GLOSSARY

A

AAA — Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.

AAA client IP address — An IP address of the AAA client, used to configure the AAA client in Access Control Server (ACS) to interact with the network device. To represent multiple network devices, specify multiple IP addresses. Separate each IP address by pressing **Enter**.

AAA server — A server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).

access — The capability to get to what you need. Data access is being able to get to (usually having permission to use) particular data on a computer.

Access Control — Ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL) — A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control System (ACS) — A AAA server that performs authentication, authorization, and accounting to manage devices in a network.

Access Control Service — A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

AP — access point. The Hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point.

access policies — The policies that limit access to the ACS web interface by IP address, TCP port range, and secure socket layer (SSL).

AR — access registrar . A RADIUS-compliant, access policy server designed to support the delivery of dial, ISDN, and new services including DSL, cable with telco-return, wireless and Voice over IP

ADR — accessibility design requirements. Provides detail on how to design accessible products, web sites, and documentations

accounts The capability of ACS to record user sessions in a log file.

ACS System Administrators Administrators with different access privileges defined under the System Configuration section of the ACS web interface. They administer and manage ACS deployments in your network.

ARP address resolution protocol. A protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

AES advanced encryption standard. A Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.

anonymous (LDAP) An LDAP session is described as anonymous if no user DN or secret is supplied when initiating the session (sending the bind).

anti-virus A software program designed to identify and remove a known or potential computer virus

API application program interface. The specific methodology by which a programmer writing an application program may make requests of the operating system or another application.

applet Java programs; an application program that uses the client's web browser to provide a user interface.

ARP Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.

ARPANET Advanced Research Projects Agency Network. A pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetrical Key Exchange Asymmetric or public key cryptography is based on the concept of a key pair. Each half of the pair (one key) can encrypt information so that only the other half (the other key) can decrypt it. One part of the key pair, the private key, is known only by the designated owner; the other part, the public key, is published widely but is still associated with the owner.

attribute (LDAP) The data in an entry is contained in attribute-value pairs. Each attribute has a name (and sometimes a short form of the name) and belongs to an objectClass. The attributes characteristics are fully described by an ASN.1 definition. One or more objectClasses may be included in a Schema. Depending on the ASN.1 definition of the attribute there can be more that one attribute-value pair of the same named attribute in an entry. One (or more) attribute(s), the naming attribute or RDN will always uniquely identify an entry.

auditing The information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

authenticated (LDAP) A session is described as authenticated if a user DN and secret is supplied when initiating the session (sending the bind).

authentication The process of confirming the correctness of the claimed identity.

authenticity The validity and conformance of the original information.

authorization The approval, permission, or empowerment for someone or something to do something.

authorization profile The basic "permissions container" for a RADIUS-based network access service. The authorization profile is where you define all permissions to be granted for a network access request. VLANs, ACLs, URL redirects, session timeout or reauthorization timers, or any other RADIUS attributes to be returned in a response are defined in the authorization profile.

B

basic authentication The simplest web-based authentication scheme that works by sending the username and password with each request.

BIND Berkeley Internet Name Domain. An implementation of DNS. DNS is used for domain name to IP address resolution.

bind (LDAP) When connection is made to an LDAP server the first operation of the sequence is called a bind. The bind operation sends the dn of the entry that will be used for authentication and the password to be used. In the case of an anonymous bind both values will be NULL.

block cipher Encrypts one block of data at a time.

bridge A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

broadcast To simultaneously send the same message to multiple recipients. One host to all hosts on network.

broadcast address An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

browser A client computer program that can retrieve and display information from servers on the World Wide Web.

C

CA Signature A digital code that vouches for the authenticity of a digital certificate. The CA signature is provided by the certificate authority (CA) that issued the certificate.

cache A special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

CSS cascading style sheet. A Web page derived from multiple sources with a defined order of precedence where the definitions of any style element conflict.

CA certificate authority. An authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

certificate-based authentication The use of Secure Sockets Layer (SSL) and certificates to authenticate and encrypt HTTP traffic.

certificate Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

CGI common gateway interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

CHAP Challenge-Handshake Authentication Protocol. A protocol that uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

CHAP is an authentication technique where after a link is established, a server sends a challenge to the requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it its own calculation of the expected hash value. If the values match, the authentication is acknowledged otherwise the connection is usually terminated.

challenge-response A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

checksum A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

cipher A cryptographic algorithm for Encryption and Decryption. The method used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled, or hidden message (called ciphertext).

ciphertext The encrypted form of the message being sent. Ciphertext is data that has been encrypted. It is the output of the encryption process and can be transformed back into a readable form (plaintext) with the appropriate decryption key.

client A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

client/server Describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations.

collision Occurs when multiple systems transmit simultaneously on the same wire.

command sets Contains a set of permitted commands for TACACS+ based, per-command authorization.

community string A character string used to identify valid sources for Simple Network Management Protocol (SNMP) requests, and to limit the scope of accessible information. Ravlin units use a community string, such as a password, allowing only a limited set of management stations to access its MIB.

computer network A collection of host computers together with the sub-network or inter-network through which they can exchange data.

confidentiality The need to ensure that information is disclosed only to those who are authorized to view it.

configuration management	The process of establishing a known baseline condition and managing it.
cookie	Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.
corruption	A threat action that undesirably alters system operation by adversely modifying system functions or data.
CoS	Class of Service. A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.
countermeasure	Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.
covert channels	The means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.
CRL	certificate revocation list. A list of certificates (more accurately: their serial numbers) which have been revoked, are no longer valid, and should not be relied upon by any system user.
CRUD	Create, read, update and delete. The basic management operations that are performed on managed data
cryptanalysis	The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.
cryptographic algorithm or hash	An algorithm that employs the science of Cryptography, including Encryption algorithms, Cryptographic Algorithm or Hash, Digital Signature Algorithm (DSA), and key agreement algorithms.
cryptography	Garbles a message in such a way that anyone who intercepts the message cannot understand it.
CSV	comma-separated value. This file format is a delimited data format that has fields separated by the comma character and records separated by new lines.
CTS	Cisco Trusted Security
CUE	Common User Experience
cut-through	A method of switching where only the header of a packet is read before it is forwarded to its destination.
CRC	Cyclic Redundancy Check. Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

D

daemon A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

DES Data Encryption Standard. A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

datagram Request for Comment 1594 says, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

decapsulation The process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

decryption The process of transforming an encrypted message into its original plaintext.

denial of service The prevention of authorized access to a system resource or the delaying of system operations and functions.

device administration Capability to control and audit the administration operations performed on network devices. The network device administrator role has full access to perform the administrative operations on network devices.

dictionaries A store to configure attributes of RADIUS and TACACS+ protocols, internal users, and internal hosts.

dictionary attack An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication Allows a web client to compute MD5 hashes of the password to prove it has the password.

digital certificate An electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

digital envelope An encrypted message with the encrypted session key.

digital signature A hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

DSA digital signature algorithm. An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

(DSS Digital Signature Standard. The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

disassembly The process of taking a binary program and deriving the source code from it.

disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.

DIT directory information tree (also known as the naming context). The hierarchy of objects that make up the local directory structure. More than one DIT may be supported by an LDAP server. The Root DSE will provide this information.

DN Distinguished Name. A DN is comprised of a series of RDNs that uniquely describe the naming attributes on the path UP the DIT from the required entry to the directory root. A DN is written LEFT to RIGHT and looks something like this:

domain A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

domain name Locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

DNS Domain Name System. The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DSA Directory System Agent X.500 term for any DAP or LDAP enabled directory service e.g. an LDAP server.

DSE DSA Specific Entry An entry in a local directory server.

due diligence The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

dumpsec A security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

DLL Dynamic Link Library. A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

E

eavesdropping Listening to a private conversation which may reveal information which can provide access to a facility or network.

Egress Filtering Filtering outbound traffic.

encapsulation The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

encryption Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

entry (LDAP) The name given to a stored object in a LDAP enabled directory. Each entry has one parent entry (object) and zero or more child entries (objects). The data content of an entry consist of one or more attributes one (or more) of which is (are) used as the naming attribute (more correctly the RDN) to uniquely identify this object in the DIT.

equality (LDAP) Equality defines the comparison rule of an attribute when used in a search filter that contains no wildcards, and both the content and length must be exactly the same. When wildcards are used, this is called a substring and the SUBSTR rule is used.

external identity store External databases that ACS accesses to perform credential and authentication validations for internal and external users (as defined by you within a policy).

Ethernet The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

event An observable occurrence in a system or network.

Exponential Backoff Algorithm Used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

exposure A threat action whereby sensitive data is directly released to an unauthorized entity.

extended ACLs A more powerful form of standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

EAP Extensible Authentication Protocol. A protocol for wireless networks that expands on Authentication methods used by the PPP (Point-to-Point Protocol), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and Public Key Encryption authentication.

EAP-MD5 Extensible Authentication Protocol-Message Digest 5. An EAP security algorithm developed by RSA Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.

EAP-TLS Extensible Authentication Protocol-Translation Layer Security. A high-security version of EAP that requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated. Used to create a secured connection for 802.1X by preinstalling a digital certificate on the client computer. EAP-TLS is the protocol that serves for mutual authentication and integrity-protected cipher suite negotiation and key exchange between a client and server. Both the client and the server use X.509 certificates to verify their identities to each other.

F

false rejects When an authentication system fails to recognize a valid user.

FTP File Transfer Protocol . A TCP/IP protocol specifying the transfer of text or binary files across the network.

filter Used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

filtering router An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

firewall A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

fragmentation The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

frames Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

full duplex A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

fully-qualified domain name A server name with a hostname followed by the full domain name.

G

gateway A network point that acts as an entrance to another network.

global system options Configuring TACACS+, EAP-TTLS, PEAP, and EAP-FAST runtime characteristics and generating EAP-FAST PAC.

H

hash functions Used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

header The extra information in a packet that is needed for the protocol stack to process the packet.

host Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Host-Based ID Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTTPS Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL. HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP and an additional encryption/authentication layer between HTTP and TCP.

hub A network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub. The central device in a star network, whether wired or wireless. Wireless access points act as hubs in wireless networks.

hybrid attack Builds on the dictionary attack method by adding numerals and symbols to dictionary words.

hybrid encryption An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

(HTML Hypertext Markup Language. The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

(HTTP Hypertext Transfer Protocol. The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

I

I18N Internationalization and localization are means of adapting software for non-native environments, especially other nations and cultures. Internationalization is the adaptation of products for potential use virtually everywhere, while localization is the addition of special features for use in a specific locale.

identity Whom someone or what something is, for example, the name by which something is known.

identity groups A logical entity that is associated with all types of users and hosts.

incremental backup A scheduled job that allows users to take smaller, periodic backups of the Monitoring & Report Viewer database.

integrity The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

internal identity store A database that contains the internal user attributes and credential information used to authenticate internal users and hosts.

IETF Internet Engineering Task Force . The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

(IP Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet.

IPsec Internet Protocol Security. A developing standard for security at the network or packet processing layer of network communication.

Interrupt A signal that informs the OS that something has occurred.

intrusion detection A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP address A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP flood A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP forwarding An Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP poofing The technique of supplying a false IP address.

ISO International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

ISP Internet Service Provider. A business or organization that provides to consumers access to the Internet and related services. In the past, most ISPs were run by the phone companies.

J

JRE Java Runtime Environment. A software bundle that allows a computer system to run a Java application.

K

Kerberos A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

key In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

L

Layer 2 Forwarding Protocol (L2F) An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP) An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

LDAP client LDAP Client describes a piece of software that provides access to an LDAP sever. Most standard web browsers provide limited LDAP client capabilities using LDAP URLs. LDAP browsers and web interfaces are both very common examples of LDAP clients. List of Open Source Clients.

Lightweight Directory Access Protocol (LDAP) LDAP is a networking protocol for querying and modifying directory services running over TCP/IP The LDAP protocol is used to locate organizations, individuals, and other resources such as files and devices in a network, on the public Internet or on a corporate Intranet.

Local Operations (secondary servers only) The operations performed to register or deregister a secondary server, or to replicate a secondary server and a request for a local mode from the Join a Distributed System page.

Log Configuration A system that uses logging categories and maintenance parameters that enable you to configure and store the logs generated for accounting messages, AAA audit and diagnostics messages, system diagnostics messages, and administrative audit messages.

M

MAC Address — A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

matchingRule (LDAP) — The method by which an attribute is compared in a search operation. A matchingRule is an ASN.1 definition that usually contains an OID a name (for example, caseIgnoreMatch [OID = 2.5.13.2]), and the data type it operates on (for example, DirectoryString).

MD5 — A one way cryptographic hash function.

MIB (Management Information Base) — A MIB is a formal description of a set of network objects that can be managed using SNMP (Simple Network Management Protocol).

monitoring and reports — In the ACS web interface, a drawer that contains the monitoring, reporting, and troubleshooting options.

MPPE Microsoft Point-to-Point Encryption — A protocol for encrypting data across PPP (Point-to-Point Protocol) and Virtual Private Network links.

N

name space (LDAP) — Term used to describe all DNs that lie in (or are contained within or bounded by) a given directory information tree (DIT). If the DIT root is dc=example,dc=com, then cn=people,dc=example,dc=com is said to lie in the name space but ou=people,dc=example,dc=net does not; it lies in the dc=example,dc=net name space.

naming attribute (LDAP) — A unique identifier for each entry in the directory information tree (DIT). Also known as the Relative Distinguished Name (RDN).

naming context (LDAP) — A a unique name space starting from (and including) the root Distinguished Name (DN). Also known as namingContext or directory information tree (DIT).

NAS (Network Access Server) — A single point of access to a remote resource. The NAS is meant to act as a gateway to guard access to a protected resource. This can be anything from a telephone network, to printers, to the Internet.

network device groups — A logical grouping of network devices by location and type.

network resources — A drawer that defines all network devices in the device repository that access the ACS network, including Network Device Groups (NDGs), network devices, AAA clients,, and external policy servers.

P

PAP (Password Authentication Protocol.) — PAP is a simple authentication protocol used to authenticate a user to a remote access server or Internet service provider(ISP).

PI (Programmatic Interface) The ACS PI is a programmatic interface that provides external applications the ability to communicate with ACS to configure and operate ACS; this includes performing the following operations on ACS objects: create, update, delete and read.

policy condition Rule-based single conditions that are based on policies, which are sets of rules used to evaluate an access request and return a decision.

policy element Global, shared object that defines policy conditions (for example, time and date, or custom conditions based on user-selected attributes) and permissions (for example, authorization profiles). Policy elements are referenced when you create policy rules.

port setting You can configure ACS to authenticate using different LDAP servers, or different databases on the same LDAP server, by creating more than one LDAP instance with different IP addresses or port settings.

PPP (Point-to-Point Protocol) PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet Protocol (IP) and is designed to handle others. It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

protocol A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

Proxy An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

Public Key In Cryptography a publicKey is a value provided by some designated authority as an Encryption Key that, combined with a private key derived from the public key, can be used to effectively encrypt messages andDigital Signatures.

The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).

Public Key Infrastructure (PKI) A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The Public Key infrastructure provides for a Digital Certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

R

RDN (LDAP) The Relative Distinguished Name (frequently but incorrectly written as Relatively Distinguished Name). The name given to an attribute(s) that is unique at its level in the hierarchy. RDNs may be single valued or multi-valued in which case two or more attributes are combined using '+' (plus) to create the RDN e.g. cn+uid. The term RDN is only meaningful when used as part of a DN to uniquely describe the attributes on the path UP the DIT from a selected entry (or search start location) to the directory root (or more correctly the Root DSE). More info.

referral (LDAP) An operation in which the LDAP server returns to an LDAP client the name (typically in the form of an LDAP URL) of another LDAP server that might be able to provide the information requested by the LDAP client.

Remote Authentication Dial-In User Service (RADIUS) RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

RFC (Request for Comments) A series of memoranda that encompass new research, innovations, and methodologies applicable to Internet technologies.

Role A set of typical administrator tasks, each with an associated set of permissions. An administrator can have more than one predefined role, and a role can apply to multiple administrators.

root (LDAP) The root entry (a.k.a base, suffix) is one of many terms used to describe the topmost entry in a DIT. The Root DSE is a a kind of super root.

Root DSE (LDAP) Conceptually the top most entry in a LDAP hierarchy - think of it as a super root and normally invisible i.e. not accessed in normal operations. Sometimes confused with root or base or suffix. DSE stands for DSA Specific Entry and DSA in turn stands for Directory System Agent (any directory enabled service providing DAP or LDAP access). Information about the rootDSE may be obtained in OpenLDAP by querying the OpenLDAProoDSE classobject and will provide information about protocol versions supported, services supported and the naming-context(s) or DIT(s) supported.

rootdn (LDAP) The rootdn is a confusingly named directive in the slapd.conf file which defines a superuser which can bypass normal directory access rules.

RPM (RedHat Package Manager) An RPM is a downloadable software package that is installable on Linux distributions that use RPM as their package management format.

S

SAN (Subject Alternative Name) Extension within certificate information.

Schema (LDAP) A package of attributes and object classes that are sometimes (nominally) related. The schema(s) in which the object classes and attributes that the application will use (reference) are packaged are identified to the LDAP server so that it can read and parse all that wonderful ASN.1 stuff. In OpenLDAP this done using the slapd.conf file.

search (LDAP) An operation that is carried out by defining a base directory name (DN), a scope, and a search filter.

Secure Sockets Layer(SSL) A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. SSL is a cryptographic protocol which provides secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, and other data transfers. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same. The term "TLS" as used here applies to both protocols unless clarified by context.

Security Policy A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

server A system entity that provides a service in response to requests from other system entities called clients.

service provisioning Service provisioning refers to the "preparation beforehand" of IT systems' materials or supplies required to carry out a specific activity. This includes the provisioning of digital services such as user accounts and access privileges on systems, networks and applications, as well as the provisioning of non-digital or "physical" resources such as cell phones and credit cards.

service selection policy A set of rules that determines which access policy applies to an incoming request.

Session A session is a virtual connection between two hosts by which network traffic is passed.

session (LDAP) A session occurs between a LDAP client and a server when the client sends a bind command. A session may be either anonymous or authenticated.

session conditions Custom conditions, and date and time conditions.

Session Key In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

shell profiles The basic “permissions container” for a TACACS+ based device administration policy, in which you define permissions to be granted for a shell access request.

SLA (Service Level Agreement) A SLA is that part of a service contract in which a certain level of service is agreed upon. A SLA is a formal negotiated agreement between two parties. It is a contract that exists between customers and their service provider, or between service providers. It transcripts the common understanding about services, priorities, responsibilities, guarantee, etc. It then specifies the levels of availability, serviceability, performance, operation or other attributes of the service like billing.

SNMP (Simple Network Management Protocol) A TCP/IP network protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SOAP (Simple Object Access Protocol) A lightweight XML-based protocol for exchange of information in a decentralized, distributed environment. SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.

SPML (Service Provisioning Markup Language) SPML is the open standard protocol for the integration and interoperation of service provisioning requests.

SSH(Secure Shell) A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

subtype (LDAP) LDAPv3 defines a number of subtypes at this time two have been defined binary (in RFC 2251) and lang (in RFC 2596). subtypes may be used when referencing an attribute and qualify e.g. cn;lang-en-us=smith would perform a search using US english. The subtype does not affect the encoding since UTF-8 (used for cn) allows for all language types. lang subtypes are case insensitive.

suffix (LDAP) Also known as root, base, is one of many terms used to describe the topmost entry in a DIT. The term is typically used because this entry is usually defined in the suffix parameter in a OpenLDAP's slapd.conf file. The Root DSE is a kind of super root. Suffix Naming.

system administration The role-based administrative functions performed by a group of administrators.

system configuration The role-based administrative functions performed by a group of administrators to configure system performance.

System Health Dashboard The Monitoring & Report Viewer Dashboard that provides information about the health status of associated ACS instances.

system operations A set of operations that you must perform to effectively deploy and manage the ACS servers in your network.

T

TACACS TACACS (Terminal Access Controller Access Control System) is an older Authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authenticationServer to determine whether access can be allowed to a given system. TACACS is an Encryption protocol and therefore less secure than the later TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols.

TACACS+ settings Used to configure TACACS+ runtime characteristics.

TCP/IP Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

U

UDP User Datagram Protocol. A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP)

URL Uniform Resource Locator. The unique address for a file that is accessible on the Internet.

user and identity store A repository of users, user attributes, and user authentication options.

user authentication option An option to enable or disable TACACS+ password authentication.

user attribute configuration An administrative task consisting of configuring an internal user's identity attributes.

V

VPN Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VSA Vendor Specific Attribute. A proprietary property or characteristic not provided by the standard Remote Authentication Dial-In User Service (RADIUS) attribute set. VSAs are defined by vendors of remote access servers to customize RADIUS for their servers.

W

WCS Cisco Wireless Control System us a platform designed to help enterprises design, control and monitor Cisco wireless LANs. WCS is the industry leading platform for wireless LAN planning, configuration, and management.

Web server A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

Web service A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. The web server interface is described in a machine-processable format, WSDL. Other systems interact with the Web service, typically using HTTP with an XML serialization in conjunction with other Web-related standards.

WSDL (Web Services Description Language) WSDL is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

X

X.509 A standard for public key infrastructure. X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.

XML (eXtensible Markup Language) XML is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.