



NOTE: Refer to the *Cisco Dictionary of Internetworking Terms and Acronyms* for terms not included in this glossary.

A

- AAA** Authentication, authorization, and accounting. The network security services that provide the primary framework through which you set up access control on your router or access server.
- address resolution** A method for resolving differences produced by the use of computer addressing schemes. Address resolution usually specifies a method for mapping network layer (Layer 3) addresses to data link layer (Layer 2) addresses.
- agent** An object or application that can be a server, a client, or both.
- ASCII** American Standard Code for Information Interchange. An 8-bit code for character representation (7 bits plus parity).
- awk** A pattern-scanning and processing language.

B

- bash** Bourne-again shell. Interactive UNIX shell based on the traditional Bourne shell, but with increased functionality.

C

- call** Voice or data connection between two endpoints.
- CBC** Cipher block chaining. Encryption algorithm that combines an encrypted block with the previous block so that identical patterns in different messages are encrypted differently, depending upon the difference in the previous data.
- CDR** Call detail record. A record written to a database for use in postprocessing activities. This includes information such as where the call originated, start time, to whom the call was made, and when the call ended.
- CHAP** Challenge-Handshake Authentication Protocol.
- cipher** Cryptographic algorithm for encryption and decryption.
- CMIP** Common Management Information Protocol. OSI network management protocol created and standardized by ISO for the monitoring and control of heterogeneous networks.
- codec** Coder-decoder. Device that transforms analog voice into digital bit stream and vice-versa.

cron Clock daemon that starts a process that executes commands at a certain date and time.

crypto Encrypted information.

D

DES Data Encryption Standard. Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.

DHCP Dynamic Host Control Protocol. A protocol used to dynamically allocate and assign IP addresses. DHCP allows you to move network devices from one subnet to another without administrative attention.

dial peer An addressable call endpoint. Voice over IP allows two types of dial peer: POTS and VoIP.

dial plan Description of the dialing arrangements for customer use on a network.

directive Configuration command that controls one or more aspects of system behavior. Directives reside in the system's configuration file.

DNIS Dialed number identification service (the called number). Feature of trunk lines where the called number is identified; this called-number information is used to route the call to the appropriate service. DNIS is a service used with toll-free dedicated services whereby calls placed to specific toll-free numbers are routed to the appropriate area within a company to be answered.

DNS Domain Naming System. A system used in the Internet for translating names of network nodes into addresses.

DSL Digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. DSL is provisioned by means of modem pairs, with one modem located at a central office and the other at the customer site. Most DSL technologies do not use the whole bandwidth of the twisted pair, leaving room for a voice channel.

DTMF Dual-tone multifrequency. Tones generated when a button is pressed on a telephone, primarily used in the U.S. and Canada.

E

E1 Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

endpoint SIP or H.323 terminal or gateway. An endpoint can call and be called. It generates and terminates the information stream.

ENUM Informally, electronic number. DNS-based method for mapping phone numbers to IP addresses.

F

- forking** Splitting of an incoming call to more than one endpoint. The first endpoint to answer the call establishes the connection; the other endpoint drops the call.
- FQDN** Fully qualified domain name. Full name of a system, rather than just its host name. For example, aldebaran is a host name; aldebaran.interop.com is an FQDN.
- FTP** File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.
- FXS** Foreign exchange station. An interface that connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco's FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, key sets, and PBXs.

G

- gateway** In the IP community, an older term referring to a routing device that connects a VoIP network with PBXs and PSTN devices. Today, the term router is used to describe nodes that perform this function, and gateway refers to a special-purpose device that performs an application-layer conversion of information from one protocol stack to another.
- GKTMP** GateKeeper Transaction Message Protocol. A text-based message protocol that is used as an interface between a gatekeeper and a back-end server such as Cisco NAM.
- GUI** Graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.

H

- H.323** A standardized communication protocol for allowing dissimilar communication devices to communicate with each other. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods. H.323 provides for the following types of network endpoints: H.323 terminals, gatekeepers, MCUs, and gateways.
- HMAC** Hash-Based Message Authentication Code. A mechanism for message authentication based on the use of cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.
- HTTP** Hypertext Transfer Protocol. The protocol used by web browsers and web servers to transfer files, such as text and graphic files.
- HTTP digest** Password-based authentication method supported by Lightweight Directory Access Protocol (LDAP) servers.

I

ICMP	Internet Control Message Protocol. A network-layer Internet protocol that governs the reporting of errors and provision of other information relevant to IP packet processing.
IETF	Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards.
IP	Internet Protocol. A network-layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type-of-service (ToS) specification, fragmentation and reassembly, and security.
IPSec	IP security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer.
ISDN	Integrated Services Digital Network. A communications protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other traffic.
ISP	Internet service provider. A company that provides Internet access to other companies and individuals.
ITU	International Telecommunications Union. An organization established by the United Nations to set international telecommunications standards and to allocate frequencies for specific uses.

J

Java	An object-oriented programming language developed at Sun Microsystems to solve a number of problems in modern programming practice. Java is used extensively on the World Wide Web, particularly for applets.
JRE	Java Runtime Environment. A subset of files included in the Java Development Kit (JDK) that provides the minimum runtime for Java technology-enabled applications.

L

LCF message	Location-confirm message. Message that contains the transport address of the destination endpoint that the gatekeeper sends in response to an LRQ message.
LDAP	Lightweight Directory Access Protocol. A protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory. LDAP enables anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a “lightweight” (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.
LEC	Local exchange carrier. A telephone company that provides customer access to the world-wide public switched network through one of its central offices.
lm	License manager. Cisco SIP proxy server software that is automatically installed when the provisioning server (pserver) is installed. It handles the storage of license keys.

LNP	Local number portability. Before Signaling System 7 (SS7), 800 numbers were not portable. If a company moved, they had to get a new number. The Telecom Act of 1996 mandated that personal phone numbers should also be portable. Telcos are required to support the porting of telephone numbers within a geographic area, increasing the demands on the SS7 network.
location server	Device that processes requests (typically from a redirect or proxy server) to provide information about the possible location of a target end user.
LRJ message	Location-reject message. Message that a gatekeeper sends to reject an LRQ message.
LRQ message	Location-request message. Message that an endpoint sends to request that a gatekeeper provide address translation.

M

MGC	Media gateway controller. A device that provides control of media and signaling gateways.
MGCP	Media Gateway Control Protocol. Protocol that helps bridge the gap between circuit-switched and IP networks. It combines Internet Protocol Device Control (IPDC) and Simple Gateway Control Protocol (SGCP), and allows software programs to exert external control and management of data communications devices or media gateways at the edges of multiservice packet networks.
MIB	Management Information Base. Database of network management information that is used and maintained by means of a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved, usually through a GUI -based network-management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
MySQL	Database used to store and access provisioning system and subscriber feature data.

N

NAM	Network application manager. A NAM contains a small configuration that allows it to directly route a subset of calls and dispatch the other requests.
name mapping	The process of associating a name with a network location.
NAPTR record	Naming-authority pointer record. Specifies a regular-expression-based rewrite rule that converts an existing string into a new domain label or uniform resource identifier (URI). This conversion enables the use of DNS to look up services for a variety of resource names that are not in domain-name syntax.
NAT	Network Address Translation. Internet standard for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
NTP	Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. NTP is capable of synchronizing distributed clocks within milliseconds over long time periods.

P

PBX	Private branch exchange. Digital or analog telephone switchboard located on the subscriber premises and used to connect private and public telephone networks.
PDU	Protocol data unit. Another term for packet.
PEM	Privacy-enhanced mail. Internet e-mail that provides confidentiality, authentication, and message integrity by means of various encryption methods. Not widely deployed in the Internet.
PID	Protocol identifier. Field in a Call Request Packet message sent to an ISP host.
POTS	Plain old telephone service. Basic telephone service supplying standard single-line telephones, telephone lines, and access to the public switched telephone network (PSTN).
proxy server	Server that initiates requests on behalf of and receives requests from a client.
pserver	Provisioning server. The main server used by the Cisco SPS GUI-based provisioning system.
PSTN	Public switched telephone network. General term referring to the variety of telephone networks and services in place worldwide. Sometimes called POTS.

Q

QoP	Quality of protection: authentication only, authentication and integrity, or both.
------------	--

R

RADIUS	Remote Authentication Dial-In User Service. An authentication and accounting system used by many internet service providers.
RAS	Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signaling performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
redirect server	Server that receives SIP requests from a client, strips out the address in the request, checks its address tables for any other addresses that might be mapped to the one in the request, and then returns the results of the address mapping to the client.
registrar server	Server that accepts REGISTER requests from user-agent clients (UACs) for registration of their current location. Registrar servers are often colocated with proxy or redirect servers.
RFC	Request for comments. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.
RPC	Remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RPM	A Linux command-line-driven package-management system capable of installing, uninstalling, verifying, querying, and updating computer software packages.
RPMS	Resource pool manager server. Server that enables telephone companies and Internet service providers to count, control, manage, and provide accounting data for shared resources for wholesale Virtual Private Dial-Up Network (VPDN) and non-VPDN dial network services across one or more network access server (NAS) stacks.
RR message	Ready-to-receive message.
RSA	Rivest, Shamir, and Adelman, inventors of the RSA public-key cryptographic system for encryption and authentication.
RSVP	Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.
RTCP	RTP Control Protocol. Protocol that monitors the quality of service (QoS) of an IPv6 RTP connection and conveys information about the on-going session.
RTP	Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.
RTSP	Real Time Streaming Protocol. Protocol that enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds such as live audio and video and stored content such as prerecorded events. RTSP is designed to work with established protocols such as RTP and HTTP.
<hr/> S	
SAP	Session Announcement Protocol. A protocol used to assist in the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants.
SDP	Session Description Protocol. A protocol used to describe the characteristics of multimedia sessions for the purpose of session announcement, session invitation, and other forms of multimedia session initiation.
sed	Stream editor. A software program that reads text files and makes editing changes according to a script of editing commands.
SES	Severely errored second. A second during which the bit error ratio is greater than a specified limit and transmission performance is significantly degraded.
SHA-1	Secure Hash Algorithm 1. An algorithm that takes a message of fewer than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
signaling	Process of sending a transmission signal for purposes of communication.

SIP	Session Initialization Protocol. A protocol that offers many of the same architectural features as H.323, but relies on IP-specific technologies such as DNS. It also incorporates the concept of fixed port numbers for all devices and allows for the use of proxy servers.
sipd	SIP proxy server. A server that handles all call processing and SIP messages.
SNMP	Simple Network Management Protocol. A network management protocol used in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
spa	SIP provisioning agent. Agent that resides on a Cisco SPS farm member and handles requests that the provisioning server gets from the GUI-based provisioning system. It receives requests from the provisioning server, accesses and updates (as needed) the SIP directives (sipd.conf) file, and provides feedback, by way of the provisioning server, to the GUI.
SRV record	Server record. Record that allows administrators to use several servers for a single domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a specific domain and receive the names of any available servers.
SSL	Secure Socket Layer. Encryption technology for the web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

T

T1	Digital WAN carrier facility. T1 carries DS-1 formatted data at 1.544 Mbps through the telephone-switching network. T1 is the North American equivalent of an E1 line.
TCB	Transaction control block. A data structure in which Cisco SPS stores from which it accesses the state information associated with SIP transactions.
TCL	Toolkit Command Language. A scripting language used for gateway products both internally and externally to Cisco IOS software code.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
TLS	Transport Layer Security Protocol. An IETF protocol that offers an alternative to SSL encryption technology.

U

UA	User agent.
UAC	User-agent client. A client application that initiates a SIP request.

UAS	User-agent server. A server application that contacts the user when a SIP request is received and returns a response on behalf of the user. The response accepts, rejects, or redirects the request.
UDP	User Datagram Protocol. A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol for the exchange of datagrams without acknowledgments or guaranteed delivery. It requires that error processing and retransmission be handled by other protocols.
URI	Uniform resource identifier. Type of formatted identifier that encapsulates the name of an Internet object and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces.
URL	Uniform resource locator. Type of formatted identifier that describes the access method and the location of an information resource object on the Internet.

V

VoIP	Voice over IP. Technology that makes it possible to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network.
VSA	Vendor-specific attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

X

XML	Extensible Markup Language. A standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures. Information structures define the type of information—for example, subscriber name or address—not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats.
------------	--

