Syslog Messages

Format

The following format is used for all Access/One Network syslog messages:

```
<recv-time> <code> <ip> <seqNumber:time-stamp, CloudName, subcloudName,
StackId, Module, sysName, subSystem> <source> <sw-version> <syslog message>
```

Element	Definition
recv-time	Time when the syslog message is received.
code	As defined by RFC for syslog daemons.
ip	Sender's IP address.
seqNumber	Internal sequence number (generated for all syslog messages).
time-stamp	Time when the message is generated.
Module	Module type.
source	Internal source information, containing event-module & event-type.
sw-version	Software build version number
Syslog message	Format is a string of ASCII text delimited by separators.

Subsystems

Syslog messages are assigned to the following subsystems:

- Wireless
- Security
- Management
- Others

Severity Levels

The following severity levels are assigned to syslog messages (shown here in descending order from the most severe):

- EMERGENCY
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFORM
- DEBUG

Assigning a severity level informs the system to automatically log all messages in that level, and all messages above that level (messages below the assigned level are not logged).

Message Listing

The following tables list syslog messages by subsystem.

Security Subsystem

Severity	Syslog Message
ALERT	Telnet local authentication failed.
WARNING	Super user login failed, invalid character.
WARNING	Super user login failed, invalid password.
WARNING	Telnet login failed, invalid password.
WARNING	CLI login failed, invalid password.
WARNING	Telnet login failed, invalid password.

Severity	Syslog Message
WARNING	CLI login failed, invalid password.
WARNING	Too many invalid login attempts.
NOTICE	Telnet user logged in, user:XXXXX.
NOTICE	CLI user logged in, user:XXXXX.
NOTICE	Telnet user logged out, user:XXXXX.
NOTICE	CLI user logged out, user:XXXXX.
NOTICE	Super user logged in.

Wireless Subsystem

Severity	Syslog Message
EMERGENCY	Failed to start the radio.
EMERGENCY	AP/STA features not enabled.
EMERGENCY	Error while starting the module. Wireless services disabled.
EMERGENCY	Radio interference detected on selected channel.
WARNING	Backhaul key mismatch. Putting it in RESTRICTED mode,mac:xx.xx.xx.xx.xx.xx.
ALERT	Radius authentication failed, mac:xx.xx.xx.xx.xx.xx.
ERROR	Association fails, can't find station in table, ssid:XXXXX,vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.x.
ERROR	Reassociation fails, can't find station in table, ssid:XXXXX, vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.x.
ERROR	Association fails, not authenticated, ssid:XXXXX,vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.

Severity	Syslog Message
ERROR	Reassociation fails, not authenticated, ssid:XXXXX,vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
ERROR	Association fails, already associated, ssid:XXXXX,vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
ERROR	Reassociation fails, already associated, ssid:XXXXX,vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
ERROR	Association fails, can't authenticate during scan, ssid:ssid:XXXXX, vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
ERROR	Reassociation fails, can't authenticate during scan, ssid:ssid:XXXXX, vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
ERROR	Association fails, reason:xxxx, wlanmode:xxxx, ssid:XXXXXX, vlan:[Id=x Tag=x],mac:xx:xx:xx:xx:xx:xx.
ERROR	Reassociation fails, reason:xxxx, wlanmode:xxxx, ssid:XXXXXX, vlan:[Id=x Tag=x],mac:xx:xx:xx:xx:xx:xx.
ERROR	Bad authentication transaction sequence, number:XX, type=XXXXX, mac:xx.xx.xx.xx.xx.xx.
ERROR	Authentication[1] fails, can't find station in table, mac:xx.xx.xx.xx.xx.xx.
ERROR	Authentication[1] fails, can't authenticate in scan mode, mac:xx.xx.xx.xx.xx.xx.
ERROR	Authentication[3] fails, can't find station in table, mac:xx.xx.xx.xx.xx.xx.
ERROR	Authentication[3] done, error in Tx, wlanmode:X, mac:xx.xx.xx.xx.xx.xx.
ERROR	Deauthentication requested, can't find station in table, mac:xx.xx.xx.xx.xx.xx.

Severity	Syslog Message
ERROR	Association fails, module is not ready, mac:xx:xx:xx:xx:xx:xx.
ERROR	Reassociation fails, module is not ready, mac:xx:xx:xx:xx:xx:xx.
WARNING	Authentication[3] fails, auth:shared, wlanmode:X, mac:xx.xx.xx.xx.xx.xx.
WARNING	Unsupported 802.11 authentication request, auth:LEAP, wlanmode:X, mac:xx.xx.xx.xx.xx.xx.
WARNING	Unsupported 802.11 authentication request, auth:x(hex), wlanmode:X, mac:xx.xx.xx.xx.xx.xx.
WARNING	Deauthentication fails, incorrect source, mac:xx.xx.xx.xx.xx.xx.
WARNING	Deauthentication fails, unknown source, mac:xx.xx.xx.xx.xx.xx.
WARNING	Association fails, wrong ssid, ssid:XXXXX, vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
WARNING	Reassociation fails, wrong ssid, ssid:XXXXX, vlan:[id=x tag=x], mac:xx.xx.xx.xx.xx.xx.
WARNING	NC-sel approves RESTRICTED Mode.
WARNING	Backhaul [mac:xx:xx:xx:xx:xx:xx] at if=XXXX is put to RESTRICTED mode.
WARNING	Loop is detected at if=XX. Mac:xx:xx:xx:xx:xx:xx.
NOTICE	NC-sel approves OPEN Mode.
NOTICE	Backhaul is using default cloud name. Putting it in RESTRICTED mode,mac:xx.xx.xx.xx.xx.xx.
NOTICE	AP has put backhaul in RESTRICTED mode.

Severity	Syslog Message
NOTICE	Stack ID is available, stackId:XXXXXX.
NOTICE	The unit/Radio x will operate as - Network Connect.
NOTICE	The unit/Radio x will operate as - Client Connect.
NOTICE	The unit/Radio x will switch to - Client Connect.
NOTICE	Added station, mac:xx.xx.xx.xx.xx.xx.
NOTICE	Deauthentication completed, mac:xx.xx.xx.xx.xx.xx.
NOTICE	Association with AP done, response NOT sent, wlanmode:X, ssid:XXXX, mac:xx:xx:xx:xx:xx:xx.
NOTICE	Reassociation with AP done, response NOT sent, wlanmode:X, ssid:XXXX, mac:xx:xx:xx:xx:xx:xx.
NOTICE	Loop is cleared at if=XX. mac:xx:xx:xx:xx:xx:xx.
NOTICE	WLNC link [if=XX] state is up. SSID=XX, BSSID=xx:xx:xx:xx:xx:xx:xx, Channel=XX, Wireless Mode=XXXX.
NOTICE	WLNC link [if=XX] state is down.
NOTICE	Access Point state is up.
NOTICE	Access Point state is down
NOTICE	Association done, ssid:XXXX, vlan:[Id=x Tag=x], mac:xx:xx:xx:xx:xx:xx:xx:xx.
NOTICE	Reassociation done, ssid:XXXX, vlan:[Id=x Tag=x], mac:xx:xx:xx:xx:xx:xx:xx:xx.
NOTICE	Disassociation done, mac:xx:xx:xx:xx:xx:xx.
NOTICE	Backhaul [mac:xx:xx:xx:xx:xx:xx] at if=XXXX is approved with OPEN mode.

Severity	Syslog Message
NOTICE	Authentication failed, type=XXX, reason=XXXX, mac:xx:xx:xx:xx:xx:xx.
NOTICE	Authentication done, type=XXX, mac:xx:xx:xx:xx:xx:xx.
NOTICE	Device will switch to Access Point.

Management Subsystem

Severity	Syslog Message
WARNING	Fan failed.
WARNING	Temperature alarm on.
WARNING	DHCP Bind failed.
WARNING	Image load failed.
NOTICE	xx.xx.xx.xx detected rogue device [xx:xx:xx:xx:xx:xx] with RSSI [xxxx] channel [xxxx] SSID [XXXXX].
NOTICE	Rogue device [xx:xx:xx:xx:xx:xx] detected by xx.xx.xx.xx aged out.
NOTICE	Detected Rogue Device [xx:xx:xx:xx:xx:xx].
NOTICE	Cloud is renamed to XXXXX.
NOTICE	Configuration update completed.
NOTICE	Configuration update started.
NOTICE	Selected AP at if=XX, mac:xx:xx:xx:xx:xx:xx.
NOTICE	I am the Master NC.
NOTICE	Temperature alarm off.
NOTICE	Fan is working.

Severity	Syslog Message
NOTICE	Include list updated.
INFORM	Load image file XXXXX from XXXXXX.
INFORM	Image load is done.
INFORM	Received DHCP, IP - xx.xx.xx.xx, Gateway - xx.xx.xx.xx.

Supported MIBs

MIBs that are supported with Access/One Network include the following:

Strix Private MIBs

STRIX-PRODUCTS.mib
Define the object identifiers assigned to various Strix hardware platforms.

STRIX-CONFIG-SYSTEM.mib
Configuration MIB for system wide parameters, including Usernames and Passwords, DHCP, DNS, SNTP, FTP, CoS, Trusted IPs, Syslog, and RADIUS accounting.

STRIX-CONFIG-WIFI.mib
Configuration MIB for 802.11 radio parameters, per-SSID configuration of authentication, keys and VLANs, Inventory list, Network Client and Client Connect configurations.

STRIX-MANAGEMENT.mib
Management MIB for taking actions, such as loading configurations, upgrading image, rebooting the entire network, and collecting network wide report from all devices.

STRIX-INVENTORY.mib
MIB to present and modify the inventory list of all modules in the network.

STRIX-SYSLOG-MIB.mib
MIB to present the buffered history of syslog messages generated by a module.

STRIX-MONITOR.mib
MIB to monitor radio status and statistics on a Wi-Fi module, and to report VLANs, device information, and a scanned list of access points.

STRIX-ROGUES.mib
MIB to present a list of rogue Access Points detected by Strix modules, and report the closest access points.

STRIX-ENT-TRAPS.mib
List of traps that Strix devices can generate.

STRIX-CONFIG-TRAPS.mib
Configuration MIB for enabling and disabling specific traps per trap manager.

STRIX-ACCESSONE-CAPABILITY.mib
Indicates the level of support implemented by an SNMP agent on the Access/ One Network with respect to standard MIBs.

Standard MIBs

RFC1213-MIB

IF-MIB (RFC 2233)

IP-MIB (RFC 2011)

TCP-MIB (RFC 2012)

UDP-MIB (RFC 2013)

SNMPv2-MIB (RFC 1907)

IEEE802DOT11-MIB

Contact Information

Strix Systems is located in Calabasas, California, just 45 minutes northwest of downtown Los Angeles and 45 minutes southeast of Santa Barbara.

Strix Systems, Inc.
26610 Agoura Road
Calabasas, CA 91302

Tel:	818.251.1000
Fax:	818.251.1099

Visit us at: http://www.strixsystems.com

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 wireless LAN (WLAN) specification that describes transmission through the physical layer (PHY) based on orthogonal frequency division multiplexing (OFDM), at a frequency of 5 GHz and data rates of up to 54 Mbps. See also, OFDM.

802.1D

The IEEE LAN specification for remote media access control (MAC) bridging.

802.11g

A supplement to the IEEE 802.11 wireless LAN (WLAN) specification that describes transmission through the physical layer (PHY) based on orthogonal frequency division multiplexing (OFDM), at a frequency of 2.4 GHz and data rates of up to 54 Mbps. See also, OFDM.

802.11i

A supplement to the IEEE 802.11 wireless LAN (WLAN) specification for enhanced security. It describes encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and AES Counter-Mode Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). These protocols provide replay protection, cryptographically keyed integrity checks, and key derivation based on the IEEE 802.1X port authentication standard. See also, TKIP.

802.1Q

The IEEE LAN specification for bridged virtual LANs (VLANs). See also, VLAN.

802.1X

The IEEE specification for port-based network access control. The 802.1X standard based on the Extensible Authentication Protocol (EAP) provides an authentication framework that supports a variety of methods for authenticating and authorizing network access for wired or wireless users. See also, EAP.

GL

802.11x

An IEEE specification that defines wireless LAN (WLAN) data link and physical layers. The specification includes data link layer media access control (MAC) sub-layer, and two sub-layers of the physical (PHY) layer-a frequency-hopping spread-spectrum (FHSS). See also, FHSS.

802.2

IEEE specification that describes the logical link control (LLC) encapsulation common to all 802 series LANs.

802.3

An IEEE LAN specification for a Carrier Sense Multiple Access with Collision Detection (CSMA-CD) Ethernet network. The standard describes physical media. An 802.3 frame uses source and destination media access control (MAC) addresses to identify its originator and receiver(s).

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication: open system and shared key. See also, 802.11x and authentication.

authorization

The process of deciding if device 'X' may use network service 'Y'. Trusted devices (the devices that are both authenticated and authorized) are allowed access to network services. Unknown (not trusted) devices may require further user authorization to access network services. This does not principally exclude that the authorization might be given by an application automatically. Authorization always includes authentication. See also, authentication.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power). See also, bit rate.

baud rate

The number of pulses of a signal that occur in one second. Thus, baud rate is the speed at which digital signal pulses travel.

Beacon

A uniframe system packet broadcast by the AP to keep the network synchronized. A beacon Includes the Net_ID (ESSID), the AP address, the broadcast destination addresses, a time stamp, a DTIM (Delivery Traffic Indicator Maps) and the TIM (Traffic Indicator Message).

bit rate

The transmission rate of binary symbols ('0' and '1'). Bit rate is equal to the total number of bits transmitted in one second.

bridge

A network component that provides inter-networking functionality at the data link or medium access layer (Layer 2). Bridges provide segmentation and re-assembly of data frames.

Cat 5

(Category 5) A category of performance for inside Ethernet wiring that defines a cable with eight insulated copper wires. Each pair is twisted around each other to reduce cross talk and electromagnetic induction. Each connection on a twisted pair requires both wires. Cat5 cables are suitable for 10/100BaseT communication.

connectivity

A path for communications signals to flow through. Connectivity exists between a pair of Nodes if the destination Node can correctly receive data from the source Node at a specified minimum data rate.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. Issues IP addresses automatically within a specified range to devices such as PCs when they are first powered up. The device retains the use of the IP address for a specific license period defined by the system administrator.

EAP

(Extensible Authentication Protocol) A general point-to-point protocol that supports multiple authentication mechanisms. Defined in RFC 2284, EAP has been adopted by IEEE 802.1X as an encapsulation protocol for carrying authentication messages in a standard message exchange between a user (client or supplicant) and an authenticator. See also, 802.1X.

EAPoL

(EAP over LAN) An encapsulated form of the Extensible Authentication Protocol (EAP), defined in the IEEE 802.1X standard, that allows EAP messages to be carried directly by a LAN media access control (MAC) service between a user (client or supplicant) and an authenticator. See also, 802.1X.

EAP-TLS

(Extensible Authentication Protocol with Transport Layer Security) Used for 802.1X authentication. EAP-TLS supports mutual authentication and uses digital certificates to address the mutual challenge. The authentication server responds to a user authentication request with a server certificate. The user then replies with its own certificate and validates the server certificate. EAP-TLS algorithm derives session encryption keys from the certificate values. The authentication server in turn sends the session encryption keys for a particular session to the user after validating the user certificate. See also, authentication and EAP.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

FHSS

(Frequency-Hopping Spread-Spectrum) One of two types of spread-spectrum radio technology used in wireless LAN (WLAN) transmissions. The FHSS technique modulates the data signal with a narrowband carrier signal that “hops” in a predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. Interference is reduced, because a narrowband interferer affects the spread-spectrum signal only if both are transmitting at the same frequency at the same time. The transmission frequencies are determined by a spreading (hopping) code. The receiver must be set to the same hopping code and must listen to the incoming signal at the proper time and frequency to receive the signal.

FTP

(File Transfer Protocol) A TCP/IP based protocol for file transfer. FTP is defined by RFC 959.

GMK

(Group Master Key) A cryptographic key used to derive a group transient key (GTK) for the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). See also, GTK and TKIP.

GTK

(Group Transient Key) A cryptographic key used to encrypt broadcast and multicast packets for transmissions using the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). See also, TKIP.

HiperLAN

(High Performance Radio Local Area Network) A set of wireless LAN (WLAN) communication standards used primarily in European countries and adopted by the European Telecommunications Standards Institute (ETSI).

homologation

The process of certifying a product or specification to verify that it meets regulatory standards.

GL

IAPP

(InterAP Protocol) A protocol being developed as the 802.11f version of the IEEE 802.11 wireless LAN (WLAN) specification to support interoperability, mobility, handover, and coordination among Access Points (APs). Implemented on top of IP, IAPP uses UDP/IP and Sub-network Access Protocol (SNAP) as transfer protocols. See also, 802.11x.

IAS

(Internet Authentication Service) Microsoft's RADIUS server. See also, RADIUS.

IGMP

(Internet Group Management Protocol) An Internet protocol defined in RFC 2236 used to report its multicast group membership to neighboring multicast routers.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs. See also, encryption and VPN.

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

master secret

A code derived from the pre-master secret. A master secret is used to encrypt Transport Layer Security (TLS) authentication exchanges and to derive a pair-wise master key (PMK). See also, PMK and TLS.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MD5

(Message Direct algorithm 5) A one-way hashing algorithm used in many authentication algorithms to derive cryptographic keys. MD5 takes a message of an arbitrary length and creates a 128-bit message digest. See also, authentication.

MIB

(Management Information Base) A set of parameters an SNMP management station can query or establish in the SNMP agent of a network device (for example, a router). Standard minimal MIBs have been defined, and vendors often have their own private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. See also, SNMP and station.

MS-CHAP

(Microsoft Challenge Handshake Authentication Protocol) Microsoft's extension to CHAP. MS-CHAP is a mutual authentication protocol that also permits a single login in a Microsoft network environment. See also, connectivity.

NAT

(Network Address Translation) RFC 3022 defines a way to translate global routable IP addresses into local and private non-routable ones.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. NTP synchronizes client workstation clocks to the U.S. Naval Observatory master clocks in Washington, D.C. and Colorado Springs, CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. See also, SNTP.

Odyssey

An 802.1X security and access control application for wireless LANs (WLANs), developed by Funk Software, Inc. See also, 802.1X.

OFDM

(Orthogonal Frequency Division Multiplexing) A technique that splits a wide frequency band into a number of narrow frequency bands and sends data across the sub-channels. The 802.11a and 802.11g standards are based on OFDM. See also, 802.11a and 802.11g.

open system authentication

The IEEE 802.11 default authentication method. The device sends an authentication management frame containing the sender's identify in the clear to the authenticating device which sends back a clear frame alerting whether it recognizes the identity of the requesting device. See also, 802.11x.

PAN

(Personal Area Network) A personal area network is used to interconnect devices used by an individual or in their immediate proximity, including devices they are carrying with them and devices that are simply nearby. According to the IEEE, PANs must be capable of supporting segments at least 10 meters in length.

PAP

(Password Authentication Protocol) One of two authentication methods that is part of PPP (CHAP is the other). PAP is a method for a device to authenticate itself with a two-way handshake. Note that PAP sends its authentication information in the clear; that is, not encrypted. PAP is defined in RFC 1334.

PCI devices

Devices that adhere to the Peripheral Component Interconnect/Interface.

PEAP

(Protected Extensible Authentication Protocol) An extension to the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS), developed by Microsoft Corporation. TLS is used in PEAP Part 1 to authenticate the server only, and thus avoids having to distribute user certificates to every client. PEAP Part 2 performs mutual authentication between the EAP client and the server. See also, EAP-TLS and TLS.

PKCS

(Public-Key Cryptography Standards) A group of specifications produced by RSA and secure systems developers, and first published in 1991. Among many other features and functions, the standards define syntax for digital certificates, certificate signing requests and key exchanges.

PKI

(Public-Key Infrastructure) Software that enables users of an insecure public network such as the Internet to exchange information securely and privately. PKI uses public-key cryptography to authenticate the message sender and encrypt the message by means of a pair of cryptographic keys, one public and one private. A trusted certificate authority (CA) creates both keys simultaneously with the same algorithm. A registration authority (RA) must verify the certificate authority before a digital certificate is issued to a requestor. PKI uses the digital certificate to identify an individual or an organization. The private key is given only to the requesting party and is never shared, and the public key is made publicly available (as part of the digital certificate) in a directory that all parties can access.

plenum-rated cable

A type of cable approved by an independent test laboratory for installation in ducts, plenums, and other air-handling spaces.

PMK

(Paise-wise Master Key) A code derived from a master secret and used as an encryption key for IEEE 802.11 encryption algorithms. A PMK is also used to derive a pair-wise transient key (PTK) for IEEE 802.11i robust security. See also, 802.11x, 802.11i and PTK.

PoE

(Power over Ethernet) A technology, defined in the IEEE 802.3af standard, to deliver power over the twisted-pair Ethernet data cables rather than power cords.

GL

PPTP

(Point-to-Point Tunneling Protocol) A protocol from Microsoft that is used to create a virtual private network (VPN) over the Internet. It uses Microsoft's Point-to-Point Encryption (MPPE), which is based on RSA's RC4. It only uses static keys and should not be used to secure WLANs. See also, VPN.

pre-master secret

A key generated during the handshake process in Transport Layer Security (TLS) protocol negotiations and used to derive a master secret. See also, TLS.

private key

In cryptography, one of a pair of keys, one public and one private, that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided to only the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else. See also, public key.

PSK

(Pre-Shared Key) The IEEE 802.11 term for a shared secret, also known as a shared key. See also, 802.11x and shared secret.

PTK

(Pair-wise Transient Key) A value derived from a pair-wise master key (PMK) and split into multiple encryption keys and message integrity code (MIC) keys for use by a client and server as temporal session keys for IEEE 802.11i robust security. See also, 802.11i and PMK.

public key

In cryptography, one of a pair of keys, one public and one private, that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption. See also, encryption and private key.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol described in RFC 2865 and RFC 2866. Developed to authenticate, authorize, and account for dial-up users, RADIUS has been widely extended to broadband and enterprise networking. The RADIUS server stores user profiles, which include passwords and authorization attributes. See also, authentication and authorization.

RC4

(River Cipher 4) A common encryption algorithm, designed by RSA., used by the Wired-Equivalent Privacy (WEP) protocol and Temporal Key Integrity Protocol (TKIP). See also, TKIP and WEP.

RA

(Registration Authority) Network software that verifies a user (client) request for a digital certificate and instructs the certificate authority (CA) to issue the certificate. Registration authorities are part of a public-key infrastructure (PKI), which enables secure exchanges of information over a network. The digital certificate contains a public key for encrypting and decrypting messages and digital signatures. See also, PKI.

roaming

The ability of a user (client) to maintain network access when moving between access points (APs).

rogue AP

An Access Point (AP) that is not authorized to operate within a wireless network. Rogue APs subvert security of an enterprise network by allowing potentially unchallenged access to the network resources by any wireless user in the physical vicinity.

rogue client

A user who is not recognized within a network, but who gains access to it by intercepting and modifying transmissions to circumvent the normal authorization and authentication processes.

RSN

(Robust Security Network) A secure wireless LAN (WLAN) based on the developing IEEE 802.11i standard. See also, 802.11i.

shared secret

A static key distributed by an out-of-band mechanism to both the sender and receiver. Also known as a shared key or pre-shared key (PSK), a shared secret is used as input to a one-way hash algorithm. When a shared secret is used for authentication and the hash output of both the sender and the receiver match, they share the same secret and are authenticated. A shared secret can also be used to generate encryption key. See also, PSK.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet. SNMP uses TCP/IP to communicate with a management platform, and offers a standard set of commands that make multi-vendor operability possible. SNMP uses a standard set of definitions, known as a MIB (Management Information Base), which can be supplemented with enterprise-specific extensions. See also, MIB.

SNTP

(Simple Network Time Protocol) A a simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified. See also, NTP.

spread spectrum

A modulation technique that spreads a signal's power over a wide band of frequencies. The main reason for the technique is that the signal is much less susceptible to electrical noise and interferences then other techniques.

SSH

(Secure SHell) A Telnet-like protocol that establishes an encrypted session.

SSID

(Service Set Identifier) The unique name shared among all devices in a wireless LAN (WLAN).

station

In IEEE 802.11 networks, any device that contains an IEEE 802.11-compliant media access control and physical layers. See also, 802.11x.

TKIP

(Temporal Key Integrity Protocol) A wireless encryption protocol that fixes the known problems in the Wired-Equivalent Privacy (WEP) protocol for existing 802.11 products. Like WEP, TKIP uses RC4 ciphering, but adds functions such as a 128-bit encryption key, a 48-bit initialization vector, a new message integrity code (MIC), and initialization vector (IV) sequencing rules to provide better protection. See also, 802.11x and WEP.

TLS

(Transport Layer Security Protocol) An authentication and encryption protocol that is the successor to the Secure Sockets Layer (SSL) protocol for private transmission over the Internet. Defined in RFC 2246, TLS provides mutual authentication with non-repudiation, encryption, algorithm negotiation, secure key derivation, and message integrity checking. TLS has been adapted for use in wireless LANs (WLANs) and is used widely in IEEE 802.1X authentication. See also, 802.1X.

TTLS

(Tunneled Transport Layer Security) An Extensible Authentication Protocol (EAP) sub-protocol developed by Funk Software, Inc. for 802.1X authentication. TTLS uses a combination of certificate and password challenge and response for authentication. The entire EAP sub-protocol exchange of attribute-value pairs takes place inside an encrypted transport layer security (TLS) tunnel. TTLS supports authentication methods defined by EAP, as well as the older Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Microsoft CHAP (MS-CHAP), and MS-CHAPV2. Compare EAP-TLS; PEAP. See also, 802.1X, connectivity, MS-CHAP, PAP and PEAP.

Tunneling

A technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a Virtual Private Network (VPN). It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. See also, PPTP and VPN.

twisted-pair wire

Type of medium using metallic type conductors twisted together to provide a path for current flow. The wire in this medium is twisted in pairs to minimize the electromagnetic interference between one pair and another.

UDP

(User Data Protocol) A connectionless protocol that works at the OSI transport layer. UDP provides datagram transport but does not acknowledge their receipt.

URL

(Uniform Resource Locator) The standard method used for identifying the location of information available to the Internet.

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

VoIP

(Voice over IP) The ability of an IP network to carry telephone voice signals as IP packets in compliance with International Telecommunications Union Telecommunication Standardization Sector (ITU-T) specification H.323. VoIP enables a router to transmit telephone calls and faxes over the Internet with no loss in functionality, reliability, or voice quality.

VPN

(Virtual Private Network) A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a “tunnel” that cannot be “entered” by data that is not properly encrypted.

WAN

(Wide Area Network) A computer network that is geographically dispersed. Commonly, a WAN comprises two or more inter-connected LANs. The Internet is the world's largest WAN. According to the IEEE, WANs interconnect facilities in different parts of a country or of the world.

WECA

Wireless Ethernet Compatibility Alliance) See also, Wi-Fi Alliance.

WEP

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers. See also, 802.11x and encryption.

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability. See also, 802.11x.

WPA

(W-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1X for authentication. See also, 802.11x, 802.1X and TKIP.

XML

(eXtensible Markup Language) A simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), with unlimited, self-defining markup symbols (tags). Developed by the World Wide Web Consortium (W3C), the XML specification provides a flexible way to create common information formats and share both the format and the data on the Internet, Intranets, and elsewhere.

Index