



GLOSSARY

A

- Access point** A device that bridges the wireless link on one side to the wired network on the other.
- Analog Channel** A circuit-switched communication path intended to carry 3.1 KHz audio in each direction.
- ARP** Address Resolution Protocol is the TCP/IP protocol that translates an Internet address into the hardware address of a network interface card.
- ATM** Asynchronous Transfer Mode is a virtual circuit, fast packet technology. Traffic of all kinds (data, voice, video) is divided into 53-byte cells and conducted over very high speed media.
- ATO** Adaptive Time Out is the time that must elapse before an acknowledgment is considered lost. After a time out, the sliding window is partially closed and the ATO is backed off.

C

- Call** A connection or attempted connection between two terminal end points on a PSTN or ISDN; for example, a telephone call between two modems.
- CHAP** Challenge Authentication Protocol is a PPP cryptographic challenge/response authentication protocol in which the clear text password is not passed in the clear over the line.
- CLID** Calling Line ID indicates to the receiver of a call, the phone number of the caller.
- CM** Cable Modem is usually a modem with an RF (cable) interface on one side and an Ethernet interface on the other. A cable modem might also have a telephone interface for “telco return,” which is used when only downstream capability exists in the cable plant.
- CNR** Cisco Network Registrar—A network management application which includes a DHCP server and a DNS server.
- Community String** A string used to authenticate the trap message sender (SNMP agent) to the trap recipient (SNMP management station).
- Control Messages** Control messages are exchanged between LAC, LNS pairs, and operate in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.
- CSG** Cable Systems Group is a billing systems company.
- CSR** Customer Service Representative—the person you call to activate or obtain service for your account.

C

- CSU/DSU** Channel Service Unit/Data Service Unit isolates your network from your exchange carrier's network. It also receives the timing, low-level framing information, and data passed from the termination point. CSU/DSUs are specific to the general circuit type.
- Customer** A user of an ISP or an enterprise. The provider offers the customer MPLS VPN service. The enterprise provides the customer remote user access to various sites. In the case of ISPs, MPLS BPN provides a scalable wholesale access/open access solution.

D

- DAP** Directory Access Protocol is a heavyweight protocol that runs over a full OSI stack and requires a significant amount of computing resources to run.
- Data Source** Sets of data and their associated environments which include operating system, DBMS, and network platforms used to access the DBMS that an application wants to access.
- DHCP** Dynamic Host Configuration Protocol—a protocol that describes the service of providing and managing IP addresses to clients on a network.
- DHCP Client** The IOS DHCP client used to generate requests for host addresses and subnets for non-PPP clients.
- DHCP Proxy Client** The IOS DHCP client used to request an address for a PPP user from a DHCP server.
- Dial Use** Dial Use is an end-system or router attached to an on-demand PSTN or ISDN, which is either the initiator or recipient of a call.
- Digital Channel** Digital Channel is a circuit-switched communication path that is intended to carry digital information in each direction.
- DNIS** Dialed Number Information String is an indication to the receiver of a call as to what phone number the caller used to reach it.
- Driver Manager** A special library that manages communication between applications and drivers. Applications call ODBC API functions in the driver managers which load and call one or more drivers on behalf of the applications.

E

- EAP** Extensible Authentication Protocol is a framework for a family of PPP authentication protocols, including cleartext, challenge/response, and arbitrary dialog sequences.

F

- FT** Field Technician is someone who installs your cable modem in your house.
- Frame Relay** Frame Relay is a cost-effective, lightweight, many-to-many, medium-speed, virtual network, link-layer technology.

I

- ISDN** Integrated Services Digital Network enables synchronous PPP access.
- ISP** Internet Service Provider is a company that provides Internet connectivity.

H

- HDLC** High-level Data Link Control is both a point-to-point and multiparty link-layer technology. HDLC provides reliable, acknowledged transfer across dedicated links.

L

- L2TP Access Concentrator (LAC)** LAC is a device attached to one or more PSTN or ISDN lines capable of PPP operation and of handling the L2TP protocol. The LAC needs only to implement the media over which L2TP is to operate to pass traffic to one or more LNSs. It may tunnel any protocol carried within PPP.
- LAN** Local Area Network consists of all of the components that create a system up to a router. These components include cables, repeaters, bridges, and software up to the network layer.
- LDAP** Lightweight Directory Access Protocol provides a standard way for Internet clients, applications, and WWW servers to access directory information across the Internet such as user names, e-mail addresses, security certificates, and other contact information.
- LEAP** Light Extensible Authentication Protocol—
- LLC** Logical Link Control is an interface that defines several common interfaces between higher-level protocols (for example, IP) and the networks they ride upon (for example, Ethernet, Token Ring, and others).
- L2TP Network Server (LNS)** An LNS operates on any platform capable of PPP termination. The LNS handles the server side of the L2TP protocol. Since L2TP relies only on the single media over which L2TP tunnels arrive, the LNS may have only a single LAN or WAN interface, yet still be able to terminate calls arriving at any LAC's full range of PPP interfaces (async, synchronous ISDN, V.120, etc.).

M

- MIB** Management Information Base—Database of network management information used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands. MIB objects are organized in a tree structure that includes public and private branches.
- MPLS** Multi-Protocol Label Switching—
- MPLS VPN** MPLS-based Virtual Private Networks
- MSO** Multiple System Operators are typically cable companies that provide Internet access for regional independent operators.

N

- NAS** Network Access Server is a device providing temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines. A NAS operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers.
- In PPTP terminology, this is referred to as the PPTP Access Concentrator (PAC). In L2TP terminology, the NAS is referred to as the L2TP Access Concentrator (LAC).
- NCP** Network Control Protocol is responsible for negotiating the protocol-specific particulars of the point-to-point protocol (PPP) link.
- Network Access Identifier** In order to provide for the routing of RADIUS authentication and accounting requests, the UserID field used in PPP and in the subsequent RADIUS authentication and accounting requests, known as the Network Access Identifier (NAI), may contain structure. This structure provides a means by which the RADIUS proxy locates the RADIUS server that is to receive the request. This same structure may also be used to locate the tunnel end point when domain-based tunneling is used.

O

- ODBC** Open Database Connectivity—a standard set of application programming interface (API) function calls (supported by Microsoft and in general use) that can be used to access data store in both relational and non-relational database management systems (DBMSs).
- ODBC Driver** Processes ODBC function calls, submits SQL requests to specific data source, and returns results to applications. ODBC drivers for specific types of data files, including database files, spreadsheet files, and text fields, are available from Microsoft Corporation.

P

packet	A block of data in a standard format for transmission.
PAP	Password Authentication Protocol is a simple PPP authentication mechanism in which a cleartext username and password are transmitted to prove identity.
Payload	The contents of a request packet.
PDU	Protocol Data Unit—An SNMP compliant request, response, or trap message.
PE Router	Provider Edge router—a router located at the edge of the provider’s MPLS core network.
POP	Point of Presence is the dial-in point or connection point for users connecting to an ISP.
PPD	Packet Processing Delay is the amount of time required for each peer to process the maximum amount of data buffered in their offered receive packet window. The PPD is the value exchanged between the LAC and LNS when a call is established. For the LNS, this number should be small. For an LAC supporting modem connections, this number could be significant.
PPP	Point-to-Point Protocol—a multiprotocol and includes UDP, Frame Relay PVC, and X.25 VC.
Profile	A collection of one or more attributes that describe how a user should be configured; for example, a profile may contain an attribute whose value specifies the type of connection service to provide the user, such as PPP, SLIP, or Telnet. Profiles can be set up for a specific user or can be shared amongst users.
Provider	Service Provider—A provider who operates the access networks and MPLS backbone and provides MPLS VPN service on the backbone.
PSTN	Public Switched Telephone Network enables async PPP through modems.

Q

Quality of Service (QoS)	A given Quality of Service level is sometimes required for a given user being tunneled between an LNS-LAC pair. For this scenario, a unique L2TP tunnel is created (generally on top of a new SVC) and encapsulated directly on top of the media providing the indicated QoS.
---------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

R

RAC Client	The IOS DHCP client used to generate requests for host addresses and subnets for non-PPP clients.
RADIUS	Remote Authentication Dial-In User Service. The RADIUS protocol provides a method that allows multiple dial-in Network Access Server (NAS) devices to share a common authentication database.
RADIUS Client	A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. A RADIUS server can act as a proxy client to other RADIUS servers.

R

RADIUS Dictionary	The RADIUS dictionary passes information between a script and the RADIUS server, or between scripts running on a single packet.
RADIUS Proxy	In order to provide for the routing of RADIUS authentication and accounting requests, a RADIUS proxy may be employed. To the NAS, the RADIUS proxy appears to act as a RADIUS server, whereas to the RADIUS server the proxy appears to act as a RADIUS client.
RADIUS Server	A server that is responsible for receiving user connection requests, authenticating the user, and then returning all of the configuration information necessary for the client to deliver the service to the user.
RAS	Remote Access Services. See RADIUS Client.
Remote DHCP Server	Usually a DHCP server in the service provider's networks, however it might also be a DHCP server in the customer's VPN.
Remote Server	A server that has been registered with the user interface, which can later be referenced as a proxy client or as the method to perform a service; for example, a remote RADIUS server can be specified to act as a proxy client.
REX	RADIUS EXtension allows you to write C and C++ programs to affect the behavior of Cisco Access Registrar.
Roaming	The ability to connect to a NAS that is not your normal POP (Point of Presence) and have the Access-Request redirected to your normal RADIUS server. The ability to use any one of multiple Internet server providers, while maintaining a formal, customer-vendor relationship with only one.
Router	A network device that connects multiple network segments and forwards packets from one network to another. The router must determine how to forward a packet based on addresses, network traffic, and cost.
Routing Tables	A table that lists all of the possible paths data can take to get from a source to a destination. Depending on how routers are configured, they may build their tables dynamically by trading information with other routers, or they may be statically configured in advance.
RTT	Round-Trip Time is the estimated round-trip time for an Acknowledgment to be received for a given transmitted packet. When the network link is a local network, this delay will be minimal (if not zero). When the network link is the Internet, this delay could be substantial and vary widely. RTT is adaptive; it adjusts to include the PPD (Packet Processing Delay) and whatever shifting network delays contribute to the time between a packet being transmitted and receiving its acknowledgment.

S

SAP	Service Access Points (source and destination) identify protocols from which a packet has come and to which a packet must be delivered.
Script	Instructions that are run in the context of a RADIUS client/server session. Scripts can be specified for servers, clients, vendors, and services. A script can be used as an incoming script, an outgoing script, or both. Incoming scripts are executed during the Access-Request portion of a dial-in session. Outgoing scripts are executed during the Access-Accept portion of a dial-in session. Scripts are referenced within the User Interface by name. Scripts can be source code for a scripting language or a binary file.

S

Service	A means of specifying the method to use to perform a function. A service can be specified for the following functions: authentication, authorization, accounting, and authentication-authorization. For example, a service can specify that authentication be performed using the local database, or a service can specify that accounting be supported by logging information to a file.
Services	Three default services are referenced by the server configuration and when processing scripts. They are Default Authentication Service, Default Authorization Service, and Default Accounting Service. Each service has a type and (if it is using remote servers) an ordered list of servers to use.
Session	Each service provided by the NAS to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. Depending on NAS support capabilities, a user may have multiple sessions in parallel or in series.
SHA-1	Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse.
Shared Secret	Used to authenticate transactions between the client and the RADIUS server. The shared secret is never sent over the network.
Shared Use Network	An IP dial-up network whose use is shared by two or more organizations. Shared use networks typically implement distributed authentication and accounting in order to facilitate the relationship amongst the sharing parties.
Silently Discard	RADIUS discards the packet without further processing. The server logs an error, including the contents of the silently discarded packet, and records the event in a statistics counter.
SLIP	Serial Line Internet Protocol is TCP/IP over direct connections and modems, which allows one computer to connect to another or to a whole network.
SMDS	Switched Multi-megabit Data Service is a high-speed Metropolitan-Area Networking technology that behaves like a LAN.
SSHA	Netscape's (iPlanet) enhancement of the SHA-1 algorithm which includes <i>salted</i> password data.
SNAP	SubNetwork Access Protocol is used when a SAP definition does not exist for the encapsulated user data protocol.
SSL	Secure Socket Layer is the protocol defined by Netscape that is used for encryption and authentication between two Internet entities. It uses public/private key certificates instead of shared secrets.
SVC	Switched Virtual Circuit is an L2TP-compatible media on top of which L2TP is directly encapsulated. SVCs are dynamically created, permitting tunnel media to be created dynamically in response to desired LNS-LAC connectivity requirements.

T

- TACACS** Terminal Access Controller Access Control System, a an authentication server that validates user IDs and passwords, thus controlling entry into systems.
- Telnet** A service that lets you log in to a system over a network just as though you were logging in from a remote character terminal attached to the system. It is commonly used to provide an Internet service that is exactly the same as the one you would get if you dialed into the system directly with a modem.
- Trap** A network message of a specific format issued by an SNMP entity on behalf of a network management agent application. A trap is used to provide the management station with an asynchronous notification of an event.
- Tunnel** A tunnel is defined by an LNS-LAC pair. The tunnel carries PPP datagrams between the LAC and the LNS; many sessions can be multiplexed over a single tunnel. A control connection operating in band over the same tunnel controls the establishment, release, and maintenance of sessions and of the tunnel itself.
- Tunnel Network Server** A server that terminates a tunnel. In PPTP terminology, this is known as the PPTP Network Server (PNS). In L2TP terminology, this is known as the L2TP Network Server (LNS).

U

- UDP** User Datagram Protocol, a data packet protocol.
- User List** The list of users registered for dial-in access.
- User Record** The UserRecord contains all the information that needs to be accessed at runtime about a particular user. This enables it to be read in one database operation in order to minimize the cost of authenticating the user. The UserRecord is stored as an encrypted string in the MCD database, because it contains the user's password, amongst other things.
- Users** Users are represented by entities in specific UserLists. See User Record.

V

- Vendor** Each NAS has a vendor associated with it. A vendor may specify attributes for the NAS that are not part of the standard specification.
- VHG** Virtual Home Gateway—a Cisco IOS component that terminates PPP sessions. It is owned and managed by the service provider on behalf of its customer to provide access to remote users of that customer's network. a single service provider device (router) may host multiple VHGs of different customers. a VHG may be dynamically brought up and down based on the access pattern of the remote users. Note that there is no single IOS feature called the VHG; it is a collection of function and features (PPP, virtual profiles, VRFs, etc.).

V

- VPN** Virtual Private Network is a way for companies to use the Internet to securely transport private data.
- VRF** Virtual routing and forwarding. A per VPM routing table on the PE router. Each VPN instantiated on that PE router has its own VRF.

X

- X.25** A reliable public data network technology consisting of private virtual circuits, virtual calling, and per-packet charging.
- X.500** Defines the Directory Access Protocol (DAP) for clients to use when contacting directory servers. DAP is a heavyweight protocol that runs over a full OSI stack and requires a significant amount of computing resources to run.

