GLOSSARY

A

ADE Application Deployment Engine.

C

CDP Cisco Discovery Protocol. A proprietary tool that network administrators use to access a summary of protocol and address information about other devices that are directly connected to the device initiating the command.

Cisco Discovery Protocol runs over the data-link layer that connects the physical media to the upper-layer protocols. Because Cisco Discovery Protocol operates at this level, two or more Cisco Discovery Protocol devices that support different network layer protocols (for example, IP and Novell IPX) can learn about each other.

Physical media that supports the Subnetwork Access Protocol (SNAP) encapsulation connect Cisco Discovery Protocol devices. These can include all LANs, Frame Relay, and other WANs, and ATM networks.

Cisco Discovery Protocol *See* CDP.

CLI command-line interface. An interface through which the user can interact with the software operating system by entering commands and optional arguments.

client Node or software program that requests services from a server. For example, the Secure Shell (SSH) client. *See also* server.

command-line interface *See* CLI.

community string A text string that acts as a password, which is used to authenticate messages sent between a management station and an IP Transfer Point (ITP) that contains an SNMP agent. The community string sends in every packet between the manager and the agent.

D

DNS Domain Name System. DNS associates various sorts of information with so-called domain names; most importantly, it serves as the "phone book" for the Internet: it translates human-readable computer hostnames (for example, *en.wikipedia.org*) into the IP addresses that networking equipment needs for delivering information. It also stores other information, such as the list of mail exchange servers that accept email for a given domain. By providing a worldwide keyword-based redirection service, the DNS is an essential component of contemporary Internet use.

DNS name Initial name of a node.

domain name The style of identifier—a sequence of case-insensitive ASCII labels separated by dots (.) (for example, *bbn.com.*)—defined for subtrees in the Internet DNS [R1034] and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

Domain Name System *See* DNS.

F

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

H

host Computer system on a network. Similar to the term node; except that host usually implies a computer system, whereas node generally applies to any network system, including access servers and ITPs.

hostname The name of the operating system's server or computer that contains the major program files.

I

IP Internet Protocol. Network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.

IP address A 32-bit address assigned to hosts by using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and written as 4 octets separated by periods (.) (dotted-decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. For routing, the network and subnetwork numbers stay together, while the host number addresses an individual host within the network or subnetwork. A subnet mask extracts network and subnetwork information from the IP address.

M

MIB Management Information Base. A directory listing information that is used and maintained by the network's management protocol of a network, such as SNMP.

N

name server A name server is a computer server that implements a name-service protocol. It normally maps a computer-usable identifier of a host to a human-usable identifier for that host. For example, a DNS server might translate the domain name *en.wikipedia.org* to the IP address 145.97.39.155.

Network Time Protocol *See* NTP.

NTP Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. NTP is designed particularly to resist the effects of variable latency (jitter).

NTP is one of the oldest Internet protocols still in use (since before 1985). NTP was originally designed by Dave Mills of the University of Delaware, who still maintains it, along with a team of volunteers.

NTP is not related to the much simpler DAYTIME (RFC 867) and TIME (RFC 868) protocols.

P

port In IP terminology, an upper-layer process that receives information from lower layers. Each numbered port associates with a specific process. For example, SMTP associates with port 25.

S

Secure Shell *See* SSH.

server An application or device that performs services for connected clients as part of a client-server architecture. A server application, as defined by RFC 2616 (HTTP/1.1), is "an application program that accepts connections in order to service requests by sending back responses." Server computers are devices designed to run such an application or applications, often for extended periods of time, with minimal human direction. Examples of servers include web servers, email servers, and file servers.

See also client.

Simple Network Management Protocol *See* SNMP.

SSH Secure Shell. A network protocol in which data is exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log in to a remote machine and execute commands; but, it also supports tunneling, forwarding arbitrary TCP ports, and X Window System (X11) connections. It can transfer files by using the associated SSH File Transfer Protocol (SFTP) or Secure Copy (SCP) protocols.

An SSH server, by default, listens on the standard TCP port 22. An SSH client program is typically used for establishing connections to an sshd daemon accepting remote connections. Both are commonly present on most modern operating systems. Proprietary, freeware, and open-source versions of various levels of complexity and completeness exist.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMPv1 SNMPv1 is a simple request/response protocol. In the SNMPv1 framework, the network-management system issues a request, and managed devices return responses.

SNMPv2C The second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations. SNMPv2C support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2C improved error-handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: No such object, No such instance, and End of MIB view.

SNMPv3 SNMPv3 is an interoperable standards-based protocol for network management, which provides secure access to devices by a combination of authenticating and encrypting packets over the network. It has primarily added security and remote configuration enhancements to SNMP. SNMPv3 provides important security features such as message integrity that ensures packets are not tampered with in-transit, authentication that verifies messages are from a valid source, and encryption of packets that prevents snooping by an unauthorized source.

T

TCP Transmission Control Protocol. Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack.

Telnet

Telnet (TELetype NETwork). A network protocol used on the Internet or LAN connections. It was developed in 1969 beginning with RFC 0015 and standardized as IETF STD 8, one of the first Internet standards.

The term Telnet also refers to software that implements the client part of the protocol. Telnet clients have been available on most UNIX systems for many years and are available for virtually all platforms. Most network equipment and operating systems with a TCP/IP stack support some kind of Telnet service server for their remote configuration (including those based on Windows NT). Recently, Secure Shell has begun to dominate remote access for UNIX-based machines.

Most often, a user establishes a telnet connection to a UNIX-like server system or a simple network device such as a switch. For example, you might "telnet in from home to check your email at work." In doing so, you would be using a Telnet client to connect from your computer to one of your servers. When the connection is established, you would then log in with your account information and execute the operating system commands remotely on that computer, such as **ls** or **cd**.

TFTP

Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

Transmission Control Protocol

See TCP.

Trivial File Transfer Protocol

See TFTP.

U

UDI

Unique Device Identifier. Each identifiable product is an entity, as defined by the Entity MIB (RFC 2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a super entity like a stack. Most Cisco entities that are orderable products leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements: product identifier (PID), version identifier (VID), and serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." You use this identifier to order an exact replacement part.

The VID is the version of the product. Whenever a product is revised, the VID is incremented, according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. This number identifies an individual, specific instance of a product.

Unique Device Identifier

See UDI.