling protocols in UNI 3.0/3.1 support five ATM service classes: Constant Bit Rate (CBR), Variable Bit Rate-Real Time (VBR-RT), Variable Bit Rate Non-Real Time (VBR-NRT), Available Bit Rate (ABR), and Unspecified Bit Rate (UBR). See also *ABR*, *ATM*, *CBR*, *NNI*, *UBR*, *UNI*, *VBR-NRT*, *VBR-RT*.

signaling protocol stack—In an Asynchronous Transfer Mode (ATM) system, a protocol stack implemented in a user's equipment and in a network peer. A signaling protocol stack consists of the following layers, in descending order, as defined by the Open Systems Interconnection (OSI) Reference Model:

Layer	Description
Layers 7-4	Call Control
Layer 3	Q.2931
Layer 2d	ATM Layer
Layer 2c	ATM Adaptation Layer (Type 5)
Layer 2b	Signaling ATM Adaptation Layer (Service Specific Connection Oriented Protocol)
Layer 2a	Signaling ATM Adaptation Layer (Service Specific Convergence Function)
Layer 1	DS3 and SONET framing

See also *ATM*.

Signaling System 7—See *SS7*.

Signaling System 7 network—See *SS7 network.*

Signaling Transfer Point—See *STP*.

signaling type—A mutually agreed-upon way to maintain synchronization and transfer data effectively between end points. The sending device and the receiving device must send signals in order to synchronize their clocks and determine where one block of data ends and the next begins. Inband signaling, ISDN D-channel signaling, and Non-Facility Associated Signaling (NFAS) are all examples of signaling types. See also *inband signaling*, *ISDN D-channel signaling*, *NFAS*.

Simple Mail Transfer Protocol—See *SMTP*.

Simple Network Management Protocol—See *SNMP*.

Simple Network Management Protocol Version 3 User-Based Security Model—See *SNMPv3 USM*.

Simple Network Time Protocol—See *SNTP*.

single-address NAT—Single-address network address translation. Single-address NAT provides a method of translating an address for hosts on the local network without borrowing IP addresses from a Dynamic Host Configuration Protocol (DHCP) server on the remote network.

For incoming calls, a TAOS unit can use its own IP address to perform NAT for multiple hosts on the local network. The TAOS unit routes incoming packets for up to 10 different TCP or UDP ports to specific servers on the local network. Translations between the local network and the Internet or remote network are static and need to be preconfigured. For outgoing calls, the TAOS unit performs NAT for multiple hosts on the local network after getting a single IP address from the remote network during PPP negotiation.

Compare with *multiple-address NAT*. See also *DHCP*, *DHCP server*, *IP address*, *NAT for LAN*.

single-stage dialing—A scenario in which a user dials the telephone number of a destination device, and an intermediary device (such as a MultiVoice gateway) automatically routes the call. Compare with *two-stage dialing*. See also *MultiVoice™*.

S interface—See *S/T interface*.

SIP—SMDS Interface Protocol. SIP is a Switched Multimegabit Data Service (SMDS) protocol that enables Customer Premises Equipment (CPE) and SMDS network equipment to interact. See also *SMDS*.

SLIP—Serial Line Internet Protocol. SLIP enables your computer to send and receive IP packets over a serial link. TAOS units do not support a direct SLIP dial-in, because SLIP does not support authentication. However, if you enable SLIP in the terminal server, a user can initiate a SLIP session, and then run an application such as File Transfer Protocol (FTP). To begin a SLIP session, the user can log in to the terminal server in terminal mode and use the SLIP command. Or, you can include the SLIP command in an expect-send script. Compare with *CSLIP*. See also *expect-send script*, *FTP*, *terminal server*.

SLIP buffer—On a fax/modem call, a buffer used for collecting IP packets before forwarding them from a TAOS unit to an analog device across the Public Switched Telephone Network (PSTN). See also *PSTN*, *SLIP*.

slot—On the backplane of a TAOS unit, the connector that provides the physical and electrical connection between a card and the TAOS unit's base resources.

slot card—A card you install on a TAOS unit to enhance its functionality.

slot compression—Compression in which the slot ID does not appear in any VJ-compressed packet except the first packet in the data stream. When you turn on VJ compression, the TAOS unit removes the TCP/IP headers, and associates a TCP/IP packet with a connection by giving it a slot ID. The first packet coming into a connection must have a slot ID, but succeeding packets need not have one. By default, the TAOS unit uses slot compression. If the packet does not have a slot ID, the TAOS unit associates it with the last-used slot ID. See also *VJ compression*.

slow poll mode—A mode in which a MultiVoice gateway attempts to register with the primary gatekeeper at 30-second intervals. See also *MultiVoice™*.

smart hub—A concentrator with network-management facilities built into the firmware. A smart hub enables you to control and plan your network configuration. Compare with *active hub*, *passive hub*. See also *concentrator*, *hub*.

SMDS—Switched Multimegabit Data Service. SMDS is a public data-switching service that provides LAN-like features and performance across wide geographic areas. As a packet-based service, SMDS enables you to create high-speed data networks with rates of up to 45Mbps. SMDS was developed by Bellcore and is offered as a service by Local Exchange Carriers (LECs) in many metropolitan areas. It uses the same fixed-size cell-relay technology as Asynchronous Transfer Mode (ATM). However, unlike ATM, SMDS is a connectionless service. See also *ATM*.

SMDS address—An address that identifies a node in a Switched Multimegabit Data Service (SMDS) configuration. An SMDS address consists of an area number and a subscriber number. See also *area number*, *SMDS*, *subscriber number*.

SMDS Interest Group—See *SIG*.

SMDS Interface Protocol—See *SIP*.

SMI—Structure of Management Information. Specifies the rules for describing management information by means of Abstract Syntax Notation One (ASN.1). The Simple Network Management Protocol Version 1 (SNMPv1) SMI is defined in RFC 1155. The SNMP v2 SMI is defined in RFC 1902. See also *ASN.1*, *SNMP*.

SMTP—Simple Mail Transfer Protocol. In the TCP/IP protocol suite, SMTP is an Application-layer protocol that uses the TCP Transport-layer protocol to send and receive electronic mail. See also *TCP/IP*.

SNAP—Subnetwork Access Protocol. SNAP is a protocol specification for the format of the Media Access Control (MAC) header of an IPX frame. SNAP includes the IEEE 802.3 protocol format with additional information in the MAC header. Compare with *802.2, 802.3, Ethernet II.* See also *IPX frame, MAC*.

SNI—Subscriber Network Interface. The SNI is the interface between the network supporting Switched Multimegabit Data Service (SMDS) and the subscriber-owned equipment. The service provider assigns SMDS addresses that identify the source and destination SNIs. Each address can be an individual address or a group address. See also *group address, individual address, SMDS, SMDS address*.

SNMP—Simple Network Management Protocol. SNMP is a standard way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent provides networking information to a manager application running on another computer. The agent can be polled by the manager, and can also use a message called a traps-PDU to send unsolicited information to the manager when an unusual event occurs. The agents and managers share a database of information, called the Management Information Base (MIB).

SNMP security uses the community name that the manager sends with each polling request and that the agent sends with each traps-PDU. Lucent Technologies supports two community names: one with read-only access and the other with read/write access to the MIB.

Three version of SNMP exist: SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2), and SNMP Version 3 (SNMPv3). Following is a brief description of each one:

- SNMPv1 is described in RFC 1157. It works as defined by the specifications of the Structure of Management Information (SMI) and operates over protocols such as User Datagram Protocol (UDP) and Internet Protocol (IP). SNMPv1 implements the protocol operations Get, GetNext, and Set.
- SNMPv2 is described in RFCs 1441 through1452. It is based on SNMPv1 and offers the additional protocol operations GetBulk and Inform.
- SNMPv3 is described in RFCs 2571 through 2575 and provides tighter security than SNMPv1 or SNMPv2.

SNMP queue—A queue containing unprocessed Simple Network Management Protocol (SNMP) requests. Compare with *backoff queue, RIP queue, UDP queue*. See also *queue*.

SNMPv3 USM—Simple Network Management Protocol Version 3 User-Based Security Model. The USM is a security method for SNMPv3 that associates security information with a user identified by a username. Any user authorized to carry out management operations at an SNMP engine must have a known username and an associated set of attributes that specify the operations the user is permitted to perform.

SNMPv3 USM provides TAOS units with the following management features:

SNMP3 USM feature	Description
Authentication	Provides data integrity and data-origin authentication. The message authentication is coded with either the Message Digest 5 (MD5) or the Secure Hash Algorithm 1 (SHA1) hash function.
Privacy	Protects messages from being copied and interpreted by unauthorized listeners on the network.
Timeliness	Protects against message delay or replay.
Discovery	Allows one SNMP engine to obtain sufficient information about a TAOS unit's SNMP engine to establish communication between an SNMP manager station and the TAOS unit.
GetBulkRequest	Added from SNMPv2 to allow the SNMPv3 manager to minimize the number of protocol exchanges required to retrieve a large amount of management information. The GetBulkRequest Protocol Data Unit (PDU) allows an SNMPv3 manager to request as large a response as possible.

See also *MD5*, *PDU*, *SHA1*, *SNMP*.

SNRM—Set Normal Response Mode. SNRM is the initial packet sent for a High-Level Data Link Control–Normal Response Mode (HDLC-NRM) call on a Short-Duration Transaction Network (SDTN). See also *HDLC-NRM*, *SDTN*.

SNTP—Simple Network Time Protocol. SNTP is a protocol that enables a group of servers to synchronize their clocks with reference to a primary time server. See also *SNTP server*, *UTC*.

SNTP server—A server that retrieves the correct time from an official source and distributes the information to other servers and networks. See also *SNTP*, *UTC*.

socket—A TCP/IP interface that facilitates a two-way link between systems, enabling applications to run over a connectionless network. A socket is defined by two addresses: the IP address of the host computer and the port address of the application or process running on the host. See also *IP address*, *port*, *TCP/IP*.

socket number—A unique value assigned to a socket in a network. See also *socket*.

Soft Permanent Virtual Circuit—See *SPVC*.

Softswitch—A software switch that provides interoperability across heterogeneous networks supporting a wide range of signaling protocols, including Signaling System 7 (SS7) and H.323. The Lucent Softswitch translates industry protocols into a generic call-signaling format, simplifying the addition of new protocols. This capability allows rich, seamless interoperability between Public Switched Telephone Network (PSTN) and IP network domains, and between multiple vendor gateways. See also *H.323*, *ICD for Softswitch*, *SS7*.

software compression—See *compression*.

software flow control—A method of flow control that uses the special characters XON and XOFF in the data stream. Compare with *hardware flow control*. See also *flow control*.

software handshaking—A synchronization method that uses the XON and XOFF characters to signal the beginning and end of a transmission. XON indicates that the device can receive data. XOFF interrupts the flow of data until an XON is sent. Compare with *hardware handshaking*. See also *handshaking*.

SONET—Synchronous Optical Network. SONET is a Bellcore specification currently used worldwide by Public Data Networks (PDNs). It defines a synchronous optical network-based User-Network Interface (UNI), either public or private, operating over single-mode optical fiber at speeds from 51.84Mbps to 9.953Gbps. See also *PDN*, *UNI*.

source address—In a frame, packet, or message sent over a bridged or routed connection, the IP, IPX, AppleTalk, or hardware address of the device that sent the transmission. Compare with *destination address*.

source auth—A feature that enables RADIUS to look up a billing code on the basis of the source IP address of a packet. When the TAOS unit places a call on behalf of a packet with the specified source address, it also sends the associated billing code to the network switch. See also *RADIUS*.

source port—The port from which a transmission originates. For example, a source port could be a User Datagram Protocol (UDP) port on an authentication server or a Simple Mail Transfer Protocol (SMTP) port on a mail server. Compare with *destination port*. See also *SMTP*, *UDP*, *UDP port*.

Source Service Access Point—See *SSAP*.

SP—Signaling Point. In Signaling System 7 (SS7), an SP is a host at which signaling messages originate and terminate. See also *SS7*.

spanning—See *call spanning*.

SPI—Security Parameter Index. The SPI is a component of an Internet Protocol Security (IPSec) Security Association (SA). IPSec uses the Authentication Header (AH) or Encapsulating Security Payload (ESP) protocol, an IP address, and the SPI to uniquely identify an SA. See also *AH*, *ESP*, *IPSec*, *SA*.

SPID—Service Profile Identifier. A SPID is a number that the telephone company uses at the Central Office (CO) switch to identify services on your ISDN line. Each SPID is derived from a telephone number. See also *CO*, *ISDN*.

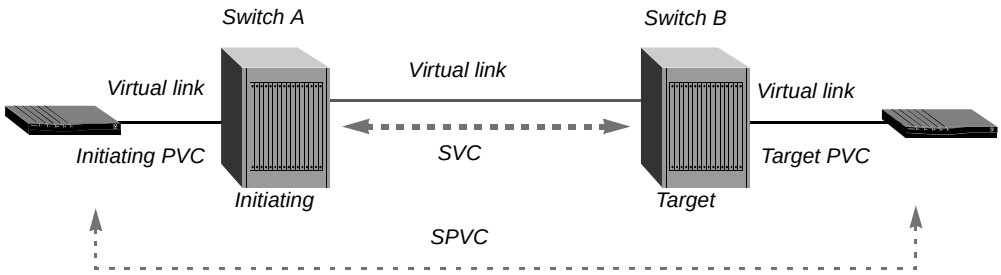
split horizon—An IPX mechanism for reducing network traffic by preventing circular routes. In the simple split-horizon scheme, a router sending updates to a neighbor omits routes that were learned from that neighbor. A split horizon with poison-reverse policy includes such routes in updates, but sets each metric to infinity. See also *IPX*, *poison reverse*.

spoofing—A procedure that enables a device to (a) mimic a legitimate network host and gain access to data within a private network, causing a security breach, (b) receive an IP address from a DHCP server across a slow WAN link, or (c) imitate a return watchdog packet for the purpose of enabling clients to remain logged in to a remote server. See also *DHCP spoofing*, *IP address spoofing*, *IPX spoofing*, *SPX spoofing*, *watchdog spoofing*.

SPVC—Soft Permanent Virtual Circuit. An Asynchronous Transfer Mode (ATM) circuit that consists of a Permanent Virtual Circuit (PVC) on a Line Interface Module (LIM) port and a Switched Virtual Circuit (SVC) on a trunk port. SPVCs allow switches to choose the best routes based on service guarantees and other metrics, and typically require configuration only on the switch that initiates the SVC. To support SPVCs, the unit must have at least a minimal Private Network-to-Network Interface (PNNI) configuration and must be PNNI-enabled.

In the configuration shown in Figure 76, Switch A initiates the signaling to set up the switch-to-switch connection, and is called the *SPVC initiator.* Switch B receives the connection setup request, and is called the *SPVC target*. TAOS units can operate in either role.

Figure 76. SPVC



The SPVC initiator is responsible for establishing, releasing, and reestablishing the SPVC. It initiates the SPVC when the virtual link at the PVC side of the ATM circuit becomes active. After computing the most efficient path to the connection destination, the SPVC initiator transmits a signaling request to the SPVC target to set up an SVC.

See also *ATM circuit*, *LIM*, *PNNI*, *PVC*, *SVC.*

SPX—Sequenced Packet Exchange. SPX is a Transport-level protocol that enables a system to perform connection-oriented packet delivery. See also *IPX*, *SPX spoofing*.

SPX spoofing—A feature that enables a WAN connection to remain idle while the application(s) requiring it are idle.

NetWare applications such as Print Server (PSERVER), Remote Printer (RPRINTER), and Remote Console (RCONSOLE), which require guaranteed packet delivery, use the NetWare SPX protocol. The client's SPX watchdog process monitors the connection with the server while the link is idle. While an SPX application is running, the SPX watchdog sends a query that reestablishes the WAN connection every 14 seconds. To enable Netware SPX clients to remain logged in without keeping the WAN connection open in times of inactivity, the TAOS unit responds to SPX watchdog requests from the LAN with a fake SPX-watchdog-reply packet, and drops any SPX-watchdog-alive packets from the LAN without sending them on to the WAN.

Compare with *DHCP spoofing*, *IP address spoofing*, *IPX spoofing*, *watchdog spoofing*. See also *SPX*.

SS7—Signaling System 7. SS7 is an internationally standardized general-purpose common-channel signaling system designed for use over a variety of digital circuit-switched networks. At the physical layer, it uses T1, T3, or E1 for data traffic and separate Time Division Multiplexing (TDM) circuits for signaling information.

TAOS units support the following methods of integration with an SS7 network. Each method requires a separate software license.

- ASGCP-Q.931+. When you use SS7 with an ASGCP-Q.931+ license, the ICD for Softswitch signaling gateway and the TAOS unit together act as a switch that routes calls intended for ISPs directly to the TAOS unit, thus avoiding the Public Switched Telephone Network (PSTN) tandem or transit switches and interoffice trunks. This method of integration enables the TAOS unit to terminate data calls in an SS7 network.
- IPDC. Internet Protocol Device Control (IPDC) is a third-party proprietary protocol. This method of integration enables a TAOS unit to terminate both voice and data calls. The signaling gateway can be ICD for Softswitch (for data only) or Lucent Softswitch (for voice or data). When you use SS7 with an IPDC license, the signaling gateway uses the IPDC protocol to convert the SS7 signaling information and call data from the PSTN into IPDC packets, which are sent to the TAOS unit. In addition, the gateway uses IPDC to convert IPDC packets received from a TAOS unit into SS7 format before sending the call to the PSTN.
- Q.931+. This International Telecommunication Union (ITU) recommendation is based on Q.931 and provides additional functions required for the SS7 signaling gateway interface. Q.931+ enables TAOS units to decrease congestion on the Public Switched Telephone Network (PSTN) caused by users connecting to the Internet. When you use a Q.931+ license, a PacketStar Connection Gateway can interact with a TAOS unit just like an ICD for Softswitch gateway using the ASGCP-Q.931+ license.

Following are the protocols supported by each signaling gateway platform:

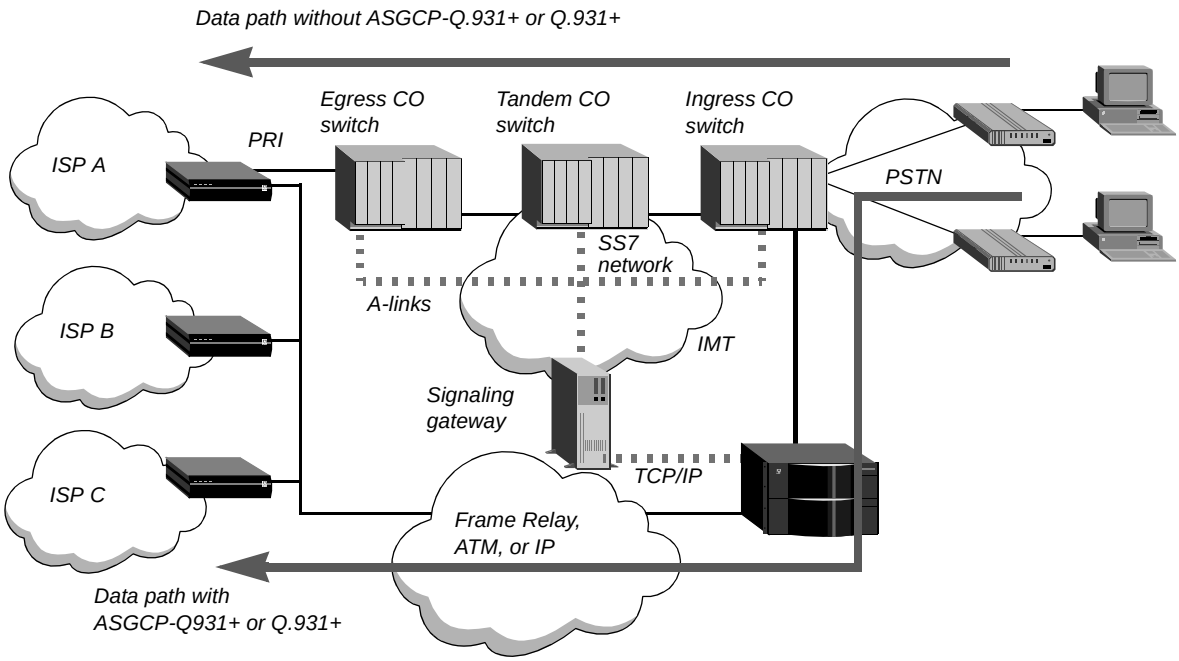
Platform	IPDC 0.15	ASGCP-Q.931+	Q.931+
ICD for Softswitch (formerly ASG)	Supported	Supported	Not supported
Lucent Softswitch	Supported	Not supported	Not supported
PacketStar Connection Gateway	Not supported	Not supported	Supported

See also *ASGCP*, *circuit switching*, *E1 line*, *IPDC*, *PSTN*, *Q.931+*, *T1 line*, *T3 line*, *TDM*.

SS7 network—Signaling System 7 network. An SS7 network uses the SS7 signaling system over a digital, circuit-switched network. When you use the Access SS7 Gateway Control Protocol-Q.931+ (ASGCP-Q.931+) or Q.931+ license, you can configure the TAOS unit to terminate data calls in an SS7 network.

Figure 77 shows an example of a TAOS unit being used for this purpose.

Figure 77. TAOS unit terminating data calls in an SS7 network

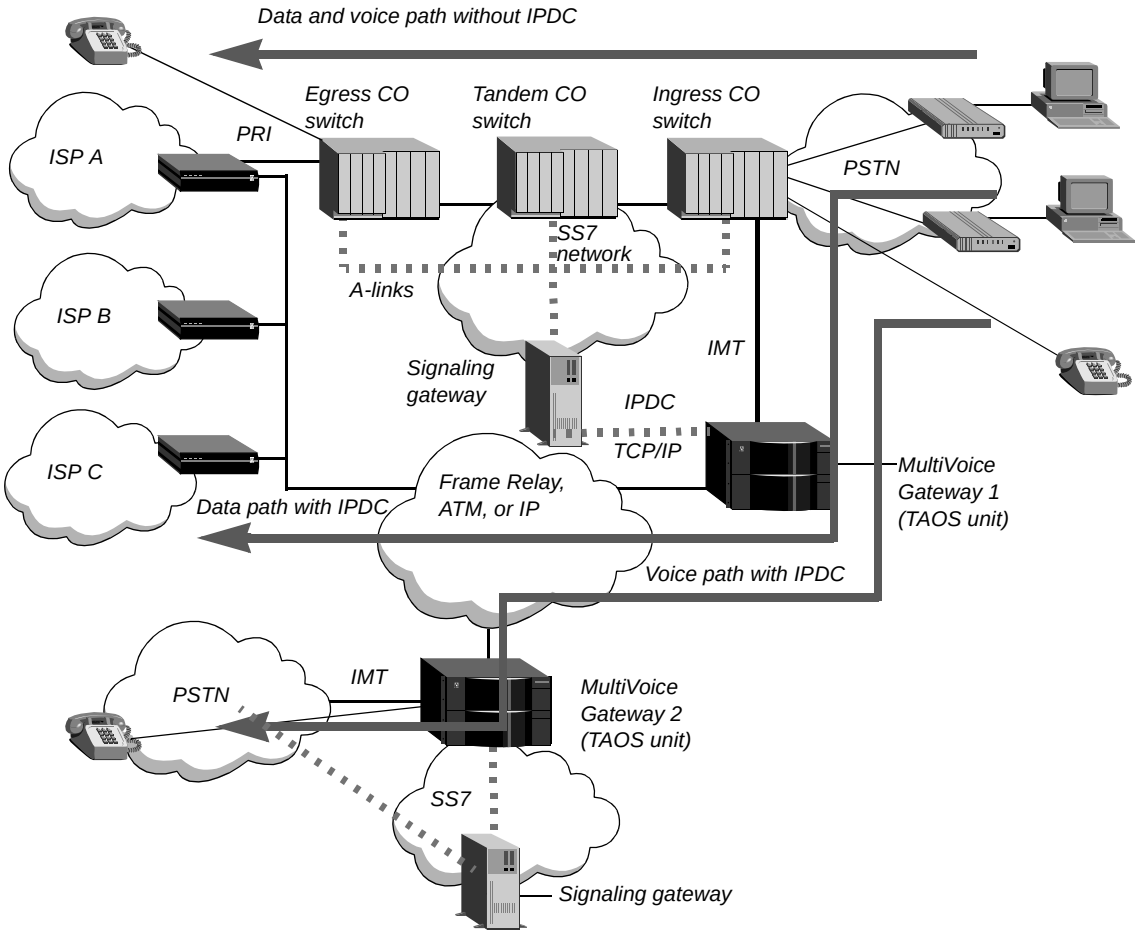


The TAOS unit is connected to the entry (ingress) Central Office (CO) switch by means of Inter-Machine Trunks (IMTs), and to a signaling gateway by means of dual-link (primary and secondary) TCP/IP links. Each CO switch is a Service Switching Point (SSP). The combination of a TAOS unit and signaling gateway is also an SSP. The signaling gateway is connected to the SS7 network by access links (A-links). The signaling gateway and the TAOS unit together act as a switch that routes calls intended for ISPs directly to the TAOS unit, thus avoiding the PSTN tandem or transit switches and interoffice trunks.

When you use the Signaling System 7 (SS7) Internet Protocol Device Control (IPDC) license, the system uses IPDC for communication between the signaling gateway and the TAOS unit. IPDC enables the TAOS unit to terminate voice or data calls.

Figure 78 shows an example of a TAOS unit being used both for Internet call diversion (data) and VoIP.

Figure 78. TAOS unit terminating voice and data calls in an SS7 network



The connection to the SS7 network is achieved through a signaling gateway. This gateway provides a bridge to the SS7 network and performs SSP functions such as initiating and managing call setup and release, and executing call routing. IPDC must be supported by both the signaling gateway and the TAOS unit.

The signaling gateway uses the IPDC protocol to convert the SS7 signaling information and call data from the PSTN into IPDC packets, which are sent to the TAOS unit. In addition, the gateway uses IPDC to convert IPDC packets received from a remote TAOS unit into SS7 format before sending the call to the PSTN. Before sending call data across the IP network, the TAOS unit uses IPDC to extract Time Division Multiplexing (TDM) and IP routing instructions from the IPDC packets received from the signaling gateway. The remote TAOS unit then forwards IPDC packets to a signaling gateway, which converts them back into SS7 messages before the call is connected.

For each type of SS7 configuration, the following events take place:

1 The ingress CO switch processes the incoming call on the basis of the called number, and then identifies the TAOS unit as the destination for the call.

2 The SS7 network sends an Initial Address Message (IAM) to the signaling gateway.

3 The signaling gateway informs the TAOS unit that a call will be coming in on one of the IMT channels from the CO switch. The message from the CO switch contains the calling and called-party number, the Circuit Identification Code (CIC), and the Destination Point Code (DPC).

4 The signaling gateway sends an Address Complete Message (ACM) to the SS7 network, acknowledging that it has received the relevant information to route the call.

5 The signaling gateway sends a call origination message to the TAOS unit to establish a path between the ingress switch and the TAOS unit.

6 The TAOS unit sets up the path and then sends an answer message to the signaling gateway so that the signaling gateway can make the proper updates to its resource management database. For a T1 or T3 network, the signaling gateway sends an answer message to the SS7 network.

7 When the path is set up, the TAOS unit accepts the call, offloading the Internet call from the PSTN to the data network. The data network used to offload the call can be a Frame Relay, Asynchronous Transfer Mode (ATM), or IP network.

See also *A-link*, *ASGCP*, *ATM*, *circuit switching*, *CIC*, *CO*, *DPC*, *Frame Relay*, *IMT*, *IPDC*, *IP network*, *signaling gateway*, *SS7*, *SSP*, *TCP/IP*, *TDM*, *VoIP*.

SSAP—Source Service Access Point. An SSAP is the Service Access Point (SAP) address at which at a Network-layer procedure requests services from the Logical Link Control (LLC) layer. See also *DSAP*, *LLC*, *SAP*.

SSP—(1) Service-Specific Part. The SSP is the portion of the Signaling ATM Adaptation Layer (SAAL) that represents the protocol and procedures associated with the signaling needs of the User-to-Network Interface (UNI). The SSP provides data recovery. Compare with *CP*. See also *SAAL*, *UNI*.

(2) Service Switching Point. A TAOS unit configured for Signaling System 7 (SS7) communication with an SS7 signaling gateway is an SSP. To operate in this capacity, the TAOS unit must have the following equipment and licenses:

- SS7 software license for Access SS7 Gateway Control Protocol-Q.931+ (ASGCP-Q.931+), Internet Protocol Device Control (IPDC), or Q.931+
- Sufficient T1, T3, or E1 trunks
- Sufficient modem or Hybrid Access cards (or both) to terminate data calls
- One or more Ethernet cards (recommended to offload the shelf controller)

If the system operates as a MultiVoice gateway in an SS7 environment, a MultiVoice software license must also be enabled and one or more MultiDSP cards must be installed to enable the system to terminate voice calls. See also *ASGCP*, *IPDC*, *MultiVoice™*, *Q.931+*, *signaling gateway*, *SS7*, *SS7 network*.

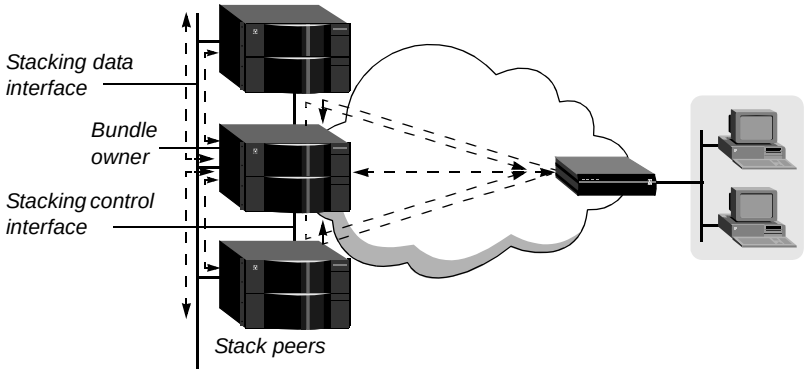
Stac compression—On a TAOS unit, a compression option that specifies a modified version of draft 0 of the Compression Control Protocol (CCP). The Stac option is a variant of the Stac LZS compression method. It was implemented before Stac LZS was standardized. Compare with *Stac LZS compression*.

Stac-9 compression—On a TAOS unit, a compression option that indicates the method specified by draft 9 of the Stac LZS compression protocol. Compare with *Stac compression*. See also *Stac LZS compression*.

stack—A group of MAX and/or MAX TNT units that act as a single logical unit with a single stack name. A stack enables incoming Multilink PPP (MP) or Multilink Protocol Plus (MP+) calls to span multiple units on a single LAN. There is no master unit in a stack. A unit can become a member of a stack or leave a stack at any time, and there is no requirement to join a stack. Units in a stack find each other by means of an Ethernet multicast packet. Because multicast packets are unlikely to cross a router, all members of a stack must reside on the same physical LAN.

The initial bandwidth of a connection is established when user equipment dials in to one of the stacked units. After the link has been authenticated, if more bandwidth is requested, the system that dialed the initial link can dial another link to add bandwidth. When stacking is enabled, the new link can be handled by any one of the stack peers. In Figure 79, the calling MAX unit dials three links, each of which is answered by a different stacked unit.

Figure 79. Stacked bundle consisting of three links

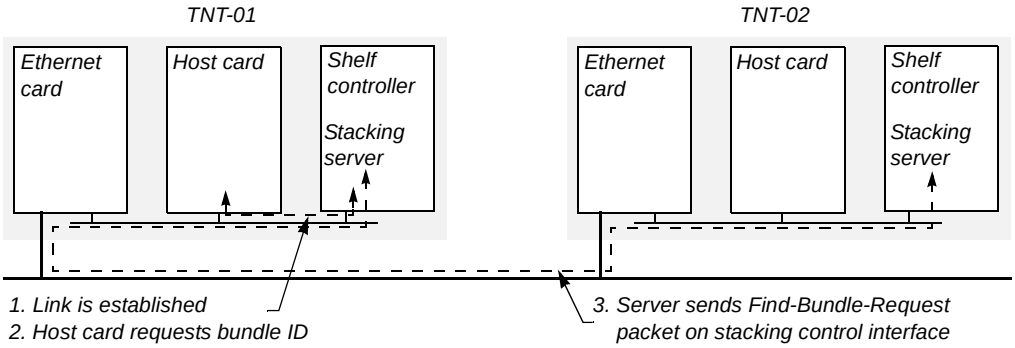


The stacked unit that establishes the initial link is the *bundle owner*. The bundle owner manages the connection's traffic across the stack. Stack peers forward incoming traffic from the WAN to the bundle owner, and the bundle owner receives outgoing traffic destined for the remote end and distributes it to bundled links. To balance the load among all available WAN channels, outgoing data packets are assigned to bundled links on a rotating basis. The stacking control interface and stacking data interface can use the same Ethernet segment, but most sites use separate segments for performance and management reasons.

If the stacking software on the shelf controller cannot determine where a bundle for the link resides (or if no bundle exists yet), it multicasts a Find-Bundle-Request packet on the Ethernet interface specified for stacking control packets. If the requesting server receives a reply that includes a bundle ID, it adds the new link to that bundle. Otherwise, it assigns a bundle ID and becomes the bundle owner. At this point, the authentication acknowledgment is sent to the caller.

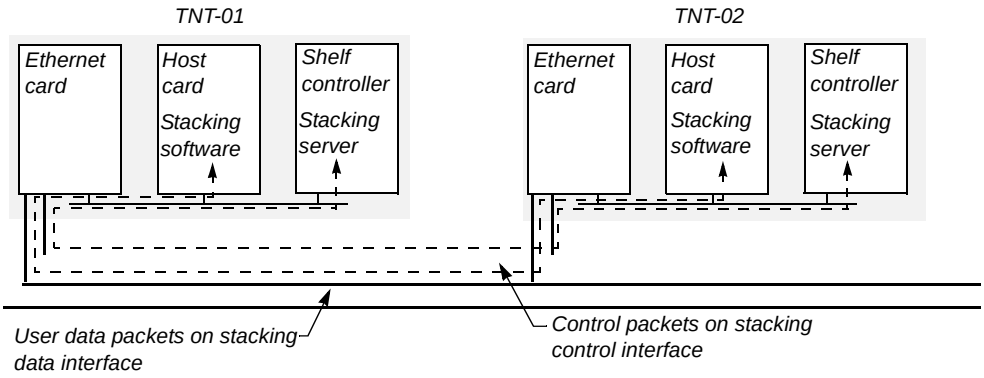
Figure 80 identifies the steps taken by the peer named TNT-01 to establish a bundle for an MP or MP+ link.

Figure 80. Stacking control messages to establish a bundle



When a bundle has been established, stacking software on the host cards exchanges stacking data packets (user data) and keepalive packets (zero-length data packets). Figure 81 shows data and control packets being exchanged for a stacked session.

Figure 81. Stacking data and control packets



Depending on how the system address is set in the peers, unicast control packets can also be received on the stacking data interface.

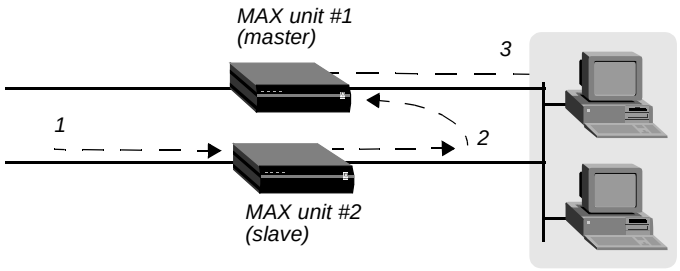
For a stack to include both MAX and MAX TNT units, the MAX units must support Stacking Protocol Version 3. Some network constraints apply when you are stacking MAX and MAX TNT units together. TAOS does not support token card authentication of stacked bundles.

See also *MP, MP+, multicast, stacked channels.*

stacked channels—In a stacked configuration of TAOS units, channels carrying outgoing data that was transferred from the bundle owner or incoming data that gets transferred to the bundle owner.

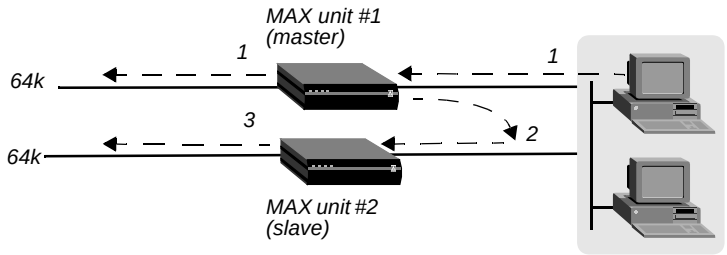
For example, assume the initial call of an MP or MP+ bundle connects to MAX unit #1. This connection is a *real* channel. (In a stacked configuration, real channels connect directly to the TAOS unit that owns the bundle.) MAX unit #1 is the bundle owner, and it manages the traffic for both channels of the bundle. As shown in Figure 82, the second call of the bundle connects to MAX unit #2. This connection is a *stacked* channel. MAX unit #2 forwards any traffic from the WAN to MAX unit #1, for transmission to the destination.

Figure 82. Packet flow from the slave channel to the Ethernet network



Likewise, as shown in Figure 83, MAX unit #1 receives all Ethernet traffic destined for the bundle, and disperses the packets between itself and MAX unit #2.

Figure 83. Packet flow from the Ethernet network



MAX unit #1 forwards some of the packets across the WAN through a real channel. MAX unit #2 sends the rest of them through a stacked channel. See also *bundle*, *bundle owner*, *stack*.

Stac Lempel-Ziv standard compression—See *Stac LZS compression*.

Stac LZS compression—Stac Lempel-Ziv standard compression. Developed by Stac Incorporated, Stac LZS compression can triple data rates. Compare with *Stac compression*. See also *Stac-9 compression*.

standby trunk—A redundant trunk that becomes active and takes over traffic handling if an active trunk becomes unavailable.

start bit—In asynchronous transmission, a bit that indicates the beginning of a new character. It is always 0 (zero). Compare with *stop bit*. See also *asynchronous transmission*.

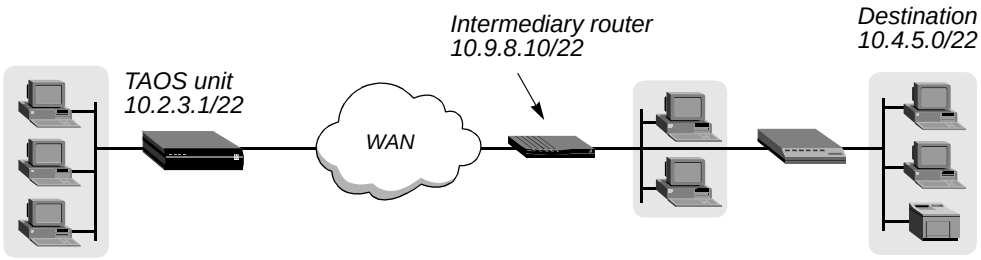
Start Control Connection Request—See *SCCRQ*.

Start record—A RADIUS-accounting or call-logging record that contains information about the beginning of a session with a TAOS unit. See also *Start session.*

Start session—An event denoting the beginning of a session with a TAOS unit. Information about a Start session event appears in a RADIUS-accounting or call-logging Start record.

static IP route—A path that specifies a destination IP network and the next-hop router to that network. If a profile specifies the destination address of a host on a remote subnet, but the packets must be routed through an intermediary device to reach that host, and RIP or OSPF is not enabled, you must configure a static route specifying the intermediary device as the next-hop router. Figure 84 shows an example.

Figure 84. Static route to a remote subnet



Compare with *dynamic route*, *multipath route*. See also *IP address, IP network, private static route, pseudo-user profile, user profile*.

static IPX route—A route that contains all the information necessary to reach one IPX server on a remote network. A TAOS unit adds its configured static routes to its routing table upon initialization. When the unit receives an outgoing packet for a server, it finds the corresponding profile and dials the connection. You must manually update static routes whenever the administrator at the remote end removes the specified server or updates its address. You do not need to create IPX routes to servers that reside on the local Ethernet network. See also *IPX server, pseudo-user profile.*

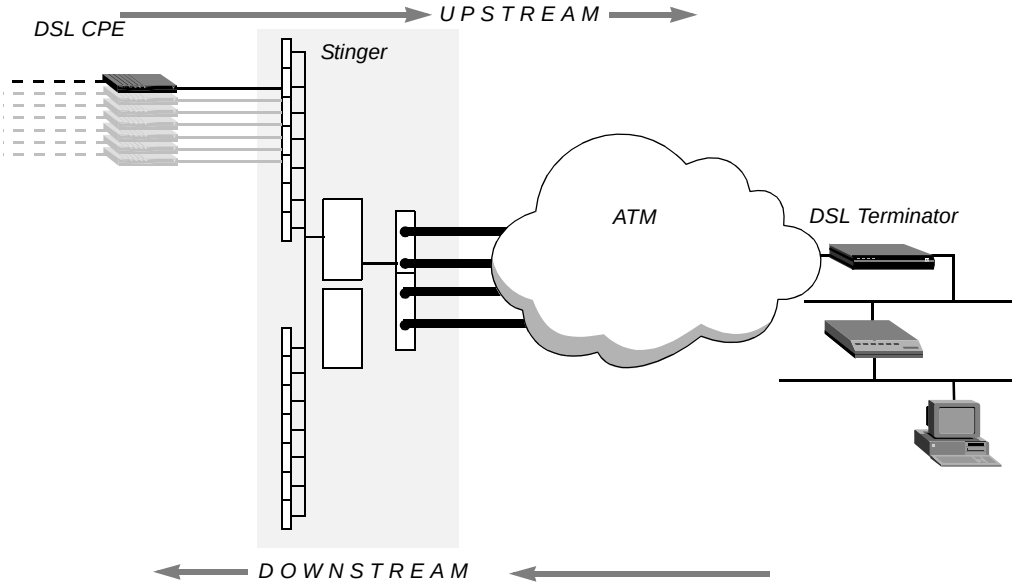
static password—A password specified in a profile. The user must enter the password to gain access to the TAOS unit. See also *user profile*.

static route—See *private static route, static IP route, static IPX route*.

station—See *host.*

Stinger™—An Asynchronous Transfer Mode (ATM) switch-through Digital Subscriber Line Access Multiplexer (DSLAM). A Stinger unit switches data from multiple ATM DSL subscribers onto a high-speed ATM backbone. Figure 85 shows an example of DSLAM operations.

Figure 85. Stinger configuration



Data transmitted from the CPE to the Stinger unit is *upstream traffic.* Data transmitted from the Stinger unit to the CPE is *downstream traffic*. *See also ATM, CPE, DSLAM*.

S/T interface—(noun) The electrical interface between a network termination type 1 (NT1) device and one or more ISDN communications devices without their own NT1 functionality. *(*adjective) Describes an ISDN communications device that connects to a network termination type 1 (NT1) device. See also *NT1*.

STM—Synchronous Transport Module. Specifies standards for electrical and optical transmission over Synchronous Digital Hierarchy (SDH) lines. See also *SDH*.

STN message—Send Tones message. A call-progress message sent by a Signaling System 7 (SS7) gateway to a TAOS unit. An STN message specifies that certain call-progress tones or voice announcements are played for callers during a Voice over IP (VoIP) call. Compare with *ASTN message*. See also *signaling gateway, SS7, VoIP*.

stop bit—In asynchronous transmission, a bit that marks the end of the character. It appears after the parity bit, if one is in use. Compare with *start bit*. See also *asynchronous transmission*.

Stop record—A RADIUS-accounting or call-logging record that contains information about the end of a session with a TAOS unit. See also *accounting, call logging, Stop session.*

Stop session—An event denoting the end of a session with a TAOS unit. Information about the Stop session event appears in a RADIUS-accounting or call-logging Stop record. See also *accounting, call logging.*

store-and-forward fax—See *IP fax*.

STP—Signaling Transfer Point. In Signaling System 7 (SS7), an STP is a packet switch that performs message routing between adjacent Signaling Points (SPs). See also *SP*, *SS7*.

STP cable—Shielded Twisted Pair cable. STP cable consists of at least two pairs of wires twisted two or more times per inch to help cancel out noise. The entire cable has a protective covering. STP cable is typically used in ARCnet and Token Ring networks. See also *ARCnet*, *Token Ring*.

straight-through cable—A cable whose terminating ends both have the same wire assignments. Compare with *crossover cable*.

Structure of Management Information—See *SMI*.

stub area—An Open Shortest Path First (OSPF) area in which all external routes are summarized by a default route. OSPF supports stub areas to reduce the cost of routing. A stub area allows no Type-5 LSAs to be propagated in the area. Instead, it depends on default routing to external destinations. Compare with *normal area*, *NSSA*. See also *area*, *ASE Type-5*, *LSA*, *Open Shortest Path First*.

subaddress—A number used for routing incoming calls to the appropriate destination on the TAOS unit.

subnet—See *IP subnet*.

subnet mask—An IP feature in which a group of bits identifies a subnet. To specify a subnet mask, a TAOS unit appends to the IP address a modifier that specifies the total number of network bits in the address.

For example, in the address 200.5.248.40/29, the /29 specification indicates that 29 bits of the address specify the network. The 3 remaining bits specify unique hosts. With 3 bits used to specify hosts on a 29-bit subnet, eight different bit-combinations are possible:

000—Reserved for the network (base address)
001
010
100
110
101
011
111—Reserved for the broadcast address of the subnet

Following are the standard and TAOS subnet formats for a class C network number:

Subnet mask	Number of host addresses	TAOS notation
255.255.255.0	254 hosts + 1 broadcast, 1 network base	/24
255.255.255.128	126 hosts + 1 broadcast, 1 network base	/25
255.255.255.192	62 hosts + 1 broadcast, 1 network base	/26
255.255.255.224	30 hosts + 1 broadcast, 1 network base	/27
255.255.255.240	14 hosts + 1 broadcast, 1 network base	/28
255.255.255.248	6 hosts + 1 broadcast, 1 network base	/29
255.255.255.252	2 hosts + 1 broadcast, 1 network base	/30
255.255.255.254	Invalid subnet mask (no hosts)	/31
255.255.255.255	1 host (a host route)	/32

The broadcast address of any subnet has the host portion of the IP address set to all ones. The network address (or base address) represents the network itself, because the host portion of the IP address is all zeros. For example, suppose that a TAOS unit's configuration assigns the following address to a remote router:

`200.5.248.120/29`

The Ethernet network attached to that router has the following address range:

`200.5.248.120` through `200.5.248.127`

A host route is a special-case IP address with a subnet mask of /32. For example:

`200.5.248.40/32`

Host routes are required for a dial-in host.

See also *host number*, *host route*, *IP*, *IP address*, *IP subnet*, *IP network number*.

SubNetwork Access Protocol—See *SNAP*.

Subscriber Network Interface—See *SNI*.

subscriber number—The last four digits of a Switched Multimegabit Data Service (SMDS) address. Compare with *area number*. See also *SMDS*.

subtending—A method of aggregation in which multiple Stinger chassis are served by a single network trunk port. Subtending reduces the number of trunks needed. See also *Stinger™*.

summarization—The process of combining routing information from one routing protocol into another for advertisement.

summary address—A single reachable address prefix that represents all end systems and nodes whose Asynchronous Transfer Mode (ATM) addresses share that prefix. A summary address serves as an abbreviation of the entire set of addresses. Private Network-to-Network Interface (PNNI) nodes use address summarization to reduce the amount of address information maintained and propagated throughout the network. A summary address can be advertised to indicate that the node can reach all the represented end systems and nodes. Or, to avoid advertising addresses that match the prefix, regardless of scope, you can suppress the summary address. The TAOS unit maintains separate sets of summary addresses and suppressed summary addresses for internal and exterior reachable addresses. See also *ATM*, *PNNI*, *reachable address*, *reachable address prefix*.

SuperDigital 128—A dedicated service available only in Japan. Subscribers receive two ISDN B channels combined into a single 128Kbps pipe.

superuser—In UNIX, a user with special privileges (also known as *root*). Only the superuser, for example, can change the password file and edit major system administration files in the `/etc` directory.

supervisory frame—On an X.25 network, a frame that can request and suspend transmission, report on link status, and acknowledge I-frames. Compare with *general frame*, *I-frame*. See also *X.25*.

Sustainable Cell Rate—See *SCR*.

SVC—Switched Virtual Circuit. An SVC is a link established by means of signaling over a packet-switched network. It appears to be a dedicated circuit, but the connection remains active only as long as needed. Compare with *PVC*. See also *Frame Relay SVC*, *packet-switched network*.

SVCC—Switched Virtual Channel Connection. An Asynchronous Transfer Mode (ATM) Virtual Channel Connection (VCC) established and dismantled dynamically by means of control signaling. See also *ATM*, *VCC*.

SWIPE—IP with Encryption. SWIPE is a Network-layer security protocol that works by adding a cryptographic authenticator to each packet and encrypting the data.

switch—A device that connects the calling party to the answering party.

Switched-56—A data service providing a single 56Kbps channel. The Switched-56 data service is available over any type of line. Because Switched-56 was the first available data service, both the service itself and the lines that used it were called Switched-56. However, any type of line can now access Switched-56 data service.

Switched-56 line—A line that provides a single 56Kbps data channel with inband signaling. See also *inband signaling*.

Switched-64—A data service providing a single 64Kbps channel. The Switched-64 data service is available over T1 PRI and ISDN BRI lines only. See also *ISDN BRI line*, *T1 PRI line*.

Switched-384—A data service consisting of a single 384Kbps circuit, called an *H0 channel*. The H0 channel is comprised of six B channels. The Switched-384 data service is available over T1 PRI lines only. Switched-384 is also known as the *H0 data service*. See also *B channel, T1 PRI line.*

Switched-1536—A data service consisting of a single 1536Kbps circuit, called an *H11 channel*. The H11 channel occupies all 24 channels on the line. You must use two T1 PRI lines to access Switched-1536. One line carries the user data, and the other line contains the D channel. Non-Facility Associated Signaling (NFAS) is required for the Switched-1536 data service because the D channel must be on a separate line. The Switched-1536 data service is available over T1 PRI lines only. Switched-1536 is also known as the *H11 data service*. See also *D channel, NFAS, T1 PRI line.*

switched channel—A channel that provides a temporary connection for the exchange of data. The channel is cleared when the call ends. Compare with *dedicated channel.*

switched circuit—A temporary connection between end points, established for the duration of a call, over which two parties exchange data. The circuit is disconnected when the call ends. Compare with *dedicated circuit.*

switched line—A line consisting of channels in use only for the duration of the connection. Compare with *dedicated line*.

Switched Multimegabit Data Service—See *SMDS.*

Switched Nx64—See *MultiRate*.

switched Permanent Virtual Circuit—See *switched PVC.*

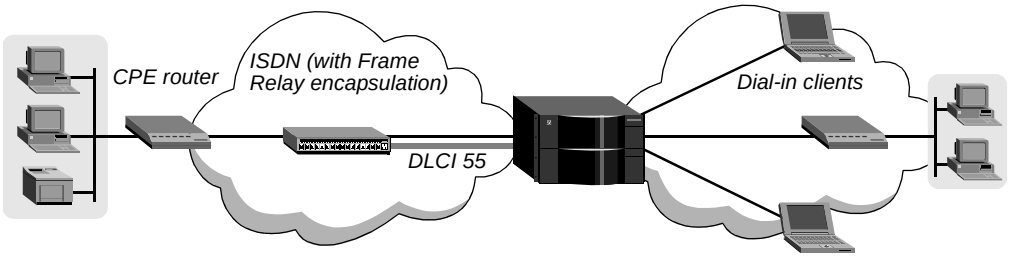
switched PVC—Switched Permanent Virtual Circuit. A switched PVC is a PVC that runs over a switched ISDN connection. A switched PVC is established in the same way as a dedicated PVC: on the basis of an exchange of LMI frames and the occurrence of a number of events. However, instead of using dedicated bandwidth, a switched PVC uses an ISDN B channel that is activated by an outgoing or incoming call. Switched PVCs can use channels on any slot card that works with the Hybrid Access cards.

To establish a switched PVC by placing an outgoing call, a TAOS unit initiates the call in the usual way. When the call has been placed and the B channel is available, the system begins exchanging LMI frames to establish Frame Relay link operations, a process that can take several seconds. Once the link is up, it works just like a PVC with an access rate of 64Kbps or 56Kbps, depending on the ISDN configuration.

To establish a switched PVC by accepting an incoming call, Calling-Line ID (CLID) or Dialed Number Information Service (DNIS) authentication is required. Either of these authentication methods enables the TAOS unit to begin using Frame Relay encapsulation before accepting the call. When the connection has been accepted, the TAOS unit follows the same procedure as for outgoing calls.

Figure 86 shows PPP clients dialing in to a TAOS unit to reach a Customer Premises Equipment (CPE) router that is accessible across Frame Relay.

Figure 86. Switched PVC to a Frame Relay switch



Compare with *PVC*, *SVC*. See also *CLID authentication*, *DNIS*, *Frame Relay*.

Switched Virtual Channel Connection—See *SVCC*.

Switched Virtual Circuit—See *SVC*.

symbolic name—A name that denotes an IP address. A symbolic name consists of a username and a domain name in the format *`username@domain_name`*. The domain name can take the format *`host_name.network_name.identifier`* (as in `tuv.xyz.edu`) or *`network_name.identifier`* (as in `abc.com`). The *`host_name`* portion corresponds to the host number of an IP address. The *`network_name`* portion corresponds to the network number of an IP address. The *`identifier`* portion is the domain identifier, and indicates the type of organization to which the host belongs. A symbolic name might be `joanne@abc.xyz.com` or `steve@wxy.edu`. See also *IP address*.

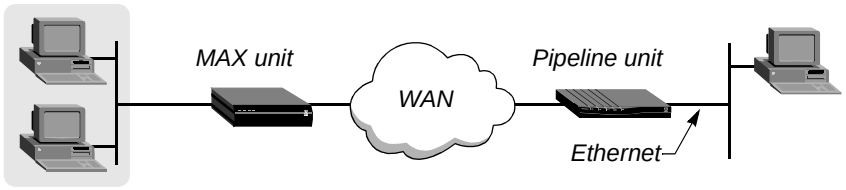
synchronization—A method of ensuring that the receiving end can recognize characters in the order in which the transmitting end sent them, and can know where one character ends and the next begins. Without synchronization, the receiving end would perceive data simply as a series of binary digits with no relation to one another.

Synchronous Digital Hierarchy—See *SDH*.

Synchronous Optical Network—See *SONET*.

synchronous PPP—A PPP connection that uses synchronous transmission. In Figure 87, a synchronous PPP session takes place between a Pipeline unit and a MAX unit.

Figure 87. Synchronous PPP connection



Synchronous PPP is also known as *sync PPP*. Compare with *asynchronous PPP*. See also *PPP*, *synchronous transmission*.

synchronous transmission—A transmission mode in which the data moves in large blocks, called messages or frames. A synchronous WAN link uses High-level Data Link Control (HDLC) encoding and connects to a router for a network-to-network link. Each synchronous call uses Point-to-Point Protocol (PPP), Multilink PPP (MP), Multilink Protocol Plus (MP+), or Frame Relay encapsulation.

In a synchronous transmission, both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins. Each side can transmit a separate synchronizing signal (called a clock), or each frame can contain its own synchronization information. In the latter method, each block of data starts with one or more control characters, usually eight bytes long, called a SYNC. The receiver interprets the SYNC as a signal that it can start accepting data.

Synchronous transmission can be up to 20 percent faster than asynchronous transmission. See also *Frame Relay*, *HDLC*, *MP*, *MP+*, *PPP*, *synchronization*.

Synchronous Transport Module—See *STM*.

sync PPP—See *synchronous PPP*.

SYN-to-SYN timer—In an X.25/T3POS configuration, a value that applies to opening frames in Local or Binary Local mode. Normally, in order to indicate that an idle link is still connected, the PAD sends SYN signals to the Data Terminal Equipment (DTE) at the interval specified by the SYN-to-SYN timer. However, if the DTE sends a SYN signal to the PAD before the PAD sends one to the DTE, the SYN-to-SYN timer specifies the period of time the PAD expects SYN signals from the DTE. If the PAD does not receive two SYN signals within the interval specified by the SYN-to-SYN timer, it tries to restore the link.

The SYN-to-SYN timer is also known as the T2 timer. See also *Binary Local mode*, *Local mode*, *X.25/T3POS*.

Syslog—A facility that sends system status messages to a host computer, known as the *Syslog host*. The Syslog host saves the system status messages in a Syslog file. For detailed information about the `syslog` daemon, see the UNIX man pages on `logger(1)`, `syslog(3)`, `syslog.conf(5)`, and `syslogd(8)`. The Syslog function requires User Datagram Protocol (UDP) port 514.

Syslog host—The station to which a TAOS unit sends system logs.

Syslog message—A message that is written to a `syslog` file on the Syslog host.

Syslog stream—The stream of records sent by a unit to a Syslog server.

system-based routing—A form of IP routing in which the entire unit has a single IP address. For systems that have a single backbone connection, system-based routing is the simplest way to configure a TAOS unit. Compare with *interface-based routing*.

T

T1 channel—One of 24 channels on a T1 line. See also *channelized T1 PRI/E1 PRI*, *fractional T1 line*, *T1 line*, *T1 PRI line*, *unchannelized T1 PRI/E1 PRI*.

T1 line—A line that supports 24 64Kbps channels, each of which can transmit and receive data or digitized voice. The line uses framing and signaling to achieve synchronous and reliable transmission. The most common configurations for T1 lines are ISDN Primary Rate Interface (T1 PRI) and unchannelized T1, including fractional T1. See also *channelized T1 PRI/E1 PRI*, *fractional T1 line*, *T1 channel*, *T1 PRI line*, *unchannelized T1 PRI/E1 PRI*.

T1 PRI line—T1 Primary Rate Interface line. A T1 PRI line has a total bandwidth of 1.544Mbps. It uses 23 B channels for user data, and one 64Kbps D channel for ISDN D-channel signaling. The B channels can be all switched, all dedicated, or a combination of switched and dedicated. The T1 PRI line is a standard in North America, Japan, and Korea. You can connect a T1 PRI line to standard voice, Switched-56, Switched-64, Switched-384, Switched-1536, and MultiRate data services. Compare with *E1 PRI line*, *ISDN BRI line*. See also *B channel*, *channelized T1 PRI/E1 PRI*, *D channel*, *dedicated channel*, *MultiRate*, *Switched-56*, *Switched-64*, *Switched-384*, *Switched-1536*, *T1 channel*, *T1 line*, *unchannelized T1 PRI/E1 PRI*.

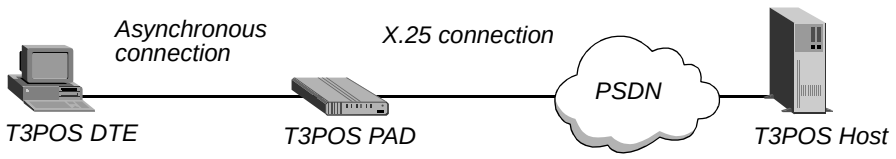
T1 Primary Rate Interface line—See *T1 PRI line*.

T1 retransmission timer—In an X.75 configuration, a value that specifies the maximum amount of time in ticks the transmitter should wait for an acknowledgment before initiating a recovery procedure. See also *X.75*.

T3 line—A digital transmission link consisting of 28 T1 lines with a total bandwidth of 44.736Mbps. See also *DS3 line*, *T1 line*.

T3POS—Transaction Processing Protocol for Point-of-Service. T3POS is a character-oriented, frame-formatted protocol designed for Point-of-Service (POS) transactions through an X.25-based packet-switched network. T3POS enables you to send data over the ISDN D channel while continuing to send traffic over both B channels. The T3POS protocol involves three parties: the T3POS DTE, the T3POS PAD, and the T3POS Host. Figure 88 shows a T3POS setup.

Figure 88. T3POS setup



A typical use of T3POS is to perform credit-card authorization over the D channel while using the B channels to transmit inventory-control data and other traffic. See also *X.25*.

T3 timer—See *ENQ handling timer*.

T4 timer—See *Response timer*.

T5 timer—See *DLE, EOT timer*.

T.38—An International Telecommunications Union (ITU) standard for real-time fax over IP. The T.38 standard makes it possible for fax devices from different vendors to communicate with one another over Internet Protocol (IP) networks. See also *IP network*, *real-time fax over IP*.

T302 timer—A value that specifies the number of milliseconds the system waits for additional called-number information for an incoming call on a T1 PRI or E1 PRI line. The TAOS unit begins collecting the trailing-digit information, and for each Setup message from the switch that does *not* include `Sending Complete Information Element`, the unit starts the T302 timer. The unit stops the timer when it receives a message that includes `Sending Complete Information Element`. The unit assumes there are no more trailing digits to collect when the T302 timer stops or expires. The T302 timer is also called the *Setup Ack timer.* See also *E1 PRI line, T1 PRI line*.

T303 timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum number of milliseconds that a TAOS unit waits for a response after a Setup message is sent. The timer is stopped when a Connect, Call Proceeding, or Release Complete message is received. See also *ATM*.

T308 timer—See *release indication timer*.

T309 timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum number of milliseconds that a TAOS unit waits for the Q.SAAL layer to reconnect. After the timer expires, calls are dropped. See also *ATM*.

T310 timer—See *call proceeding timer*.

T313 timer—See *connect request timer*.

T316 timer—See *restart request timer*.

T322 timer—In an Asynchronous Transfer Mode (ATM) configuration, a value that specifies the maximum number of milliseconds that a TAOS unit can wait for a response after a Status Enquiry message is sent. See also *ATM*.

TA—Terminal Adapter. A TA is a protocol converter that adapts non-ISDN equipment (such as a telephone, fax, or modem), and enables it to work over an ISDN connection. A TA has two functions. First, it must change the format of transmitted data to match the V.120 standard for asynchronous transfer over a B channel. Second, it must provide a way of setting up and clearing calls, usually by means of Hayes AT commands. A TA is to an ISDN line what a modem is to an analog telephone line. However, some of the D-channel information does not pass through the TA, so non-ISDN equipment cannot take full advantage of ISDN facilities, such as Calling-Line ID (CLID). See also *AT command set*, *CLID*, *ISDN*, *V.120*.

TACACS—Terminal Access Concentrator Access Control Server. TACACS is a very simple query-and-response protocol that enables a TAOS unit to check a user's password in order to grant or prevent access. A TACACS server supports only the basic password exchanges that Password Authentication Protocol (PAP) uses. It does not support Challenge Handshake Authentication Protocol (CHAP). See also *CHAP*, *PAP*.

TACACS+—Terminal Access Concentrator Access Control Server Plus. TACACS+ is a proprietary Cisco enhancement to the Terminal Access Concentrator Access Control Server (TACACS) protocol. TACACS+ handles the transfer of authentication and authorization information between a Network Access Server (NAS) and an authentication server, encrypting password information and forwarding it over the network. TACACS+ supports AppleTalk Remote Access (ARA), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), and Telnet. In addition, TACACS+ uses the Transmission Control Protocol (TCP) to transmit accounting information to an accounting server. See also *CHAP*, *NAS*, *PAP*, *PPP*, *SLIP*, *TCP*, *Telnet.*

TACP—Transmit ATM Cell Processor. A TACP is a processor that delineates transmitted Asynchronous Transfer Mode (ATM) cells; filters transmitted cells on the basis of their idle status, unassigned status, or associated Header Check Sequence (HCS) errors; and descrambles the transmit cell payload. Compare with *RACP*. See also *ATM*, *HCS*.

tag—(1) In an Open Shortest Path First (OSPF) configuration, a method of flagging a route as external—that is, as having been imported into the OSPF database from outside the router's Autonomous System (AS).

(2) In a tunneling configuration, a number identifying a RADIUS attribute set for transparent tunneling to dial-in networks. A tag is a number from 1 through 31 that you can add to one or more RADIUS attributes that support transparent tunneling. Attributes that share the same tag number form an attribute set. The user's profile includes a primary attribute set, which specifies all of the values required to set up the tunnel, and additional attribute sets that can be used to establish a tunnel if the primary server is unavailable.

The number of attribute sets used is limited for some protocols, as follows:

Tunnel protocol	Attribute sets used
Layer 2 Tunneling Protocol (L2TP)	All specified attribute sets are used.
Layer 2 Forwarding (L2F)	All specified attribute sets are used.
Point-to-Point Tunneling Protocol (PPTP)	Only the attribute set with the highest priority is used. Priority is defined by the Tunnel-Preference value or by tag order.
Ascend Tunnel Management Protocol (ATMP)	Only the two sets with the highest priority are used. (From the second attribute set, only the Tunnel-Server-Endpoint value is used. Other values can be omitted.) Priority is determined by the Tunnel-Preference value or by tag order.

Consider the following:

- Attribute sets in the same user profile are processed in numeric order (the set with tag 1 is processed before the set with tag 2, and so forth), unless the sets are reordered by means of the Tunnel-Preference attribute.
- A tag value of 0 (zero) is considered untagged. Untagged attribute sets are processed before tagged attribute sets, unless a Tunnel-Preference setting specifies otherwise.
- A user profile can specify up to 32 tunnel attribute sets. However, because the system waits a certain interval before each attempt to initiate a tunnel, and retries a certain number of times, the client's PPP connection typically times out before 32 tunnel attempts are made.
- All the attribute sets in a profile must specify similar tunnel protocols—all Layer 3 tunnels (such as ATMP) or all Layer 2 tunnels (such as L2TP or L2F). You can mix L2TP with L2F, but not with ATMP.

See also *AS*, *ATMP*, *external route*, *L2F*, *L2TP*, *OSPF*, *PPTP*, *RADIUS*.

tagging—In an Asynchronous Transfer Mode (ATM) configuration, a method of identifying a high-priority cell (CLP=0) as a low-priority cell (CLP=1), as opposed to simply dropping the cells from the cell stream when the high-priority cell stream is nonconforming. In a tunneling configuration, a method of identifying a RADIUS attribute set for transparent tunneling to dial-in networks. See also *ATM*, *CLP*, *tag*, *tunneling*.

TAOS—True Access™ Operating System. TAOS is a comprehensive software architecture for WAN access. It consists of two main components: the standard TAOS kernel and optional TAOS extensions.

The TAOS kernel supports IP routing, modem management, terminal-server functionality, authentication, authorization, accounting, WAN protocols, and bandwidth management. TAOS extensions enable service providers and corporations to further customize and enhance their WAN access services. The extensions include the following:

- Global Digital Access for ISDN and Frame Relay environments, including support for ISDN clients, Frame Relay concentration, and ISDN signaling.
- IntragyCentral, the embedded WAN access switch component of Intragy enterprise access software suite. IntragyCentral provides multiprotocol routing, multiprotocol dial access, transparent bridging, and modem pooling for LAN-based outgoing dial and fax.
- Tunneling support for Virtual Private Networks (VPNs).
- Quality of Service (QoS) solutions, including videoconferencing support.
- NavisAccess.

See also *authentication*, *authorization*, *Frame Relay*, *Intragy*™, *IP address*, *IP routing*, *QoS*, *terminal server*, *VPN*.

tariff—A document filed by a regulated telephone company with a state public utility commission or the Federal Communications Commission. A tariff details services, equipment, and pricing publicly offered by the telephone company.

Tc—Committed Rate Measurement Interval, the time interval during which the user can send only a Committed Burst (Bc) amount of data and an Excess Burst (Be) amount of data. Incoming data causes the system to begin the timer, and data flow ends when the time interval is over. As data is received over time interval Tc, a determination is made as to whether the frame is

- Under the value for Bc
- Over the Bc value, but under the Be value
- Over the Be value

In general, the duration of Tc is proportional to the burstiness of the traffic. Tc is computed from the Committed Information Rate (CIR) value and Bc as Tc=Bc/CIR. See also *Bc*, *Be*, *CIR*.

T-carrier circuit—A T1 or T3 circuit. A T1 circuit transmits voice and data at speeds of up to 1.544Mbps over 24 channels of 56Kbps each. A T3 circuit is equivalent to 28 T1 circuits, or 672 channels, and provides a total bandwidth of 44.736Mbps. Compare with *E-carrier circuit*. See also *T1 line*, *T3 line*.

TCP—Transmission Control Protocol. TCP operates at the Transport layer, providing connected-oriented services. It uses IP to deliver packets. See also *IP*, *TCP/IP*.

TCP-Clear—See *Raw TCP*.

TCP/IP—Transmission Control Protocol/Internet Protocol. TCP/IP is a family of protocols that defines the format of data packets sent across a network, and it is the communications standard for data transmission between different platforms. The TCP/IP family consists of the following protocols and services:

OSI layer	Protocol name	Description of service
Application	Boot Protocol (BOOTP) File Transfer Protocol (FTP) Telnet	User services that provide applications a computer can use
	Network File System (NFS) Network Information Service (NIS) Remote Procedure Call (RPC) Simple Mail Transfer Protocol (SMTP) Simple Network Management Protocol (SNMP)	File-transfer, mail, and management services
Session	Border Gateway Protocol Version 4 (BGP-4) Gateway-to-Gateway Protocol (GGP) Interior Gateway Protocol (IGP)	Gateway protocols that enable networks to share routing and status information
Transport	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)	Transport protocols that control data transmission between computers
Network	Internet Protocol (IP) Internet Control Message Protocol (ICMP) Routing Information Protocol (RIP) Open Shortest Path First (OSPF)	Routing protocols that control addressing and packet assembly, and determine the best route for a packet to take to arrive at its destination
	Domain Name System (DNS) Address Resolution Protocol (ARP) Reverse Address Resolution Protocol (RARP)	Network-address services and protocols that handle the way each computer on a network is identified

See also *ARP*, *BOOTP*, *DNS*, *FTP*, *GGP*, *ICMP*, *IGP*, *IP*, *NFS*, *NIS*, *OSPF*, *RARP*, *RIP*, *RPC*, *SMTP*, *SNMP*, *TCP*, *Telnet*, *UDP*.

TCP/IP header compression—See *VJ compression*.

TCP timeout—A value that specifies the maximum length of time the TAOS unit can attempt to connect to one of the IP hosts in the list provided by the Domain Name System (DNS) server. Because the first host on the list might not be available, the timeout value should be short enough to enable the TAOS unit to go on to the next address on the list before the client software times out. This feature applies to all TCP connections initiated from the unit, including Telnet, Rlogin, TCP-Clear, and the TCP portion of DNS queries. See also *DNS*, *Raw TCP*, *Rlogin*, *Telnet*.

TD—Transmit Data. TD is a signal that indicates that the modem is sending data. See also *DB-25 pin connector*.

TDM—Time Division Multiplexing. TDM is a scheme that uses time-slot assignments to combine information from multiple channels into a single stream of data. Compare with *FDM*.

TE—Terminal Equipment. A TE device resides on the user side of an ISDN connection. Compare with *NT equipment*. See also *network side*, *user side*.

Telecommunications Industry Association—See *TIA*.

telecommuter—A work-at-home computer user who uses remote-access technology to connect to the corporate LAN backbone. For example, a telecommuter can establish a link with the LAN by means of a modem connected to an analog line, an ISDN Terminal Adapter (TA) or router connected to an ISDN line, or a Channel Service Unit/Data Service Unit (CSU/DSU) connected to a Switched-56 line. See also *analog line*, *CSU*, *DSU*, *ISDN line*, *modem*, *TA*.

Telnet—A protocol that links two computers in order to provide a terminal connection to the remote machine. Instead of dialing in to the computer, you use Telnet to connect to it over the Internet. When you initiate a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

Telnet host—A device with which you establish a Telnet session. See also *Telnet*, *Telnet session*.

Telnet mode—The mode in which terminal-server Telnet users communicate with the Telnet host. See also *ASCII mode*, *Binary mode*, *Transparent mode*.

Telnet password—The password a user must enter to gain access to the TAOS unit by means of Telnet. A user is allowed three tries of 60 seconds each to enter the correct password. See also *Telnet*, *Telnet host*, *Telnet session*.

Telnet session—A terminal connection to a remote machine by means of the Telnet protocol. After you set up a basic IP configuration on a TAOS unit, each user can initiate a Telnet session to the unit from a local workstation or from a WAN connection.

terabyte—A data measurement unit equal to 1,000GB or one trillion bytes.

terminal—A computer that does not have its own processor and that must connect to a terminal server in asynchronous mode to use its Central Processing Unit (CPU). VT100, ANSI, and TTY are types of terminals.

Terminal Adapter—See *TA*.

Terminal Access Concentrator Access Control Server—See *TACACS*.

Terminal Access Concentrator Access Control Server Plus—See *TACACS+*.

terminal-emulation program—See *terminal emulator*.

terminal emulator—A program that makes your computer function like a terminal so that you can connect to a terminal server. Your computer acts like a terminal during the connection. All processing takes place remotely. A terminal emulator is also called a *terminal emulation program*. See also *terminal server*.

Terminal Equipment—See *TE*.

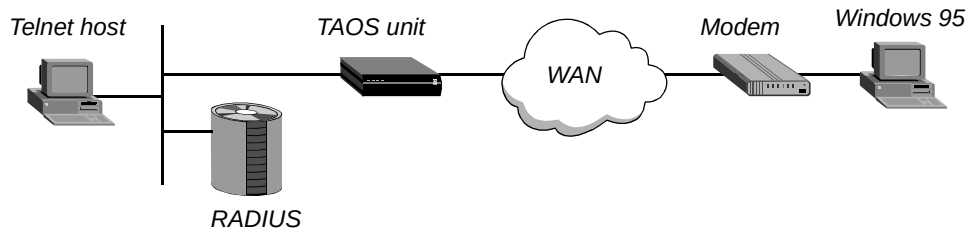
terminal mode—A terminal-server access mode in which the TAOS unit negotiates a user-to-host session. Instead of providing only a login name and password, you can set up an expect-send script that includes not only those two values, but also the terminal-server prompt and a command, such as PPP, SLIP, TCP, Telnet, or Rlogin. Initiation of a session with a host then becomes part of the login process, so the user never actually sees the terminal-server command-line prompt. Alternatively, you can provide access to the command line and restrict the commands you make accessible to the user. See also *expect-send script*, *PPP*, *Rlogin*, *SLIP*, *TCP*, *Telnet*, *terminal server*.

terminal server—A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. A terminal communicates with the terminal server over an asynchronous serial port (typically an RS-232 port) through a modem. A terminal converts the data it receives from the terminal server into a display and does no further processing of the data. A terminal also converts the operator's keystrokes into data for transmission to the terminal server.

A TAOS unit's terminal-server software receives asynchronous calls after they have been processed by a digital modem. Typically, a modem or V.120 Terminal Adapter (TA) dials these calls. V.120 and TCP calls are enabled by default. If the caller does not send Point-to-Point Protocol (PPP) packets immediately, the terminal server starts a login sequence.

Figure 89 shows an incoming modem call. A PC running SoftComm initiates the connection. (SoftComm is a program that causes the user's modem to dial into the TAOS unit.) The TAOS unit directs the call to its digital modem, and then forwards the calls to its terminal-server software. In Figure 89, the TAOS unit immediately directs the call to a Telnet host.

Figure 89. Terminal-server connection



When it receives a name and password from the caller, the terminal server authenticates them by means of a profile or external authentication server, and then performs one of the following actions:

- Displays the terminal-server command-line prompt
- Displays a menu of hosts the user can log in to
- Immediately logs the user in to a designated host
- Initiates a PPP or SLIP session with the user

To protect the command line from unauthorized access, you can also choose to assign the terminal server its own password.

If it receives an asynchronous PPP call, the terminal server does not begin a login sequence. Instead, it responds with a PPP packet, and Link Control Protocol (LCP) negotiation begins, including negotiation for Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) authentication. The terminal server directs the call to the router software, and the connection proceeds as for a regular synchronous PPP session. The user bypasses the terminal-server interface altogether.

In most cases, the terminal server is a stepping stone toward access to one or more network hosts. To enable host access, you can configure the terminal server in terminal mode, immediate mode, or menu mode. See also *asynchronous PPP*, *CHAP*, *digital modem*, *immediate mode*, *menu mode*, *modem*, *PAP*, *PPP*, *SLIP*, *terminal mode*, *user profile*, *V.120 TA*.

terminal-server connection—A connection between a terminal and a terminal server over a LAN or WAN link. See also *terminal server*.

terminal-server idle timer—A value that specifies the number of seconds a terminal-server connection must remain idle before the TAOS unit disconnects the session. See also *terminal server*, *terminal-server session*.

terminal-server session—An end-to-end connection between a terminal and a terminal server. Usually, the terminal-server session begins when the call goes online and ends when the call disconnects. TAOS units support all the common capabilities of standard terminal servers, including Telnet, Domain Name System (DNS), login and password control, Call Detail Reporting (CDR), and authentication services. See also *CDR*, *DNS*, *Telnet*, *terminal server*.

Terminal Timing signal— Specified in the V.35, X.21, and RS-449 serial interfaces, a clock signal that compensates for the phase difference between Send Data and Send Timing. See also *RS-449*, *V.35*, *X.21*.

TFTP—Trivial File Transfer Protocol. TFTP is a simplified version of FTP. It enables you to transfer files from one computer to another.

thick Ethernet—See *10Base5*.

thicknet—See *10Base5*.

thin Ethernet—See *10Base2*.

thinnet—See *10Base2*.

third-party routing—A feature that enables the TAOS unit to advertise Open Shortest Path First (OSPF) routes to external destinations on behalf of another gateway, commonly known as advertising a forwarding address. When third-party routing is enabled, the TAOS unit advertises the IP address of another gateway. If third-party routing is disabled, the TAOS unit advertises itself as the forwarding address to an external destination.

Depending on the exact topology of the network, other routers might be able to route packets directly to the forwarding address without involving the advertising TAOS unit, thereby increasing the total network throughput. In this scenario, all OSPF routers must know how to route to the forwarding address. See also *OSPF*.

throughput—The actual speed of a network.

TIA—Telecommunications Industry Association. The TIA is a group that determines standards for the electrical level of data transmission.

tick—An IBM unit of measurement that corresponds to one-eighteenth of a second.

Time Division Multiplexing—See *TDM*.

timeout—An event in which a device or user exceeded a configured time limit for responding to a device or process.

Time Slot Interchange—See *TSI*.

Time Slot Interchange Switch—See *TSIS*.

tip grounding—The occurrence of a short on the tip wire. If the tip wire is grounded and the ring wire is either open or grounded, the telephone line is dead, because there is no path over which electricity can flow. If the tip wire is grounded and the ring wire is closed, the current flows on the ring side, but the tip side is shorted out. See also *ring wire*, *tip wire*.

tip lead—The end of a tip wire. Compare with *ring lead*. See also *tip wire.*

tip wire—The positive (+) wire in a telephone circuit. Compare with *ring wire.*

TM—Trunk Module. On a Stinger unit, each Trunk Module provides outgoing Asynchronous Transfer Mode (ATM) transmissions. Trunk-to-trunk aggregation is also supported. You can choose to run the full trunk-side bandwidth, or set up a redundant switchover configuration in which one TM is passive. Each TM supports four interfaces for a total trunk-side bandwidth of 622Mbps. See also *ATM*, *Stinger*™.

token—A password that appears in the LCD display of a token card. See also *token card*, *token-card authentication*, *token-card server*.

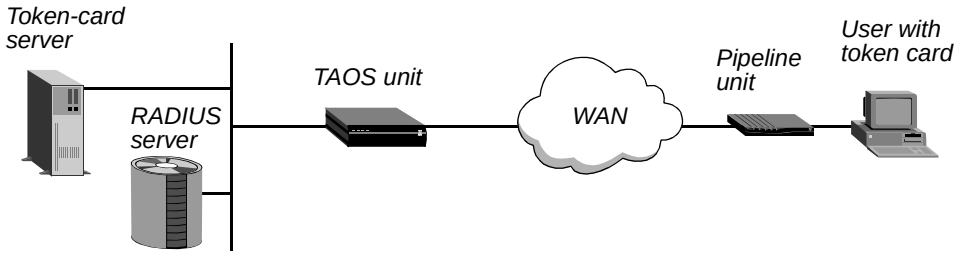
token card—A hardware device, typically shaped liked a credit-card calculator, that displays a current, one-time-only password called a *token.* The token grants a user access to a secure network, and changes many times per day. Token cards keep changing authentication information continuously up-to-date by maintaining a synchronized clock with a token-card server, such as a Security Dynamics ACE/Server or an Enigma Logic SafeWord server. To gain access to a secure network, each user must have a token card.

A token card protects against replay attacks, in which an unauthorized user records valid authentication information exchanged between systems, and then replays it later to gain entry. Because the token is a one-time-only password, replay is impossible. See also *ACE authentication, SafeWord authentication, token, token-card authentication, token-card server*.

token-card authentication—A form of authentication requiring that users change passwords many times per day. A TAOS unit supports token-card authentication by using a RADIUS server as the intermediary between the TAOS unit answering the call and an authentication server (such as a Security Dynamics ACE/Server or an Enigma Logic SafeWord server).

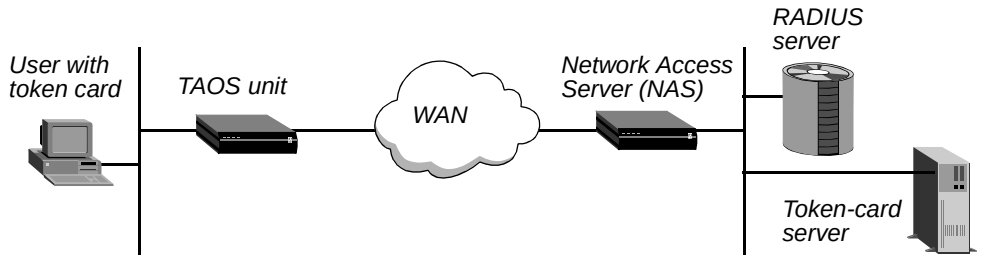
Figure 90 shows a dial-in connection to a TAOS unit. The remote user must use a token card to gain access to the secure network.

Figure 90. Token-card authentication for dial-in connections



The next figure, Figure 91, shows a dial-out connection from the TAOS unit. The local user must use a token card to gain access to the remote secure network.

Figure 91. Token-card authentication for dial-out connections



A local user with a token card initiates a connection by logging in to the TAOS unit's terminal server and dialing out to the remote unit. These actions require that the user have login privileges to the TAOS unit, and that the TAOS unit have a profile configured for a connection to the remote device.

See also *ACE authentication, SafeWord authentication, token, token card, token-card server*.

token-card server—A server that maintains a synchronized clock with hand-held token cards to provide users with a current, one-time-only password, called a *token*. The correct token is required for access to a secure network. Examples of token-card servers are the Security Dynamics ACE/Server and the Enigma Logic SafeWord server. See also *ACE authentication, SafeWord authentication, token, token card, token-card authentication.*

Token Ring—A network architecture that uses a ring topology, baseband signaling, and the token-passing media-access method. Token Ring can operate at 1, 4, or 16Mbps, and supports four-wire twisted pair or fiberoptic media.

tone transponder mode—On a Signaling System 7 (SS7) network, a method of performing a continuity test. In tone transponder mode for a T1 line, the channel can detect either a 2010Hz or 1780Hz tone. In tone transponder mode for an E1 line, the channel can detect either a 2000Hz or 1780Hz tone. When either tone is detected, the other one is returned. You can use tone transponder mode only for lines provisioned for incoming 2-wire and 4-wire-to-2-wire continuity tests. See also *2-wire continuity test*, *continuity test*, *SS7 network*.

topology—The design of a network. *Physical topology* refers to the layout of the hardware. *Logical topology* refers to the paths that messages take to get from one node to another.

TOS—Type of Service. A feature that enables an Internet device to select the Quality of Service (QoS) for an application. The TOS is specified by precedence, delay, throughput, reliability, and cost. You can configure a TAOS unit to set priority bits and TOS classes of service on behalf of customer applications. The TAOS unit does not implement priority queuing, but it does set information that can be used by upstream routers to prioritize and select links for particular data streams. See also *precedence*, *QoS*, *TOS filter*.

TOS filter—Type of Service filter. A TOS filter is a packet filter that enables you to specify a precedence value, a TOS value, and many of the same values as an IP filter. Like other kinds of packet filters, a TOS filter can affect incoming packets, outgoing packets, or both. Compare with *generic filter*, *IP filter*, *IPX filter*. See also *packet filter*, *precedence*, *TOS*.

TPDU—Transport Protocol Data Unit. A packet, created at the Transport layer, that contains control information and a payload.

traditional toll service—A term denoting traditional long-distance service.

traffic descriptor—In Asynchronous Transfer Mode (ATM) transmission, a designation that determines the number and type of cells admitted into a congested queue, and whether or not high-priority cells are tagged as low-priority cells when traffic exceeds specified thresholds. Following are the ATM traffic descriptors:

- Peak Cell Rate (PCR)
- Sustainable Cell Rate (SCR)
- Maximum Burst Size (MBS)
- Cell Loss Priority (CLP)
- Tagging
- Best Effort

See also *ATM*, *Best Effort*, *CLP*, *MBS*, *PCR*, *SCR*, *tagging*.

traffic policing—An Asynchronous Transfer Mode (ATM) method of monitoring and controlling the rate of traffic by buffering or discarding cells that do not conform to the terms of the Quality of Service (QoS) contract. See also *ATM*, *QoS contract*, *traffic shaping*.

traffic shaper—In an Asynchronous Transfer Mode (ATM) configuration, a group of settings that define characteristics for different types of traffic. For example, a traffic shaper for voice transmissions might require a constant amount of bandwidth and low delay times, while a traffic shaper for file transfers might specify variable bandwidth and longer delays. When you define a traffic shaper, you can apply it to any number of connections. See also *ATM*, *traffic shaping*.

traffic shaping—In Frame Relay, a set of rules for defining traffic flow and ensuring that the transmission of guaranteed packets occurs in a certain way. In an Asynchronous Transfer Mode (ATM) configuration, a method of modifying the traffic characteristics of a stream of cells to achieve better network efficiency and meet all Quality of Service (QoS) objectives. See also *ATM*, *Frame Relay*, *QoS*, *traffic policing*.

Transaction Processing Protocol for Point-of-Service—See *T3POS*.

transaction server—A program that performs database transaction requests on behalf of a client. See also *SDTN*.

transceiver—A device that transmits and receives analog or digital signals (for example, the LAN component that places signals onto the network cable and picks up signals from the cable). Usually, the transceiver is built into the Network Interface Card (NIC), but some types of networks necessitate an external transceiver. In an Ethernet network, a transceiver is also called a *Medium Access Unit (MAU)*. See also *Ethernet transceiver*, *NIC*.

transform—An Internet Protocol Security (IPSec) component consisting of a security protocol and its algorithms. For example, the Authentication Header (AH) protocol and the MD5 authentication algorithm make up one transform; the Encapsulating Security Payload (ESP) protocol and the DES-CBC encryption algorithm constitute another. See also *AH*, *DES-CBC*, *ESP*, *IPSec*, *MD5*.

translation-mode ATM-Frame Relay circuit—A circuit in which the system removes Frame Relay Multiprotocol Encapsulation (RFC 1490) from the data stream received on a Frame Relay interface and adds ATM Multiprotocol Encapsulation (RFC 1483) to the data stream sent on an ATM interface (and vice versa) from one side of the circuit to the other. Compare with *transparent-mode ATM-Frame Relay circuit*. See also *ATM*, *Frame Relay*.

translation table—A table used by network address translation (NAT) for LAN. The translation table is limited to 500 addresses. A translation table entry represents one TCP or UDP connection. The translation table entries are reused as long as packets match an entry. All entries expire when a connection disconnects.

Transmission Control Protocol—See *TCP*.

Transmission Control Protocol/Internet Protocol—See *TCP/IP*.

Transmit Data—See *TD*.

transmit data rate—The rate of data sent by a TAOS unit. Compare with *receive data rate*.

transparent bridge—A bridge that notes a packet's source address and creates a bridging table associating a host's Media Access Control (MAC) address with a particular Ethernet interface. See also *bridge*, *bridging*.

Transparent mode—A data-transfer mode for host-initiated calls on an X.25/T3POS network; also, a Telnet mode. In Transparent mode for an X.25/T3POS network, the T3POS PAD does not provide any error recovery. Rather, the Data Terminal Equipment (DTE) and the host system provide error recovery for the connection. In Transparent mode, however, the T3POS PAD does recognize a DLE, EOT command from the DTE, and clears the call when it receives one.

In Transparent mode for a Telnet connection, you can send and receive binary files without being in Binary mode. You can also run the same file-transfer protocols available in Binary mode. Compare with *ASCII mode*, *Binary mode*, *Binary Local mode*, *Blind mode*, *Local mode*. See also *DLE*, *EOT command*, *DTE*, *PAD*, *X.25/T3POS*.

transparent-mode ATM-Frame Relay circuit—A circuit in which the system performs no ATM-to-Frame Relay or Frame Relay-to-ATM conversion, but simply passes the data stream from one end to the other. Transparent-mode ATM-Frame Relay circuits are defined in the *FRF.8 Frame Relay ATM/PVC Service Interworking Implementation Agreement*. Transparent mode requires that the circuit end points support compatible upper-layer protocols for applications such as packetized voice. Compare with *translation-mode ATM-Frame Relay circuit*. See also *ATM*, *Frame Relay*.

transparent modem—A MultiVoice feature in which a TAOS unit transparently requests end-to-end G.711 encoding and bandwidth for the call when it detects a modem in a Voice over IP (VoIP) channel. The echo cancelers are disabled when the TAOS unit enters transparent modem mode. The data is encoded transparently as an audio-mode type, either G.711 U-law (64Kbps) or G.711 A-law (64Kbps). Settings take effect with the next incoming Public Switched Telephone Network (PSTN) call.

If a TAOS unit has been licensed for real-time fax, users can run either a high-speed modem, with speeds greater than 2400bps, or a fax terminal in the VoIP channel. This capability provides a fallback for real-time fax transmissions. Both fax terminals and high-speed modems transmit a single tone when they answer a call, but they do not use the same tone. The TAOS unit can therefore detect the type of equipment answering the call and send the appropriate H.245 request-mode message. For a transparent modem, the message requests a switchover from the current audio codec to G.711 with no echo canceler. For real-time fax, the request is to switch to T.38 data mode.

See also *A-Law*, *MultiVoice™*, *PSTN*, *U-Law*, *VoIP*.

transparent tunneling— A configuration in which a tunnel to a dial-in network is created automatically, without any explicit action by the user. See also *tag*, *tunneling*.

Transport layer—The middle layer of the OSI Reference Model. The Transport layer provides data transfer at the proper speed, quality, and error rate, ensuring reliable delivery. See also *OSI Reference Model*.

transport mode—An Internet Protocol Security (IPSec) mode that provides security services for higher-layer protocols, including selected portions of the IP header and other selected options. Transport mode operates between two hosts. Compare with *tunnel mode*. See also *AH*, *ESP*, *IPSec*.

Transport Protocol Data Unit—See *TPDU*.

trap—See *traps-PDU*.

traps-PDU—A message that a Simple Network Management Protocol (SNMP) agent sends to a manager application to inform the manager of network events. See also *agent*, *community name*, *manager*, *MIB*, *SNMP*.

Triple Data Encryption Standard-Cypher Block Chaining—See *3DES-CBC*.

Trivial File Transfer Protocol—See *TFTP*.

True Access™ Operating System—See *TAOS*.

true connect—A feature that enables the system to delay alert and connect messages sent to the Public Switched Telephone Network (PSTN). Without the true connect feature, incoming Voice over IP (VoIP) calls from the PSTN are connected at the local gateway before any H.323 signaling is sent to the remote gateway. As a result, a PSTN charge is incurred at the time of the connection to the local gateway, before the called party receives and answers the call from the remote gateway. With true connect, you avoid incurring charges before a VoIP call has been answered. See also *gateway*, *H.323*, *PSTN*, *VoIP*.

trunk—A high-capacity communications circuit between two systems.

trunk deactivation—A feature that enables a MultiVoice gateway to automatically deactivate trunks used for Voice over IP (VoIP) calls when a gateway becomes unavailable. Trunk deactivation prevents the Public Switched Telephone Network (PSTN) switch from routing subsequent calls to the trunks configured for VoIP. Current calls remain active until they are terminated by the caller or PSTN. Trunks configured to accept VoIP calls are made unavailable to the PSTN under the following conditions:

- A gateway cannot register with either a primary or secondary gatekeeper.
- A gateway's trunk connection with the PSTN is unavailable, so that gateway is forced to unregister itself from its gatekeepers.

When you use the trunk deactivation feature, gatekeepers in the MultiVoice network route calls to other available gateways, use network resources more efficiently, and improve service quality for users. See also *MultiVoice™*, *PSTN*, *VoIP*.

trunk group—A group of switched channels to use for outgoing calls. To specify that outgoing calls use a specific bandwidth, you can configure a profile to refer to a specific trunk group. You can also use trunk groups to separate lines supplied by different carriers. Each set of lines can be used as a backup if a switch becomes unavailable.

The decision to use trunk groups is a global one. Once you enable the use of trunk groups, every switched channel must be assigned a trunk-group number or it will not be available for outgoing calls. In addition, trunk groups limit the number of channels available to any given multichannel call, because only channels within the same trunk group can be aggregated.

Trunk Module—See *TM*.

trunk port sparing—A method of designating a secondary trunk port as a backup to another trunk port in the system. When the sparing function is in use, and the primary trunk port becomes inactive, all of its Virtual Channels (VC) are terminated and set up on the spare, maintaining their original VPI/VCI numbers. If the spare port becomes inactive, all of its VCs are terminated and set up again on the primary port, maintaining their original VPI/VCI numbers.

If the physical connection on an active port breaks or is operating in only one direction, one end will detect that the connection has been lost and will switch to the spare port, but the other end will not. The receiver error should be reported to the other end by means of the remote alarm reporting facilities of the physical layer. See also *VC, VCI, VPI*.

trunk restoration—A process that reroutes the Permanent Virtual Circuits (PVCs) on the backup trunk to the primary trunk.

trunk prefixing—A feature that enables a TAOS unit to identify the entry (ingress) trunk number to the exit (egress) gateway or call signaling entity by prepending the ingress trunk number to the Dialed Number Information Service (DNIS) number. The Q.931 Called Party Number Information Element (IE) in an H.225/Q.931 Setup message then contains the DNIS number prefixed by the incoming trunk number. See also *DNIS, H.225, Q.931*.

trunk-side connection—A line that extends from the telephone company's Central Office (CO) to the telephone network. Typically, a trunk-side connection is high-bandwidth and all digital. Compare with *line-side connection*.

TSI—Time Slot Interchange. A device that performs Time Division Multiplexing (TDM) in a Time Slot Interchange Switch (TSIS). A TSI device groups multiplexed channels into a frame. It then writes each channel of the incoming frame into data memory at the slot address determined by control memory. The TSI device reads each slot of data memory, puts it in an outgoing multiplexed frame, and sends the outgoing channels to a demultiplexer. See also *multiplexing, TDM*.

TSIS—Time Slot Interchange Switch. A device that uses a Time Slot Interchange (TSI) to multiplex channels into a frame.

TTL—Time To Live. A field in an Internet Protocol (IP) packet, TTL indicates whether the packet has been in the network too long. Because each router subtracts at least one count from the TTL field, the count typically indicates the number of router hops the packet can travel before a router discards it. When the count reaches zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) message to the sender, who can choose to resend the data.

If you use IP multicast forwarding, the TTL value indicates how far a packet can be forwarded. The packet has one of the following TTL values:

TTL value	Indicates packet is
0	Restricted to the same host
1	Restricted to the same subnet
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Not restricted to any area or device

See also *ICMP, IP, IP multicast forwarding.*

tunneling—A way of overcoming protocol restrictions on a network by encapsulating packets that use an unsupported protocol inside packets that use a protocol supported by the network.

tunnel mode—An Internet Protocol Security (IPSec) mode required for connections between a host that does not perform IPSec processing and a security gateway. In tunnel mode, IP packets are encapsulated in an outer IP header that specifies the IPSec processing destination. Compare with *transport mode*. See also *AH*, *ESP*, *IPSec*.

tunnel server—When a tunneling protocol is in use, the system that decapsulates the packets. Examples of tunneling protocols are Ascend Tunnel Management Protocol (ATMP), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP). See also *ATMP*, *L2TP*, *PPTP*.

twisted-pair cable—A cable consisting of two or more copper wires twisted together in pairs. Telephone wiring is an example of twisted-pair cable. Twisted-pair cable can be shielded or unshielded. See also *STP cable*, *UTP cable*.

twisted-pair Ethernet—See *10BaseT*.

two-stage dialing—A scenario in which a user must first dial in to an intermediary device, such as a MultiVoice gateway, and then dial the telephone number of the destination device. Compare with *single-stage dialing*. See also *MultiVoice*™.

two-wire subscriber loop—A two-wire WAN link connecting the Customer Premises Equipment (CPE) to the carrier's switch. See also *CPE*.

Type-5 LSA—See *ASE Type-5*.

Type-7 LSA—See *ASE Type-7*.

Type of Service—See *TOS*.

U

UART—Universal Asynchronous Receiver/Transmitter. A UART is a chip that provides a RS-232C Data Terminal Equipment (DTE) interface to a device, enabling the unit to communicate with its attached serial devices. See also *asynchronous transmission*, *DTE*, *RS-232C*, *serial transmission*.

UBR—Unspecified Bit Rate. UBR is an Asynchronous Transfer Mode (ATM) service class that handles bursty LAN traffic and data that is tolerant of delays and cell loss. UBR is a best-effort service that does not specify bit-rate or traffic values, and offers no Quality of Service (QoS) guarantees. Compare with *ABR*, *CBR*, *QoS*, *VBR-NRT*, *VBR-RT*. See also *ATM*.

UCHCS errors—Uncorrectable Header Check Sequence errors. UCHCS errors are Header Check Sequence (HCS) errors that the receiving unit cannot correct. Compare with *CHCS errors*. See also *HCS*.

UDI—Unrestricted Digital Information. A category of data transfer in which the bit format is entirely unrestricted. Compare with *RDI*.

UDP—User Datagram Protocol. UDP is a Transport-layer protocol that provides connectionless service without packet acknowledgment. See also *Transport layer*, *UDP port*.

UDP port—A16-bit number that enables multiple processes to use User Datagram Protocol (UDP) services on the same host. A UDP address is the combination of a 32-bit IP address and a 16-bit port number. Examples of well-known UDP ports are 7 (for Echo packets), 161 (for SNMP packets), and 514 (for Syslog packets). See also *UDP*.

UDP queue—A queue containing unprocessed User Datagram Protocol (UDP) requests. Compare with *backoff queue*, *RIP queue*, *SNMP queue*. See also *queue*.

U interface—(noun) The electrical interface between an ISDN telephone line and a network termination type 1 (NT1) device. (adjective) An ISDN communications device that connects directly to an ISDN telephone line. A U-interface device contains its own NT1 device. See also *NT1*.

U-Law—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for sampling data by means of Pulse Coded Modulation (PCM). U-Law is most commonly used in North America and Japan. Compare with *A-Law*. See also *PCM*.

Unavailable Second—On a SONET network, a second in which the interface is unavailable at the specified layer. An interface is considered unavailable after 10 consecutive Severely Errored Seconds. See also *Severely Errored Second*, *SONET*.

unchannelized T1 PRI/E1 PRI—A service that uses the entire bandwidth of a T1 PRI line (1.544Mbps) or of an E1 PRI line (2.048Mbps). You can use an unchannelized line for a dedicated connection, such as the link to a Frame Relay network. A TAOS unit treats the line as though it were a single connection at a fixed speed, without individual channels. Compare with *channelized T1 PRI/E1 PRI*. See also *E1 PRI line*, *T1 PRI line*.

Uncorrectable Header Check Sequence errors—See *UCHCS errors*.

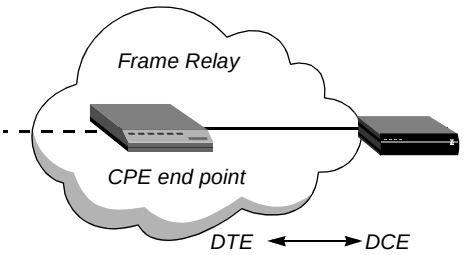
UNI—User-to-Network Interface. A UNI is the interface between an end user and a network end point (a router or a switch) on the Frame Relay or Asynchronous Transfer Mode (ATM) network.

In Frame Relay, Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) devices perform UNI procedures for link management. These procedures occur in one direction. The DTE requests information and the DCE provides it. When configured with a UNI to Frame Relay, a TAOS unit can act as the user side (UNI-DTE) communicating with the network side (UNI-DCE) of a switch, or as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device. In an ATM network, a UNI connects an ATM end system, such as a router, with an ATM switch. Compare with *NNI*. See also *DCE*, *DTE*, *Frame Relay network*, *UNI-DCE interface*, *UNI-DTE interface.*

unicast network—A network in which a router sends packets to one user at a time. Compare with *broadcast network*, *multicast network.*

UNI-DCE interface—User-to-Network Interface–Data-Circuit-terminating-Equipment interface. On a UNI-DCE interface, the TAOS unit acts as the network side communicating with the user side (UNI-DTE) of a Frame Relay device. Figure 92 shows an example of a TAOS unit with a DCE interface.

Figure 92. Frame Relay DCE interface

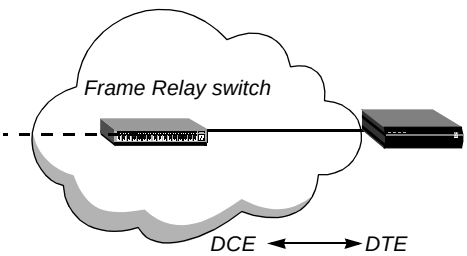


Compare with *UNI-DTE interface*. See also *DCE*, *DTE*, *Frame Relay network*, *UNI*.

UNI-DTE interface—User-to-Network Interface–Data-Terminal-Equipment interface. On a UNI-DTE interface, the TAOS unit acts as the user side communicating with the network-side DCE switch. It initiates link-management functions by sending a Status Enquiry message to the UNI-DCE device. Status enquiries can be about the status of Permanent Virtual Circuit (PVC) segments the DTE knows about, and they can include requests for information about the integrity of the data link between the UNI-DTE and UNI-DCE interfaces.

Figure 93 shows an example of a TAOS unit with a UNI-DTE interface.

Figure 93. Frame Relay DTE interface



Compare with *UNI-DCE interface*. See also *DCE*, *DTE*, *Frame Relay switch*, *UNI*.

Universal Asynchronous Receiver/Transmitter—See *UDP*.

UNIX—A 32-bit operating system that enables multiple users to share resources and perform multiple tasks at the same time. UNIX was developed at Bell Laboratories in 1969. Its development has occurred along two lines: the AT&T System versions and the UC Berkeley Distribution (BSD) releases. The two strains were combined by the UNIX Systems Group into System V Release 4.2 (SVR 4.2).

UNIX hosts file—The `/etc/hosts` file on the UNIX host. The UNIX hosts file contains the names and IP address of all the hosts with which the UNIX server can communicate.

UNIX password—A password entered in the `/etc/password` file on the UNIX host. In a RADIUS user profile, setting the password to `UNIX` provides authentication through the normal UNIX authentication procedure. You cannot specify a UNIX password with Challenge Handshake Authentication Protocol (CHAP) authentication. See also *CHAP*.

UNIX password file—The `/etc/password` file on the UNIX host. The UNIX password file contains passwords for standard UNIX authentication.

unnumbered interface—A link that uses system-based routing, in which a TAOS unit has a single IP address for all of its interfaces. If all interfaces are unnumbered, the TAOS unit operates as a purely system-based router. Compare with *interface-based routing*, *numbered interface*. See also *IP routing*, *system-based routing*.

Unrestricted Digital Information—See *UDI*.

unshielded cable—Any cable not protected from electromagnetic or radio-frequency interference.

Unshielded Twisted Pair cable—See *UTP cable*.

Unspecified Bit Rate—see *UBR*.

UPC—Usage Parameter Control. UPC is a method of policing Asynchronous Transfer Mode (ATM) transmissions to ensure that incoming data does not exceed its Quality of Service (QoS) contract. If a cell exceeds the contract, the TAOS unit takes one of the following actions:

- Delays the traffic until the congestion lessens and there is available bandwidth to deliver the data
- Tags the cell by setting the Cell Loss Priority (CLP) bit to 1
- Discards the cell

See also *ATM*, *CLP*, *QoS contract*.

upstream path—The path a call takes from the end user's home to the carrier's Central Office (CO).

Usage Parameter Control—See *UPC*.

User-Based Security Model—See *SNMPv3 USM*.

User Datagram Protocol—See *UDP*.

user facility—See *facility*.

username—The name a user must enter to gain access to the services of a TAOS unit. See also *password*.

user profile—A RADIUS entry that contains authentication, incoming call configuration, dial-out, routing, and filter information. Each user profile consists of a series of attributes. The attributes specify a username and password, and enable you to configure routing, call management, and restrictions on the types of TAOS unit resources a caller can access. See also *pseudo-user profile*, *RADIUS*, *RADIUS server*.

user side—The end of an ISDN connection that terminates at the user's equipment. Because ISDN links exist only between the CO and the customer, an ISDN link can be viewed as having two sides: the network side, where the Network Terminating (NT) equipment resides, and the user side, where the Terminal Equipment (TE) resides. The user side can connect only to the network side, and vice versa. Both the network side and the user side perform the same functions, but the format of the messages is different. For example, the network side must always set a bit and the user side must always clear it. These differences allow either side of a connection attempt to determine whether the other side is the correct type. Compare with *network side*.

User-to-Network Interface—See *UNI*.

UTC—Coordinated Universal Time. Formerly known as Greenwich Mean Time (GMT), UTC is the time at the Greenwich observatory, used as a reference point for calculating standard time values.

UTP cable—Unshielded Twisted Pair cable. UTP cable consists of at least four pairs of wires twisted two or more times per inch in order to help cancel out noise. The cable has no outside covering. UTP cable is typically used in telephone lines for voice service, ARCnet networks, 10BaseT Ethernet networks, and particular sections of Token Ring networks. See also*10BaseT*, *ARCnet*, *Token Ring*.

UTP Ethernet—See *10BaseT*.

V

V.21—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for 300bps full-duplex modems.

V.22—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that supports a data rate of up to 1200bps at 600 baud. Compare with *V.22bis*.

V.22bis—An extension of the V.22 standard, providing a data rate of up to 2400bps at 600 baud. See also *V.22*.

V.23—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for 600bps and 1200bps full-duplex modems.

V.24—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that specifies a Physical-layer interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE). V.24 is nearly identical to RS-232. See also *DCE*, *DTE*, *RS-232*.

V.25bis—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for automatic calling and answering equipment on the Public Switched Telephone Network (PSTN). See also *PSTN*.

V.32—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for full-duplex modem transmission of data across telephone lines at rates of up to 9600bps, with a fallback rate of 4800bps. A V.32 modem automatically adjusts its transmission speed on the basis of line quality. Compare with *V.32bis*. See also *full duplex*.

V.32bis—An extension of the V.32 standard, providing a data rate of up to 14,400bps or fallback to 12000bps, 9600bps, 7200bps, and 4800bps. Compare with *V.32*.

V.34—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for full-duplex modem transmission of data across telephone lines at rates of up to 28,800bps. A V.34 modem automatically adjusts its transmission speed on the basis of line quality.

V.35—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for high-speed synchronous data transmission and exchange. In the United States, most routers and Data Service Units (DSUs) that connect to T1 lines use V.35. See also *DSU*, *router*, *synchronous transmission*, *T1 line.*

V.42—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) error-detection standard for high-speed modems over digital telephone lines. The V.42 standard makes use of the Link Access Procedure, Modem (LAPM). See also *LAPM.*

V.42bis—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) data-compression standard for use with V.42 technology. The V.42bis data-compression standard provides a maximum of a four-to-one data-compression ratio. Because compression algorithms are software based, overhead can cause problems in real-time environments. Most of the time, V.42bis can sense when compression is unnecessary, and so can avoid slowing the transfer of precompressed files. See also *data compression.*

V.90—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for devices that provide a downstream data rate of up to 56Kbps. V.90 modems offer analog modem users a high-speed alternative to 33.6Kbps modems. However, this increased data rate over the local loop is possible only with the right network conditions. A true 56Kbps implementation

- Works only on the downstream, or receiving, path of the call.
- Requires end-to-end V.90 equipment.
- Requires a server trunk-side connection to the Central Office (CO) switch to ensure the existence of only a single analog-to-digital (A-D) conversion.
- Works over the local loop, using the existing infrastructure.

See also *A-D conversion*, *CO*, *local loop*, *modem*, *trunk-side connection*.

V.110—A rate-adaption standard, based on fixed frames, that subdivides the ISDN channel so that it can carry one lower-speed data channel. See also *V.110 TA*.

V.110 TA—V.110 Terminal Adapter. A V.110 TA is a device that changes the format of asynchronous data to match the specifications of the V.110 standard for data transmission over an ISDN line. See also *TA*, *V.110*.

V.120—A standard for converting asynchronous data into synchronous ISDN data. Using standard, asynchronous-only COM ports and a V.120 Terminal Adapter (TA), two computers can communicate over an ISDN connection. See also *V.120 TA*.

V.120 TA—V.120 Terminal Adapter. A V.120 TA is an asynchronous device that changes the format of asynchronous data to match the specifications of the V.120 standard for data transmission over an ISDN line. A V.120 TA is also known as an *ISDN modem*. See also *TA*, *V.120*.

Van Jacobson compression—See *VJ compression*.

Variable Bit Rate-Non Real Time—See *VBR-NRT*.

Variable Bit Rate-Real Time—*VBR-RT*.

Variable-Length Subnet Mask—See *VLSM*.

VBR-NRT—Variable Bit Rate-Non Real Time. VBR-NRT is an Asynchronous Transfer Mode (ATM) service class that handles packaging for the transfer of long, bursty data streams over an established ATM connection. This service is also used for short, bursty LAN traffic. Compare with *ABR*, *CBR*, *VBR-RT*. See also *ATM*.

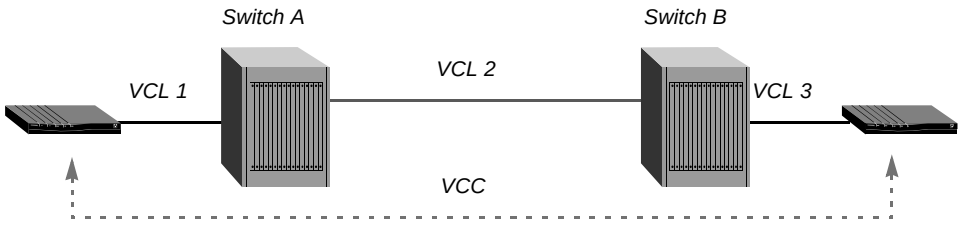
VBR-RT—Variable Bit Rate-Real Time. VBR-RT is an Asynchronous Transfer Mode (ATM) service class that handles the packaging of special delay-sensitive applications, such as packet video, that require low cell-delay variation between end points. Compare with *ABR*, *CBR*, *VBR-NRT*. See also *ATM*.

VC—(1) Virtual Channel. A communications link that provides unidirectional transmission of Asynchronous Transfer Mode (ATM) cells between two points over a shared facility. The link can be established on-demand (as a switched service), or preprovisioned (as Frame Relay PVCs). The two communicating ATM entities are associated by a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI). All communications proceed along the same VC, preserving cell sequence and quality of service. See also *ATM*, *VCI*, *VPI*.

(2) Virtual Circuit. On a Frame Relay, X.25 or Open Shortest Path First (OSPF) network, a VC is a bidirectional data path between two end points. See also *Frame Relay network*, *OSPF*, *PVC*, *SVC*, *X.25*.

VCC—Virtual Channel Connection. An Asynchronous Transfer Mode (ATM) connection consisting of individual Virtual Channel Links (VCLs) and identified by a VPI-VCI pair in ATM cell headers. Figure 94 shows multiple VCLs concatenated to form a VCC.

Figure 94. VCLs forming a VCC



See also *ATM*, *VCI*, *VCL*, *VPI*.

VCE timer—Virtual Call Establishment timer. On an X.25/PAD network, a value that specifies the number of seconds to maintain a connection to a character-oriented device (such as the terminal server) that has not established a virtual call. See also *X.25/PAD*.

VCI—Virtual Channel Identifier. A VCI is a 16-bit field in the Asynchronous Transfer Mode (ATM) cell header. The VCI identifies a Virtual Channel (VC) between two end points. An ATM switch uses the Virtual Path Identifier (VPI) and VCI values when routing packets. See also *ATM*, *CLP*, *GFC*, *HEC*, *Payload*, *PT*, *VC*, *VPI*.

VCL—Virtual Channel Link. An Asynchronous Transfer Mode (ATM) virtual link identified by a VPI-VCI pair in ATM cell headers. See also *ATM*, *VCC*, *VCI*, *VPI*.

VDSL—Very High Bit-Rate Digital Subscriber Line. VDSL is an asymmetric DSL technology that offers data rates from 13Mbps to 52Mbps downstream and from 1.5Mbps to 2.3Mbps upstream. Compare with *ADSL*, *HDSL*, *IDSL*, *RADSL*, *SDSL*. See also *DSL*.

Vendor-Specific Attribute support—See *VSA support*.

Very High Bit-Rate Digital Subscriber Line—See *VDSL*.

videoconferencing—The use of a digital video-transmission system to communicate by video and voice. A digital video-transmission system typically consists of a camera, codec, network-access equipment, network, and audio system. See also *codec*.

Video Service Unit—See *VSU*.

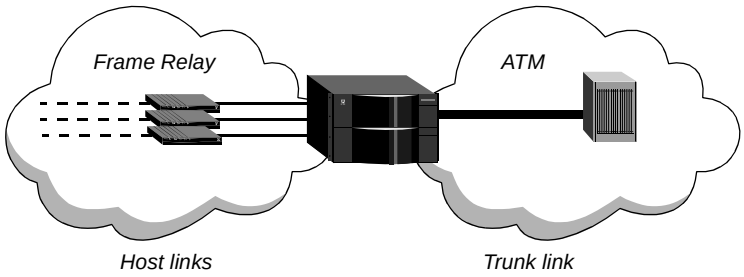
virtual AppleTalk network—A network required for a TAOS unit to route AppleTalk to dial-in clients. You define a virtual AppleTalk network by defining a unique network range. See also *AppleTalk routing*, *network range*.

virtual bandwidth—Channel capacity calculated to allow for the oversubscription of channel usage. See also *bandwidth*, *channel*.

Virtual Channel—See *VC*.

virtual channel trunking—A configuration in which a circuit can have more than two end points. Multiple end points are designated as host links and only one end point is designated as a trunk link. The system aggregates traffic from multiple host links onto one trunk link, creating an *N*:1 circuit, as shown in Figure 95.

Figure 95. N:1 circuit between multiple Frame Relay hosts and an ATM trunk



With virtual channel trunking, the circuit end points can include multiple Frame Relay Data Link Connection Identifier (DLCI) interfaces and an Asynchronous Transfer Mode (ATM) VPI-VCI interface, as long as only one trunk link is specified. When the system receives upstream traffic from a host link, it learns the host's Media Access Control (MAC) address and then forwards the data to the trunk-link interface. When the system receives downstream traffic from the trunk link, it uses the destination MAC address to transmit the packets on the appropriate host link. See also *ATM*, *DLCI*, *Frame Relay*, *MAC address*.

Virtual Circuit—See *VC*.

Virtual Channel Connection—See *VCC*.

Virtual Channel Identifier—See *VCI*.

Virtual Channel Link—See *VCL*.

virtual connection—A set of multiple virtual links concatenated across several Asynchronous Transfer Mode (ATM) switches and extending between two end points. A virtual connection can be a Virtual Channel Connection (VCC) or a Virtual Path Connection (VPC), depending on whether its virtual links are identified in ATM cell headers by a Virtual Path Identifier-Virtual Channel Identifier (VPI-VCI) pair or by the VPI field alone. See also *ATM*, *VCC*, *VCI*, *VPC*, *VPI*.

virtual IPX network—A network required for a TAOS unit to route IPX to dial-in clients. When a NetWare client dials in, the TAOS unit negotiates a routing session by assigning the client a network address on the virtual IPX network. The client must accept the network number that the TAOS unit assigns. If the client has its own node number, the TAOS unit uses that number to form the full network:node address. If the client does not have a node number, the TAOS unit assigns it a unique node address on the virtual network. See also *IPX network, node*.

virtual link—An Asynchronous Transfer Mode (ATM) connection between one device and another. A virtual link can be a Virtual Channel Link (VCL) or Virtual Path Link (VPL), depending on whether it is identified in ATM cell headers by a Virtual Path Identifier-Virtual Channel Identifier (VPI-VCI) pair or by the VPI field alone. See also *ATM, VCL, VCI, VPL, VPI.*

Virtual Path—See *VP*.

Virtual Path Connection—See *VPC.*

Virtual Path Identifier—See *VPI.*

Virtual Path Link—See *VPL*.

Virtual Private Network—See *VPN*.

Virtual Router—See *VRouter*.

Visa-II—A Link-layer encapsulation protocol that facilitates communication between dial-in Visa terminals and a transaction server. See also *SDTN, transaction server*.

VJ compression—Van Jacobson compression. VJ compression is a method for compressing Transmission Control Protocol (TCP) headers in order to decrease round-trip times on Serial Line Internet Protocol (SLIP) connections. The version of SLIP implementing VJ compression is called Compressed Serial Line Internet Protocol (CSLIP). See also *compression, CSLIP, SLIP*.

VLSM—Variable-Length Subnet Mask. Applying a VLSM is a way to configure an IP subnet for maximum flexibility. Two different subnets of the same IP network number might have different masks and, therefore, different sizes. A packet is routed to the longest or most specific match. See also *IP subnet, subnet mask.*

voice announcement file—In a MultiVoice environment, a file that contains a custom voice announcement that a TAOS unit plays to callers to indicate call progress. See also *MultiVoice™*.

voice compression—A method of transmitting voice across an IP network by means of compressed audio frames. An audio codec is used to pack (and unpack) analog speech into digital audio frames. See also *voice packet size*.

Voice over IP—See *VoIP*.

voice packet size—The number of compressed audio frames that a TAOS unit assigns to each Real-Time Transport Protocol (RTP) packet to transport voice across an IP network. See also *voice compression.*

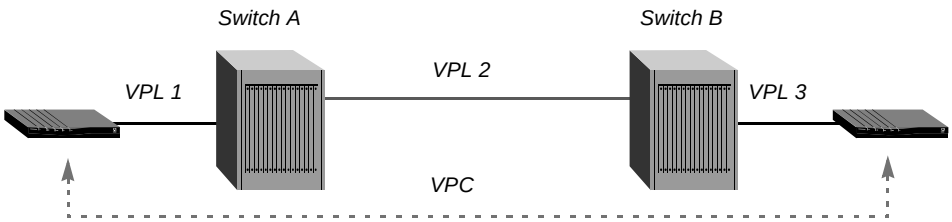
voice splitter—See *POTS splitter*.

VoIP—Voice over IP. VoIP refers to a set of methods for managing the transmission of voice information. The transmission takes place by means of the Internet Protocol (IP). A device can send voice data in digital form, thereby avoiding the expenses associated with ordinary telephone service. See also *IP*.

VP—Virtual Path. In Asynchronous Transfer Mode (ATM), a VP is a group of Virtual Channels (VCs) carried between two points. It provides a way to bundle traffic headed in the same direction. See also *VC.*

VPC—Virtual Path Connection. An Asynchronous Transfer Mode (ATM) connection consisting of individual Virtual Path Links (VPLs) identified by the Virtual Path Identifier (VPI) field in ATM cell headers. Figure 96 shows multiple VPLs concatenated to form a VPC.

Figure 96. VPLs forming a VPC



See also *ATM*, *VPI*, *VPL*.

VPI—Virtual Path Identifier. A VPI is an 8-bit field in the Asynchronous Transfer Mode (ATM) cell header. The VPI identifies the Virtual Path (VP) over which the system should route the cell. See also *ATM*, *CLP*, *GFC*, *HEC*, *Payload*, *PT*, *VC*, *VCI*, *VP*.

VPL—Virtual Path Link. An Asynchronous Transfer Mode (ATM) virtual link identified by the Virtual Path Identifier (VPI) field in ATM cell headers. See also *ATM*, *VPC*, *VPI.*

VPN—Virtual Private Network. A VPN is a private network that uses the Internet to carry all traffic. It can link all the offices, telecommuters, traveling employees, customers, and suppliers for a single organization. A VPN is virtual because it uses a public network but functions as a private network. Each user sees only his or her own traffic. See also *private network.*

VRouter—Virtual Router. A VRouter is a grouping of IP or IPX interfaces. Each VRouter with IP interfaces has its own associated IP routing table, IP ARP table, IP route cache, and IP address pools, and maintains its own routing and packet statistics. Each VRouter with IPX interfaces has its own associated IPX routing table, IPX ARP table, IPX service table, IPX session table, IPX address pools, IPX ping statistics, IPX traffic statistics, and IPX dial-in route tables.

Before the introduction of VRouters, a TAOS unit maintained a single IP or IPX routing table that enabled the router to reach any of its many interfaces. Each interface known to the unit required a unique address. When you set up VRouters, addresses must be unique within the VRouter's routing domain, but not necessarily within the TAOS unit. Because each VRouter maintains its own routing table, and because it knows about only those interfaces that explicitly specify the same VRouter, there is no requirement that the private networks maintain unique address spaces.

Figure 97 shows a TAOS unit transmitting data between IP interfaces by means of standard router behavior, with no VRouters operating.

Figure 97. Standard IP routing

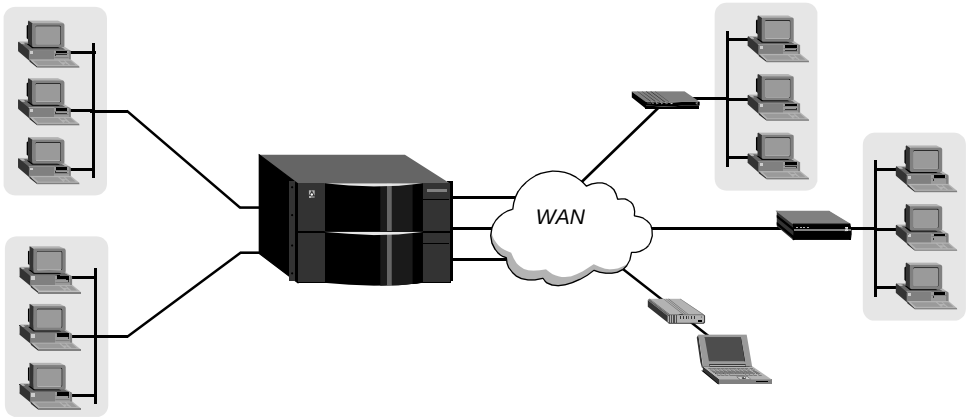
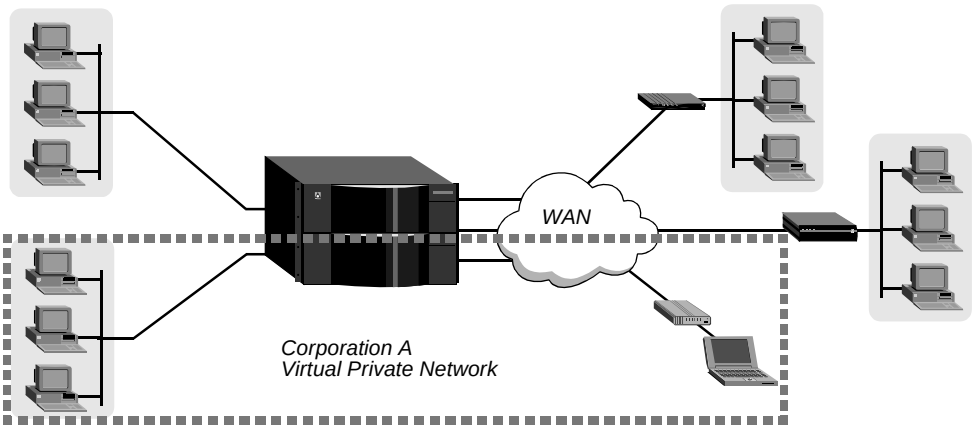


Figure 98 shows a TAOS unit with one VRouter operating for Corporation A. Interfaces related to Corporation A are grouped and handled by one VRouter, creating a Virtual Private Network (VPN) for Corporation A. Corporation A's WAN interfaces can dial in to a local TAOS unit, which can be on a public network, to reach Corporation A's private LANs.

Figure 98. Virtual IP routing



When a VRouter is defined, the main TAOS unit's router operates as the global VRouter. All interfaces that are not explicitly grouped with a defined VRouter are grouped with the global VRouter.

A VRouter supports configuration of dynamic routing protocols (such as RIP) for VRouters other than the global VRouter. For each VRouter configured on the TAOS unit, an instance of RIP is created to process routes. The new instance of RIP sends and receives update packets only on the interfaces associated with its particular VRouter and manipulates only that VRouter's routing table. A default instance of RIP is always created for the global VRouter.

You can configure and manage Domain Name System (DNS) information separately for each VRouter, completely segmenting the VRouter's DNS information from any other hosts.

See also *ARP*, *DNS*, *IP routing*, *IP routing table*, *RIP*, *VPN*.

VSA support—Vendor-Specific Attribute support. VSA support is a feature that enables companies to extend RADIUS operations without leading to possible attribute collisions (two attributes with the same type number but different meanings).

RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*, specifies methods of handling vendor extensions and of encrypting and decrypting the User-Password value. The Ascend-legacy implementation of these functions does not conform to the RFC-defined methods. Ascend extended RADIUS operations by adding Ascend vendor attributes, such as Ascend-Xmit-Rate, and used its own Ascend algorithm for User-Password encryption.

The current TAOS software ensures RADIUS RFC compliance with support for the Vendor-Specific Attribute (VSA) and the RFC-defined User-Password encryption algorithm. Lucent Technologies maintains backward compatibility by making VSA compatibility mode configurable. However, new attributes (attributes of Type 91 or lower) are available only in VSA compatibility mode. Earlier attributes (attributes of Type 92 or higher) are available in both VSA compatibility mode and the default mode, which is compatible with older implementations.

VSA support accommodates three formats: standard RFC, 8-bit VSA, and 16-bit VSA. All standard RFC 2058 attributes use the following format:

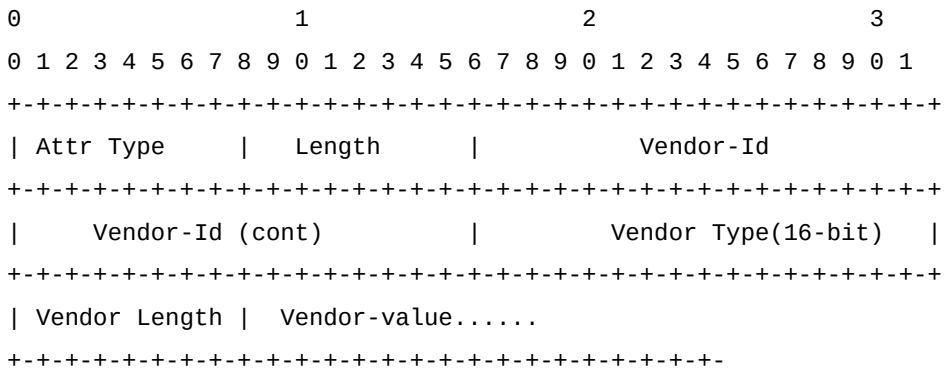
```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Attr Type     |   Length      |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

If the Attr Type value is not Vendor-Specific, the system uses the standard RFC format to decode the attribute.

When you use the 8-bit VSA format, Attr-Type is set to Vendor-Specific (26) and Vendor-Id is set to Ascend-Vendor-Id (529). Following is the 8-bit VSA format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Attr Type     |   Length      |           Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Vendor-Id (cont)          | Vendor Type(8)|  Vendor length|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Vendor-value......
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Following is the 16-bit VSA format:



Consider the following:

- Attr-Type is set to Vendor-Specific (26).
- Vendor-Id is set to Lucent-Vendor-Id (4846).
- Vendor Length is set to the octet count of Vendor Type, Vendor Length, and Vendor-value.

At this time, only NavisRadius supports 16-bit VSAs.

Note: Some vendors have interpreted RFC 2138 to allow packing more than one vendor attribute in a single VSA. Lucent Technologies does not support this use. A TAOS unit sends a single vendor attribute per VSA. If it receives a VSA that contains more than one vendor attribute, it recognizes the first vendor attribute and ignores the rest.

See also *attribute*, *RADIUS*.

VSU—Video Service Unit. Part of the Multiband product, a VSU can be used as a dual-56 CSU/DSU, and can be upgraded to a 384Kbps multiplexer. See also *Multiband*™.

VT100—An ASCII-character data terminal, consisting of a screen and keyboard. Manufactured by Digital Equipment Corporation (DEC), the VT100 has become an industry standard data terminal. VT100 emulation software enables a standard PC to act as a VT100 terminal. See also *terminal emulator*.

W

WAN—Wide Area Network. A WAN is an internetwork of devices, generally consisting of several networks distributed over a wide geographic distance, connected by telephone lines, and using different hardware platforms and encapsulation protocols. See also *internetwork*.

WAN connection—A connection between two end points over a WAN, as opposed to a local connection over a serial or Ethernet link. See also *WAN*.

WAN interface—The port, on a TAOS unit, that is connected to a WAN line. See also *WAN*.

WAN port—A T1 or E1 port that provides a point-to-point connection between the TAOS unit and another device. See also *E1 line*, *T1 line*.

warmboot—A reboot performed while the operating system is running. Compare with *coldboot*.

warmstart—The process by which a TAOS unit reinitializes itself in such a way that the configuration of the SNMP manager or the system itself is not altered. Compare with *coldstart*.

watchdog spoofing—A method of imitating a return session-keepalive packet. An IPX server sends session-keepalive packets to clients who must return the packet to keep a session active. A TAOS unit can reply to NetWare Core Protocol (NCP) watchdog packets on behalf of clients on the other side of a bridge, causing the IPX server to sense that the link is still active. Compare with *DHCP spoofing*, *IP address spoofing*, *IPX spoofing*, *SPX spoofing*. See also *IPX server*, *NCP*.

Wide Area Network—See *WAN*.

Window-control Operation based on Reception Memory Automatic Retransmission Request—See *WORM-ARQ*.

Windows Internet Name Service—See *WINS*.

wink—On a telephone line, a signal made up of an on-hook/off-hook/on-hook transition.

wink-start signaling—A signaling method in which the Customer Premises Equipment (CPE) signals an off-hook condition by sending a pulse to the Central Office (CO). Compare with *ground-start signaling*, *loop-start signaling*.

WINS—Windows Internet Name Service. WINS is a Microsoft product that manages the mapping between resource names and IP addresses. The Domain Name System (DNS) service used on the Internet cannot dynamically map IP addresses to local resource names. Through dynamic database updates, WINS lets a user gain access to network resources by means of user-friendly names, rather than by means of IP addresses.

wireless modem—A modem that uses radio transmission technology to transmit data between remote locations. A wireless modem is often used by mobile clients in locations where access to a landline connection is not feasible. See also *wireless technology*.

wireless technology—A communications system in which electromagnetic waves carry the signal through space. Examples of wireless equipment include cellular telephones, pagers, the cordless mouse, and wireless transceivers for connecting to the Internet. See also *wireless modem*.

wiring hub—See *hub*.

WORM-ARQ—Window-control Operation based on Reception Memory Automatic Retransmission Request. A technology that maintains transmission quality for Personal Digital Cellular (PDC) wireless phones in Japan. See also *PDC*.

X

X.3—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) recommendation that defines the user facilities available on all X.25 networks. See also *facility*, *X.25*.

X.3 profile—A complete set of X.3 parameters for Data Terminal Equipment (DTE) on an X.25 network. See also *DTE*, *X.25*.

X.21—A set of connector, electrical, and dialing specifications for the synchronous interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) on a digital network. See also *DCE*, *DTE*.

X.21bis—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that specifies the Physical-layer protocol for communication between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) on an X.25 network. X.21bis is nearly identical to RS-232. See also *DCE*, *DTE*, *RS-232*, *X.25*.

X.25—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) protocol that enables users to transmit information over a packet-switched network. X.25 enables remote devices to communicate with one another across high-speed digital links without the expense of individual dedicated lines. The X.25 protocol handles both high-volume data transfers and interactive use of host machines. As a full-duplex, connection-oriented protocol, X.25 uses Virtual Circuits (VCs) and provides services such as multiplexing, in-sequence delivery, transfer of addressing information, segmenting and reassembly, flow control, transfer of expedited data, error control, reset, and restart. Allocation of logical channels can be either static, using a Permanent Virtual Circuit (PVC), or dynamic, using a Switched Virtual Circuit (SVC).

X.25 uses the first three layers of the OSI model. The Physical layer implements several standards, such as V.35, RS-232 and X.21bis. The Data Link layer uses an implementation of Link Access Procedure, Balanced (LAPB) and provides an error-free link between two connected devices. The Network Layer uses the Packet Layer Protocol (PLP). PLP is primarily concerned with network-routing functions and the multiplexing of simultaneous logical connections over a single physical connection.

X.25 exchanges packets between local Data Terminal Equipment (DTE) and remote Data Circuit-terminating Equipment (DCE).

See also *DCE*, *digital modem*, *DTE*, *OSI Reference Model*, *PLP*, *PVC*, *SVC*, *VC*, *X.25/PAD*, *X.25/IP*, *X.25/T3POS*.

X.25/IP—Internet Protocol over X.25. A method of transporting IP packets on X.25 facilities when the circuit is established as an end-to-end X.25 connection. See also *X.25*, *X.25/PAD*, *X.25/T3POS*.

X.25/IP inactivity timer—See *inactivity timer*.

X.25/Packet Assembler/Disassembler—See *X.25/PAD*.

X.25/PAD—X.25/Packet Assembler/Disassembler. In an X.25/PAD configuration, PAD-generated packets are transported by means of the X.25 protocol. The PAD assembles data from terminals into packets for transmission to an X.25 network, and disassembles incoming packets from the network into a separate data stream for each terminal. In addition to this multiplexing function, the PAD provides a nearly error-free connection.

A TAOS unit's X.25/PAD implementation enables users to gain access to a public or private packet-switched network over a dedicated ISDN connection. When a user calls X.25/PAD through a modem, the terminal server uses a local Connection profile or a RADIUS user profile to perform authentication.

See also *packet switching*, *PAD*, *X.25*, *X.25/IP*, *X.25/T3POS*.

X.25/T3POS—X.25/Transaction Processing Protocol for Point-of-Service. X.25/T3POS is a character-oriented, frame-formatted protocol designed for an X.25 packet-switched network. The protocol provides reliable and efficient data transactions between a host device and Data Terminal Equipment (DTE). The DTE is usually a client device communicating through an asynchronous port, while the host is a mainframe communicating by means of an X.25 packet network. A TAOS unit converts data arriving from the DTE to a format capable of being transmitted over a packet network. In addition, X.25/T3POS enables you to send data over the ISDN D channel while continuing to send traffic over both B channels. See also *asynchronous transmission*, *B channel*, *D channel*, *DTE*, *X.25*, *X.25/PAD*, *X.25/IP*.

X.25/Transaction Processing Protocol for Point-of-Service—See *X.25/T3POS*.

X.29—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that defines the interface for the exchange of control information and user data over a packet-switched network between Data Terminal Equipment (DTE) and a Packet Assembler/Disassembler (PAD). See also *DTE*, *PAD*.

X.32—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that defines the interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for devices connecting to a Public Data Network (PDN) by means of an ISDN link, a Public Switched Telephone Network (PSTN), or a Circuit-Switched Public Data Network (CSPDN). See also *CSPDN*, *DCE*, *DTE*, *ISDN*, *PSTN*.

X.75—The International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard for connecting packet-switched networks. See also *packet switching*.

X.121—An International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) standard that specifies the addressing conventions for any Data Terminal Equipment (DTE) connected to an X.25 network. See also *DTE*, *X.25*.

xDSL—A term denoting all types of Digital Subscriber Line (DSL) implementations. See also *ADSL*, *DSL*, *HDSL*, *IDSL*, *RADSL*, *SDSL*, *VDSL*.

Xmodem—An error-correction protocol for modems. Modems that use Xmodem transmit data in 128-byte blocks. If a modem receives a block successfully, it returns a positive acknowledgment (ACK). If a modem detects an error, it sends back a negative acknowledgment (NAK), and the other modem resends the data.

Y

Yellow Alarm signal—See *RAI*.

Z

zombie route—A route that has been deleted from the main routing table. To cause neighboring routers to flush the route from their tables, a zombie route is advertised with an infinite metric (16) for a period of 2 minutes. See also *IP routing table*.

zone—(1) An AppleTalk entity that enables you to organize the services available on your network. (2) A group of H.323 gateways that register with a single gatekeeper. See also *default zone*, *gatekeeper*, *gatekeeper virtual zone*, *gateway*, *zone list*.

zone list—A list of up to 32 AppleTalk zone names for the local network. Each name consists of up to 32 characters, including embedded spaces. The characters must be in the standard printing character set, and must not include an asterisk (*). See also *default zone*, *zone*.