Network infrastructure solutions Security best practices

Strong network security and mobility requires a comprehensive strategy with multiple layers of defense

Alcatel·Lucent
Enterprise

Table of Contents

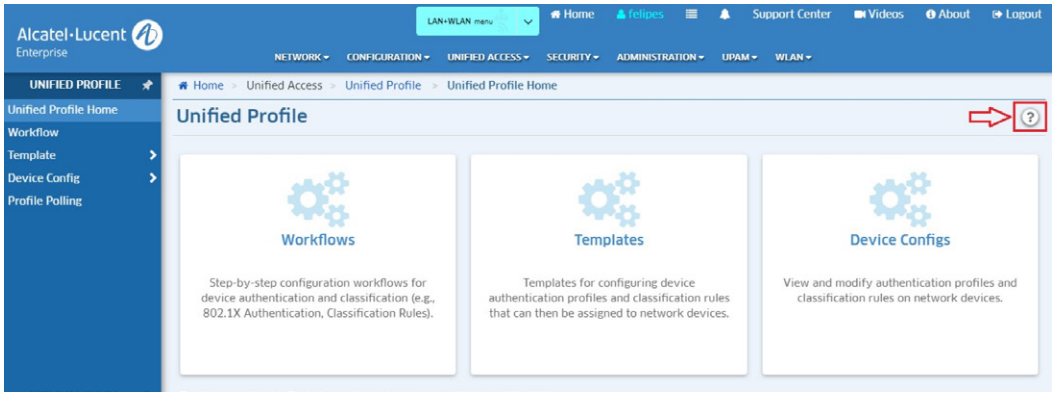
Introduction

This document provides Alcatel-Lucent Enterprise (ALE) specifications for recommended security configurations for the Alcatel-Lucent OmniSwitch® and Alcatel-Lucent OmniAccess® Stellar WLAN equipment in campus networks.

Multiple matters must be considered when configuring networking equipment in campus networks; depending on the location, networking equipment may have a variety of functions. Proper network security requires a comprehensive approach with multiple layers of defense; Alcatel-Lucent OmniSwitch and OmniAccess Stellar WLAN are “security ready” out of the box.

This document provides suggestions and best practices for adding and maintaining security of an OmniSwitch and Stellar WLAN network with secure configurations. Detailed security options with CLI syntax and examples are provided in the following OmniSwitch User Guides: Switch Management, CLI, Network Configuration Guides, as well as through the Alcatel-Lucent OmniVista® on-line user guide. The OmniVista user guide is a context-sensitive on-line configuration guide within the management application screens. The on-line user guide can be assessed while configuring OmniVista features by simply clicking on the help “?” (see Figure 1, below) in the upper right corner of the OmniVista browser window.

Figure 1



OmniVista provisioning, configuration and monitoring is 100% recommended for Stellar WLAN enterprise deployments. For OmniSwitch equipment configuration and provisioning: OmniVista, Webview, or CLI configuration is supported. However, OmniVista is highly recommended to provision an end-to-end networking solution, through one ‘pane-of-glass’ to support both OmniSwitch and Stellar WLAN equipment.

Top five security suggestions for hardening the network infrastructure

1. Install hardened/secure diversified Alcatel-Lucent Operating Software (AOS) code in the OmniSwitch

ALE secure diversified code technology uses a proactive security approach through Independent verification and validation (IV&V) and operational vulnerability scanning and analysis of switch software within the network equipment portfolio. It reviews the source code for: 1) equipment software vulnerabilities; 2) system exploits; 3) embedded malware; and 4) back-door in software

2. Change the default password to a strong pass phrase

Many breaches are due to network-based devices where the default password has not been changed or simply changed to 1234567. Default passwords are easy to obtain through hacker sites (for example http://www.phenoelit- us.org/dpl/dpl.html). Once an intruder has access to the administrator account they can change the password, locking out the owner and taking control of the device. Further recommendations on securing passwords appear later in this document.

3. Update the OmniSwitch and Stellar WLAN software regularly

Unfortunately, even mature, secure code, such as the openSSH and openSSL used in AOS, have security updates. It is important to apply the updates to your network. It is recommended that an update be scheduled approximately every 6 months. CERT alerts (https://www.us-cert.gov/ncas) should be monitored to see if additional security updates may be warranted. With the ISSU (In Service Software Update) feature available in AOS for both the OmniSwitch 6900 and 9900, security updates usually do not require a switch reboot. ALE Customer Support helps by providing tested maintenance releases approximately every 12 weeks. Critical updates, such as CERT alerts, are made available immediately after testing; they are not delayed for the next normal scheduled update.

Regularly check for ALE security advisories through its dedicated public page at ALE Security Advisories support site or you can also sign up to automatically receive security advisories for both OmniSwitch and Stellar wireless.

4. Avoid insecure protocols

Many older protocols are provided with AOS to work with existing networks. Insecure protocols include: telnet, FTP, TFTP, SNMPv1, SNMPv2. The reasons they are considered insecure are listed later in this document. However, it is recommended that the network be configured to disable 'insecure' protocols, or at least, minimize their use.

5. Review the latest US-CERT recommendations and security best practices

Cybersecurity vulnerability patching is always evolving, the network administrator attempts to covers many of the possible vulnerabilities that may be inadvertently left open; therefore, it is recommended to review and study the latest publications of the National Cyber Awareness System Alerts for Cybersecurity and Infrastructure Security Agency (US-CERT). Most of those recommendations are already addressed through this document for AOS and Stellar Wireless equipment; however, their listing is more extensive and it covers other IT infrastructure areas that may be vulnerable to cyberattacks that are not referenced in this document. Here a list of resources one can access for the most recent alerts from US-CERT:

- Sign up for new alerts through email
- Extensive list of best practices published in September 2020 - Alert (AA20-245A): Technical Approaches to Uncovering and Remediating Malicious Activity
- New alerts in 2021

Security best practices and recommendations: Common practices for the OmniSwitch and OmniAccess Stellar wireless access points

The following security best practices and recommendations apply to Network Core (OS9900 and OS6900), Distribution (OS6900 and OS6860E), Access Switches (OS6860E, OS6560, OS6450 and OS6350), as well as OmniAccess Stellar WLAN Wave 2 Access Points (APs) using WIPS (Wireless Intrusion Protection System) and console access, configured through OmniVista.

The following sections address:

1. Install the hardened/secure diversified code in OmniSwitch
2. Secure the switch/Access point (physical access to equipment)
3. Address the network protocols and services (NTP, SNMP, STP, among others)
4. Authorized Network Access Control (NAC, IoT, UNP, among others)

1. Install hardened/secure diversified code in the OmniSwitch

ALE secure diversified code promotes security and assurance at the network device level using independent verification and validation of source code and software diversification to prevent exploitation.

OmniSwitch products can also be delivered that are, TAA Country of Origin USA compliant with AOS software loaded from USA-based servers onto the OmniSwitch in a USA factory.

Secure diversified code employs multiple techniques to identify vulnerabilities, such as software architecture reviews, source code analysis (using both manual techniques and automated tools), vulnerability scanning tools and techniques, as well as analysis of known vulnerabilities in third-party code.

Software diversification

Software diversification rearranges the memory map of the executable program so that various instances of the same software, while functionally identical, are arranged differently in memory. In AOS 8.6R01, ALE has adopted address system layout randomization (ASLR) as a standard feature. ASLR results in a unique memory layout of the running software each time the OmniSwitch reboots, to impede or prevent software exploitation. ASLR is depicted below, showing how two system boots result in two different memory layouts for code segments, data segments, dynamic libraries, among others.

ALE secure diversified code technology hardens the OmniSwitch software through a combination of:

- IV&V and vulnerability analysis of switch source code
- Software diversification to prevent exploitation
- Secure software delivery to ALE customers

The above three-layer approach not only ensures security, but chain of software custody control as well.

2. Secure the Switch/Access Point

Control physical access

Physical access to switches, APs, and wiring closets allows a malicious actor to power cycle a switch, remove or replace critical components, or to alter cable wiring. Physical access to network jacks allows a malicious actor to enter the network inside the firewall. It is recommended that critical switches be housed in locked rooms with limited access. The OmniSwitch's coldStart and warmStart traps should be monitored to detect cycling of critical switches. It is recommended that the APs be managed through the Alcatel-Lucent OmniVista 2500 Network Management System (OV-2500) or the Alcatel-Lucent OmniVista® Cirrus Network Management as a Service (OV-CIRRUS).

Train personnel

Organizations work hard to select honest employees, however, without information security awareness training the employees may inadvertently leave network elements vulnerable to misuse. ALE offers training classes to enhance the skills of network personnel.

Set the correct date and time

NTP should be used to allow proper synchronization of events in logs and to ensure proper password aging. If an anomaly occurs, having a common time basis enables the separation of the cause from the effect, and greatly improves the ability to perform a forensic analysis. The NTP server should use key encryption to prevent a rogue NTP server from affecting the network. A key file will need to be loaded onto the switch.

Suggested secure configuration for the OmniSwitch if done through CLI:

- **ntp key load**
- **ntp key key_number trusted**
- **ntp server ip_address prefer key key_number**
- **ntp client enable**
- **ipservice network-time**

If an NTP server is unavailable it is recommended that the system date and time be regularly updated manually on the switch.

Commands for manually updating the date and time:

- **System date mm/dd/yyyy**
- **System time hh:mm:ss**
- **System time-and-date synchro**

The Stellar WLAN equipment will synchronize with the OmniVista or an external NTP server, when available.

Keep local passwords secure

Suggested secure OmniSwitch cli configuration:

- **user admin password user_defined_password**
- **user password-expiration 90**
- **user password-min-age 1**
- **user lockout-window 3**
- **user lockout-threshold 5**
- **user lockout-duration 4**
- **user password-size min 8 (default)**
- **user password-policy cannot-contain-username enable**
- **user password-policy min-uppercase 1**
- **user password-policy min-lowercase 1**
- **user password-policy min-digit 1**
- **user password-policy min-nonalpha 1**
- **user password-history 5**

user admin password changes the admin accounts password. This is essential as a default password is a common vulnerability exploited by malicious actors..

user password-expiration forces users to change their password after the expiration number of days. Changing the password often reduces the risk of accidental disclosure.

user password-min-age is used to prevent a user from cycling through passwords to get back to their original password within a single session. This applies to all accounts including admin.

user lockout-window, user lockout-threshold and **user lockout-duration** are used to stop malicious actors and automated systems from trying to guess the password using a brute-force attack. The normal login process has built-in delays on user-password authentication failure which discourages guessing. The literature suggests that a longer lock-out period should be used after extending failures to allow an administrator to identify the breach. The period should be sufficiently long enough for an administrator to be notified and take appropriate action. The values recommended are a balance between blocking programmatic password crackers and potential denial of authorized access. Account lock-up does not apply to the admin account.

user password-size, user password-history, and **user password-policy** commands are used to require complex passwords be set by users; values are taken from T1.276-2003. Passwords using these criteria are complex enough to provide a minimum level of security. However, organizations may require stronger passwords. Once commands for enforcing password strength are entered, be sure to update existing passwords.

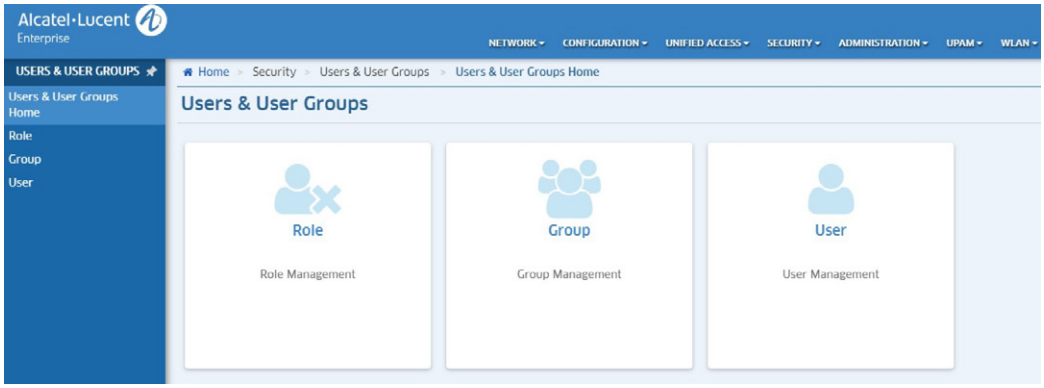
Once a password expires the next login will prompt the user to change the password.
The password aging and lock-out commands only apply to local accounts. See the RADIUS manufacturer's guide to apply these to remote accounts.

Assigning management access for the Stellar Wireless Access Points in 'Enterprise Mode' is done through OmniVista 2500 (OV-2500) or OmniVista Cirrus (OV-CIRRUS). For tighter security, and for flexibility and scalability provisioning, OV-2500 and OV-CIRRUS management are recommended for Stellar WLAN.

OmniVista to enable Users and User Groups management

The Users and User Groups application enables the administrator to control user access to OmniVista and to network devices. Access to OmniVista is controlled through the definition of user logins and passwords. Access to network switches and Stellar WLAN APs is controlled through use of User Groups, which have specified levels of access to those network devices. Access can be further defined with the User Role feature, which can be used to specify read/write access to specific OmniVista applications and network devices. All OmniVista users must be assigned to at least one User Group, which defines the access rights and roles for its members. User Groups and user logins are configured from the Users and User Groups application, and constitute one level of network security, see Figure 2 for "Users and User Groups" configuration main screen:

Figure 2



User Groups, Users, and User Roles are configured using the following screens:

- Role Management: Used to configure User Roles to restrict user access/rights to specific devices and OmniVista applications
- Group Management: Used to configure User Groups to define access to OmniVista, network devices. A User Role is associated with a User Group to specify read/write access to specific devices and OmniVista applications.
- User Management: Used to configure Users and assign the User to a User Group
- Authentication Server: Used to specify the OmniVista Login Server

Note: A User Role is an option that enables you to provide user access/rights to specific applications and network devices. For the most part, configuring Users and User Groups is sufficient.

All user accounts (other than admin, should use remote authentication)

T1.276-2003 and other standards recommend using a remote RADIUS server for account control. This allows network wide control of accounts reducing the risk of inadvertently leaving an account unsecured. The admin account should be the only local account to be used for emergency reconfiguration.

Suggested OmniSwitch CLI secure configuration:

- **aaa radius-server radius_server host ip_address**
- **aaa authentication default radius_server local**

aaa radius-server *radius_server* **host** *ip_address* configures access to the RADIUS server.

aaa authentication default *radius_server* **local** specifies that all authentication of access to the switch and Stellar Wireless APs should first be checked using the radius server and then using the local database.

In addition to the recommended Radius usage for administrator authentication, ALE best practices recommend enabling Transport Layer Security (TLS). TLS is a cryptographic protocol that provides end-to-end communications security over networks.

Note: Refer to the Switch Configuration guide for the AOS cli syntax, the syntax provided above is an example for reference purposes, please refer to the Switch Management Guide for the complete set of CLI commands and configuration options. For example, when configuring 'tsl' the following syntax is recommended:

aaa radius-server *server_name* **host** *{hostname | ip_address | ipv6_address} [hostname2| ip_address2 | ipv6_address2]* {**key** *secret* | **hash-key** *hash_secret* | **prompt-key}[salt | hash-salt** *hash_salt]* [**retransmit** *retries*] [**timeout** *seconds*] [**auth-port** *auth_port]* [**acct- port** *acct_port*] [**vrf-name name**] **[ssl | no ssl]**

aaa ldap-server *server_name* **host** *{hostname | ip_address} [hostname2 | ip_address2]* **dn** *dn_name* {**password** *super_password* | **prompt-password}[salt | hash-salt** *hash_salt*] [**base** *search_base]* [**retransmit** *retries*] [**timeout** *seconds*] **[ssl | no ssl]** [**port** *port*] [**vrf- name** *name*]

swlog output {tty {enable | disable} | console | flash | socket *{ip_address | ipv6Address | domain_name}* [**tls**] **[remote command-log] [vrf-name name]}**

snmp station *{ip_address | ipv6_address | domain_name} {[port] [username]* **[v1 | v2 | v3 | v3 tsm local-identity** *local_string* r**emote-identity** *remote_string]* **[enable | disable]}**

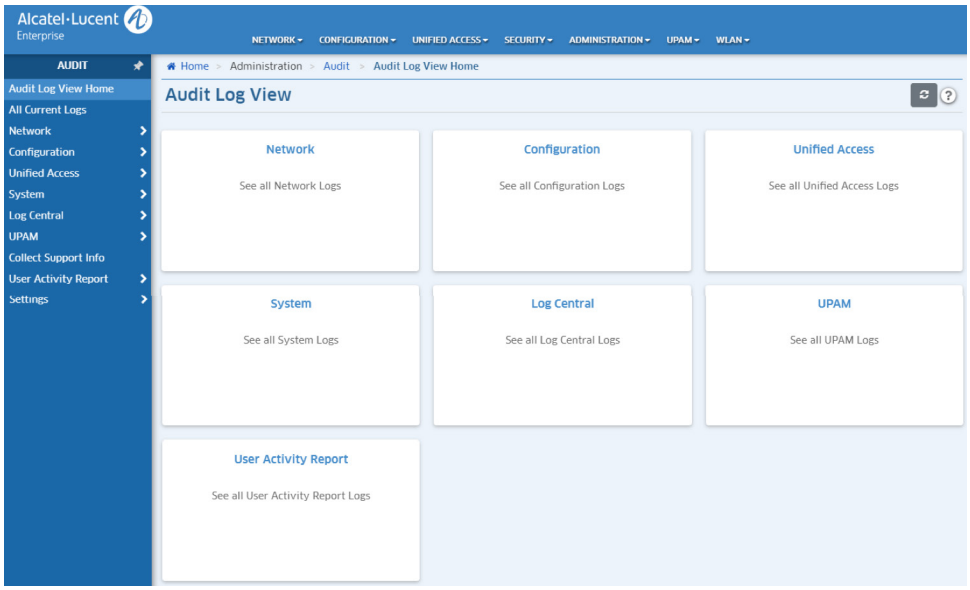
ssl pki client validate-certificate admin-state {enable | disable}

Maintain and review activity logs

The OmniSwitch is set up to assist in monitoring activity on the switch with SNMP traps and network notifications, local switch log and remote syslog (via switch log). OmniVista can be used for monitoring both OmniSwitch and Stellar Wireless network elements, see Figure 3 for AOS specific cli commands. For the Stellar WLAN, it is recommended that they be deployed in Enterprise mode for better security management and provisioning through OmniVista.

It is recommended that the OmniVista 2500 NMS be deployed to manage the OmniSwitch and Stellar WLAN. Multiple logs can be accessed through the Audit Log View Home. There are options to display the logs by function, for example; Network, Configuration, Unified Access, System, Log Central, UPAM and User Activity Report, see Figure 3 for a screen capture of the available logs:

Figure 3



OmniSwitch CLI Command Logging

The OmniSwitch provides command logging via the command-log command; if the network administration needs to log all cli commands on a per-switch basis, the command-log command needs to be enabled. This feature allows users to record the most recent commands entered via

Telnet, Secure Shell, and console sessions. In addition to a list of commands entered, the results of each command entry are recorded. Results include information such as whether a command was successfully executed, or whether a syntax or configuration error occurred.

For detailed information related to command logging commands, refer to the OmniSwitch AOS Release 8 CLI Reference Guide.

Cryptographic Support (FCS_CKM, FCS_COP)

TLS/SSL

The OmniSwitch product family implements TLS/SSL to provide a secure channel for interaction with server communications. The TLS/SSL cipher suite (selection of cryptographic algorithms) allowed for use by the switch is determined in the SSL handshake sequence by the SSL server, selected from the set of cipher suites supported by the client. Dependent on the negotiated cipher suite, the TLS/SSL protocol uses the asymmetric key pairs on the server and client to authenticate and exchange information used in the key agreement protocol. The symmetric session key set is derived by each side of the TLS/SSL protocol, used for encryption and message integrity cryptographic functions, and destroyed when the session is closed. The TOE destroys symmetric session keys used by TLS/SSL by clearing and de-allocating the key's volatile and non-volatile memory. If the keys are not destroyed then the key destruction process is repeated.

The OmniSwitch provides self-signed certificates in the default configuration; the certificate may be replaced with a well-known TLS/SSL-certificate or a certificate generated using the tools described in Authentication using X.509 Certificates (Extended – FIA_X509_EXT).

SSHv2 and SFTP

The OmniSwitch implements SSHv2 and SFTP, providing shell or FTP commands over a secure channel protected by symmetric cryptography, with keys derived using a key agreement scheme. A DSA key pair is generated if no key pair is found, including first time usage of the OmniSwitch. This key pair (/network/ssh_host_dsa_key and /network/ssh_host_dsa_key.pub) may also be replaced by using key generation tools described in Authentication using X.509 Certificates (Extended – FIA_X509_EXT).

3. Enabling Network Protocols and Services (NTP, SNMP, LLDP, MACsec, among others)

Enable Network Time Protocol in the Switch

NTP is designed to use MD5 encryption authentication to prevent outside influence upon NTP timestamp information. This is done by using a key file. The key file is loaded into the switch memory and consists of a text file that lists key identifiers that correspond to NTP entities.

If authentication is enabled on an NTP switch, any NTP message sent to the switch must contain the correct key ID in the message packet, to use in decryption. Likewise, any message sent from the authentication enabled switch will not be readable unless the receiving NTP entity possesses the correct key ID.

The key file is a text (.txt) file that contains a list of keys that are used to authenticate NTP servers. Key files are created by a system administrator independent of the NTP protocol, and placed in the switch memory when the switch boots.

The NTP software is disabled on the switch by default. To activate the switch as an NTP client, enter the ntp client command as shown:

-> ntp client admin-status enable

This sets the switch to act as an NTP client in the passive mode, meaning the client will receive updates from a designated NTP server.

To disable the NTP software, enter the ntp client command as shown:

-> ntp client admin-status disable

Regarding the Stellar WLAN Access Points in Enterprise mode, all security parameters (including NTP, Radius, and Unified Access AAA parameters) will be provisioned through OmniVista unified management.

Turn off insecure protocols

Insecure protocols are provided by AOS to support legacy systems. They are not recommended. Secure protocols are available which provide the same type of functionality. All services which are not used should be disabled to further reduce exposure. For example, if SNMP is not used, then the enable commands for SNMP should be removed.

Suggested secure configuration:

- **no ip service all, ip service ssh, ip service snmp, ip service http disables** all IP services except secure protocols
- **ssh enable, ssh pubkey-auth enable** require SSH to work with public key certificates. The user key must be loaded on the switch in /flash/network/pub.
- **snmp security privacy all** requires SNMP accesses to use v3

Disabled Protocol	Replacement	Reason
telnet	ssh	telnet does not use encryption or certificates.
ftp	sftp scp	FTP does not use encryption or certificates.
tftp	sftp scp	TFTP does not require user authentication and does not use encryption.
snmp v1	snmp v3	SNMP v1 does not provide for user authentication. v3 provides encryption.
snmp v2	snmp v3	SNMP v2 does not provide for user authentication. v3 provides encryption.
avlan-http	avlan-secure-http	Disable unless avlan is used. HTTP is an insecure protocol.
avlan-secure- http		Disable unless AVLAN is used.
avlan-telnet		Disable unless AVLAN is used. Telnet is an insecure protocol.
udp-relay		Disable unless relay service is used.
ntp		Disable unless NTP is used.

Block network protocols from user ports

If network protocols are not blocked from user ports a rogue networking device could send these protocols and disrupt normal network operation.

OmniSwitch AOS cli as follows:

- **policy port group UserPorts** slot/port slot/port identifies which ports or port ranges are user ports. User ports are currently limited to 126 ports.
- **qos user-port shutdown** causes the port to shut down or block when a packet of the protocols specified is received. This prevents users from inadvertently providing network services; refer to the **OmniSwitch Switch Management Guide** and **Network Configuration Guide** for detail syntax and examples to configure these secured parameters.

Hide device uniqueness using session control

Part of network security is not allowing a malicious actor to have knowledge of a device's identity or type. It is recommended that any pre-banner be the same for all devices on the network whether servers or network equipment. This prevents providing a malicious actor with information about the possible weakness of a device. It is recommended that a warning banner be used either pre- or post-login, that warns users about the ownership of the network and consequences of misuse. This can deter casual misuse and in many geographic regions, is a legal requirement.

Enable Link Layer Discovery Protocol (LLDP)

The OmniSwitch LLDP Agent Security mechanism provides a solution for secure access to the network by detecting rogue devices and preventing them from accessing the internal network. LLDP agent security can be achieved by allowing only one trusted LLDP remote agent on a network port.

The user is provided with an option to configure the Chassis ID subtype that can be used in validating the Chassis ID type in the incoming LLDP PDU. If the Chassis ID is not configured, by default, the first LLDP remote agent is learned with the received Chassis ID. When more than one LLDP agent is learned on a port, the port is moved to a violation state.

The OmniSwitch LLDP Agent Security mechanism provides a solution for secure access to the network by detecting rogue devices and preventing them from accessing the internal network. LLDP agent security can be achieved by allowing only one trusted LLDP remote agent on a network port.

Enable Distributed Denial of Service (DDoS) filtering triggers

By default, the switch filters Distributed Denial of Service (DDoS) attacks, which are security attacks aimed at devices that are available on a private network or the Internet. Few attacks are targeted at system bugs or vulnerabilities (for example, teardrop attacks), while other types of attacks involve generating large volumes of traffic so that network service is denied to legitimate network users (such as pepsi attacks). These attacks include the following:

- ICMP Ping of Death: Ping packets that exceed the largest IP datagram size (65535 bytes) are sent to a host and crash the system.
- SYN Attack: Floods a system with a series of TCP SYN packets, resulting in the host issuing SYN-ACK responses. The half open TCP connections can exhaust TCP resources, such that no other TCP connections are accepted.
- Land Attack: Spoofed packets are sent with the SYN flag set to a host on any open port that is listening. The machine can crash or reboot to respond.
- Pepsi Attack: The most common form of UDP flooding directed at harming networks. A pepsi attack is an attack consisting of many spoofed UDP packets aimed at diagnostic ports on network devices. A pepsi attack can cause network devices to use up a large amount of CPU time responding to these packets.
- ARP Flood Attack: Floods a switch with many ARP requests, resulting in the switch using a large amount of the CPU time to respond to these requests. If the number of ARP requests exceeds the preset value of 500 per second, an attack is detected.
- Invalid IP Attack: Packets with invalid source or destination IP addresses are received by the switch.
- When such an Invalid-IP attack is detected, the packets are dropped and SNMP traps are generated.

- Multicast IP and MAC Address Mismatch: This attack is detected when:
  - ¬ The source MAC address of a packet received by a switch is a Multicast MAC address.
  - ¬ The destination IP and MAC addresses of a packet received by a switch is same as the Multicast IP and MAC addresses, but the Multicast IP and the Multicast MAC addresses do not match.

  Note: In both the conditions described above in "Multicast IP and MAC Address Mismatch", packets are dropped and SNMP traps are generated.

  - ¬ The destination IP is a unicast IP and the destination MAC address is either a Broadcast or Multicast address. In such a condition, an event is recorded in the DoS statistics. No SNMP traps are generated as valid packets can also fall under this category.
- Ping overload: Floods a switch with many ICMP packets, resulting in the switch using a large amount of CPU time to respond to these packets. If the number of ICMP packets exceeds 100 per second, a DoS attack is detected. By default, the detection of attack is disabled.
- Packets with loopback source IP address: Packets with an invalid source address of 127.0.0.0/8 (loopback network) are received by the switch. When such packets are detected, they are dropped, and SNMP traps are generated.

The switch can be set to detect various types of port scans by monitoring for TCP or UDP packets sent to open or closed ports. Monitoring is done in the following manner:

- Packet penalty values set. TCP and UDP packets destined for open or closed ports are assigned a penalty value. Each time a packet of this type is received, is assigned penalty value is added to a running total. This total is cumulative and includes all TCP and UDP packets destined for open or closed ports.
- Port scan penalty value threshold. The switch is given a port scan penalty value threshold. This number is the maximum value the running penalty total can achieve before triggering an SNMP trap.
- Decay value. A decay value is set. The running penalty total is divided by the decay value every minute.
- Trap generation. If the total penalty value exceeds the set port scan penalty value threshold, a trap is generated to alert the administrator that a port scan can be in progress.

Enable DCHP security features

There are two DHCP security features available: DHCP relay agent information option (Option-82) and DHCP Snooping. The DHCP Option-82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information.

Although DHCP Option-82 is a subcomponent of DHCP Snooping, these two features are mutually exclusive. If the DHCP Option-82 feature is enabled for the switch, then DHCP Snooping is not available.

The reverse is also true. If DHCP Snooping is enabled, then DHCP Option-82 is not available. In addition, the following differences exist between these two features:

- DHCP Snooping does require and use the Option-82 data insertion capability, but does not implement any other behaviors defined in RFC 3046.
- DHCP Snooping is configurable at the switch level and on a per-VLAN basis, but DHCP Option-82 is only configurable at the switch level.

Note: DHCP Snooping now provides multiple VLAN tagging support.

The following section provides additional information about each DHCP security feature and how to configure feature parameters using the Command Line Interface (CLI).

This implementation of the DHCP relay agent information option (Option-82) feature is based on the functionality defined in RFC 3046. By default, DHCP Option-82 functionality is disabled. The ip helper agent-information command is used to enable this feature at the switch level.

When this feature is enabled, communications between a DHCP client and a DHCP server are authenticated by the relay agent. To accomplish this task, the agent adds Option-82 data to the end of the options field in DHCP packets sent from a client to a DHCP server. Option-82 consists of two sub options: Circuit ID and Remote ID. The agent fills in the following information for each of these sub options:

- **Circuit ID**—the VLAN ID and slot/port from where the DHCP packet originated
- **Remote ID**—the MAC address of the router interface associated with the VLAN ID specified in the Circuit ID sub option

The **ip helper dhcp-snooping option-82 format** command is used to configure the type of data (base MAC address, system name, interface alias, or user-defined) that is inserted into the above Option-82 sub-options. The system name and user-defined text are reported in ASCII text format, but the MAC address is still reported in hex-based format.

Spanning Tree security

All OmniSwitch ports are automatically eligible for root port selection. A port in a CIST/MSTI instance or per-VLAN instance can be prevented from becoming the root port by restricting the role of the port (also referred to as enabling root guard). This is done using the **spantree cist restricted-role** command or the **spantree lan restricted-role** command regardless of which mode (per-VLAN or flat) is active for the switch.

When root guard is enabled for a port, it cannot become the root port, even if it is the most likely candidate for becoming the root port. However, this same port is designated as the alternate port when the root port is selected.

Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology. However, note that enabling the restricted role status for a port may impact connectivity within the network.

OSPF Router Interface Authentication

OSPF allows for the use of authentication on configured interfaces. When authentication is enabled, only neighbors using the same type of authentication and the matching passwords or keys can communicate.

There are two types of authentication: Simple and MD5. Simple authentication requires only a text string as a password, while MD5 is a form of encrypted authentication that requires a key and a password. Both types of authentication require the use of more than one command.

Simple authentication

To enable simple authentication on an interface, enter the ip ospf interface auth-type command with the interface name. Once simple authentication is enabled, the password must be set with the ip ospf interface auth-key command.

MD5 encryption

To configure the same interface as above with MD5 encryption, enter the ip ospf interface auth-type as shown below:

-> ip ospf interface vlan-213 auth-type md5

Once MD5 authentication is set, a key identification and key string must be set with the ip ospf interface md5 key command. Refer to the AOS CLI Guide for the complete syntax to configure the above functions.

IPSec for Alcatel-Lucent OmniSwitch® 6860 and Alcatel-Lucent OmniSwitch® 6860E

IPSec provides protection to IPv6 traffic. To achieve this, IPsec provides security services for IPv6 packets at the network layer. These services include access control, data integrity, authentication, protection against replay, and data confidentiality. IPsec enables a system to select the security protocols, encryption and authentication algorithms and use any cryptographic key as required. IPsec uses the following two protocols to provide security for an IPv6 datagram:

- Encapsulating Security Payload (ESP) to provide confidentiality, data origin authentication and connectionless integrity
- Authentication Header (AH) to provide connectionless integrity and data origin authentication for IPv6 datagrams and to provide optional protection against replay attacks. Unlike ESP, AH does not provide confidentiality.

IPsec on an OmniSwitch operates in Transport mode. In transport mode only the payload of the IPv6 packet is encapsulated and an IPsec header (AH or ESP) is inserted between the original IPv6 header and the upper-layer protocol header.

MACsec

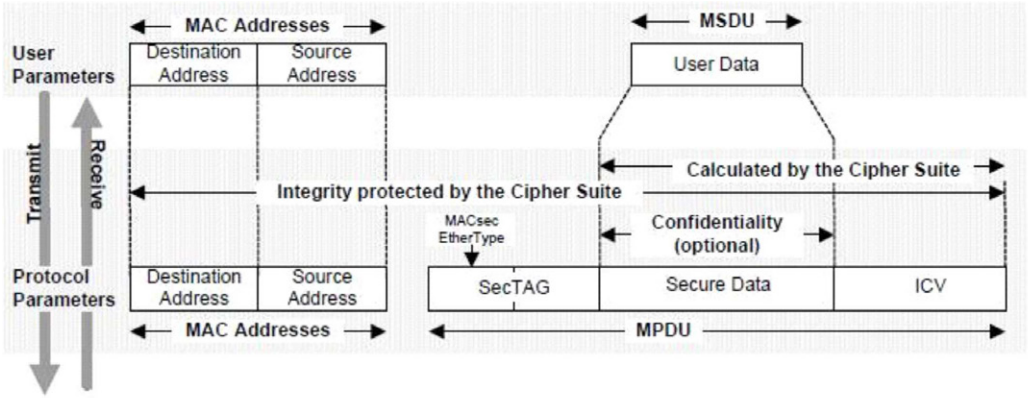
For added security on the uplinks and some user ports, most OmniSwitch models and the Multi-Gig Stellar access point, support the IEEE 802.1AE-2006 MACsec (MAC Security) standard. The purpose of MACsec is that it provides point-to-point or also known as, hop-to-hop security on Ethernet links between directly connected nodes. MACsec prevents DDoS/M-in-M/playback attacks, intrusion, wire-tapping, masquerading, among others. MACsec can be used to secure most of the traffic on Ethernet links - LLDP frames, LACP frames, DHCP/ARP packets, and more. ALE recommends enabling MACsec in backbone switches to secure traffic transported through those uplinks. Other excellent applications for this technology exist today; for example, Data Center Interconnect (DCI) applications where all transported traffic can be encrypted at wire rate.

MACsec-enabled links work by securing through matching security keys. Data integrity checks are done by appending an 8-byte or 16-byte header and a 16-byte tail to all Ethernet frames traversing the secured link.

On the wire, a MACsec packet starts with an Ethernet header with etherType 0x88E5, followed by an 8-byte or 16-byte SecTag header containing information about the decryption key, a packet number and Secure Channel Identifier. The SecTag header is followed by the payload (which may be optionally encrypted) and the Integrity Check Value (ICV) generated by GCM-AES of size 16 bytes.

Each node in a MACsec-protected network has at least one transmit secure channel associated with a Secure Channel Identifier (SCI). Configuration parameters such as enable encryption or perform replay protection are stored in the context of the transmit secure channel. A single secure channel is unidirectional, that is, it can be applied to either inbound or outbound traffic.

Figure 4



OmniSwitch and OmniAccess Stellar hardware with MACsec support in PHYs

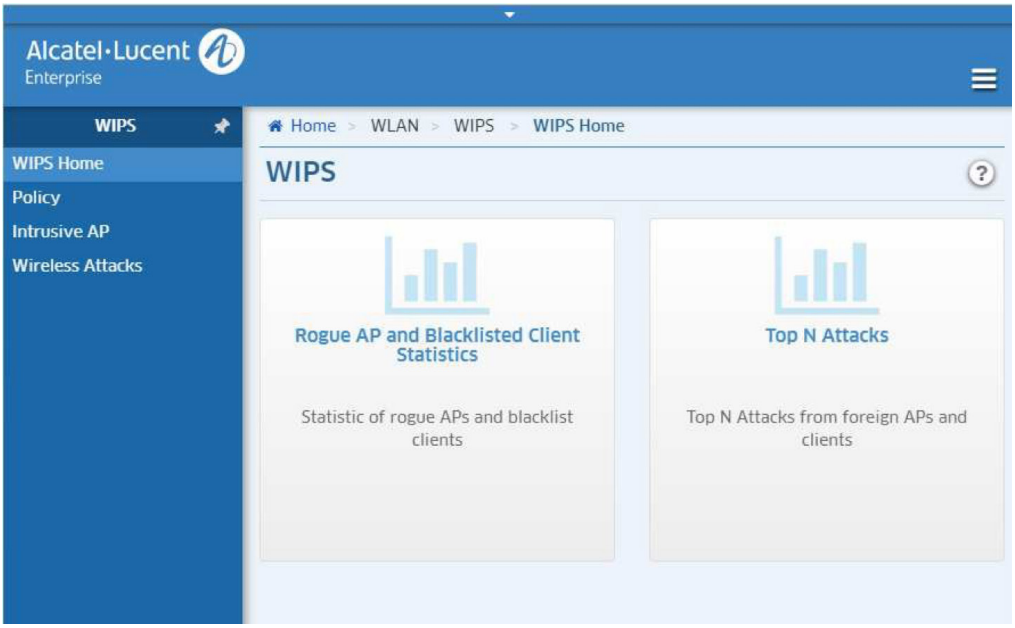
The following OmniSwitch and OmniAccess Stellar wireless hardware supports MACsec through some of its PHYs. The table below lists the product model in the first column; the second column denotes which PHYs are MACsec enabled; the third column lists the software features which enable the enforcement of the MACsec functionality.

Product model	Where supported / Hardware capable	Software features supported
OS9900	All ports except OS99-CNI-U8. If needed on the CMM, the 4x10G 'splitter' cable must be used (not supported on 100GE or 40GE ports), only supported for 10G speeds	Provides secure access to network, data integrity, data origin authentication, and (optionally) data encryption - all at Layer 2: 1) 802.1AE-2006 for encryption over Ethernet. 2) 802.1X-2010 - MACSec Key Agreement (MKA) Protocol Software support released in Phases: Keys are managed using a 3rd party key manager. Delivers standard operation. MACsec Key Agreement (MKA) Protocol, node discovery, SA key generation/distribution, PN synchronization. MACsec: clear tag support & EAPOL DMAC (support in network edge - OS6860/E, OS6560 and OS6465).
OS6860E-P24Z8	All 1G / 10G ports not supported in MultiGig ports	
OS6860/6860E (Legacy models)	10GE uplinks only	
OS6860E-P24 & P24Z8	All ports (user ports + uplinks)	
OS6560-48 / P48	All ports on these two 48-port models	
OS6560-X10	All ports	
OS6465-P6/P12	All ports	
OS6465-P28	All ports (except on the P28 not on the 2x10G SFP+ ports)	
OS6465T	All ports	
OS6860N-P48M	Supported on all 1GE & 10GE ports (the other N models; for example, in the 6860N-U28 and P24Z, supported on the 10G uplinks only	AOS features listed above supporting both 128- and 256-bit keys.
OS6900-X48C4E	All 10GE SFP+ ports	AOS features listed above supporting both 128- and 256-bit keys.
Stellar AP 1230, 1320 & 1360	On MultiGig port only	Hardware-ready

Wireless Intrusion Protection System (WIPS)

Protecting the wireless network: Since an 802.11 network is open and borderless, it makes it vulnerable to attacks (for example; rogue APs, unauthorized clients, DDoS attacks). The Stellar WLAN security best practices are enabled through the Wireless Intrusion Protection System (WIPS) application which monitors the wireless radio spectrum for the presence of unsafe access points and clients, and can take countermeasures to mitigate the impact of foreign intrusions. Figure 4, the WIPS screen) provides an overview of wireless network threats/intrusions for Stellar APs, and enables users to set up policies to detect threats and take countermeasures.

Figure 5



The WIPS Home Page provides links to an overview of network threats and intrusions for Stellar APs, including Rogue APs and Blacklisted Clients, as well as network attacks over a 24- hour, or one-week period.

Creating Wireless Attack Policies

A rogue AP is not the only threat to the wireless network. Other wireless attacks can be detected and mitigated for both APs and Clients. To create Wireless Attack Policies, you must enable Wireless Detection. When configuring a policy, each detection policy can be set to one of the following levels. When a level is selected, all detection policies included in that level are displayed and selected.

- **High:** Enables all applicable detection mechanisms, including all the options of low and medium level settings
- **Medium:** Enables important detection mechanisms including all the options of the low-level settings
- **Low (Default):** Enables only the most critical detection mechanisms
- **Custom:** Enables only the selected detection mechanisms. When this level is selected, all detection mechanisms are displayed. Select the ones you want to include in the policy.

An AP 'Attack Detection Policy' detects multiple attacks originating from foreign APs. Refer to the OmniVista 2500 or OmniVista Cirrus online user guide for a list of AP attack detection policies that can be configured and enabled to protect the wireless network from malicious actors.

4. Authorized Network Access Control (including: ACL, NAC, IoT, UNP)

Purpose and Usage of Access Control Lists

Access Control Lists (ACLs) are QoS policies used to control whether packet flows are allowed or denied at the switch or router interface. ACLs are sometimes referred to as filtering lists.

ACLs are distinguished by the kind of traffic they filter. In a QoS policy rule, the type of traffic is specified in the policy condition. The policy action determines whether the traffic is allowed or denied.

For detailed descriptions about configuring policy rules, see QoS Policy Overview and Creating Policies in the Network Configuration Guide.

In general, the types of ACLs include:

- Layer 2 ACLs: For filtering traffic at the MAC layer. Usually uses MAC addresses or MAC groups for filtering
- Layer 3/4 ACLs: For filtering traffic at the network layer. Typically uses IP addresses or IP ports for filtering; note that IPX filtering is not supported.
- Multicast ACLs: For filtering IGMP traffic
- Security ACLs: For improving network security. These ACLs utilize specific security features, such as user ports groups to prevent source IP address spoofing, ICMP drop rules and TCP connection rules.

Port Mapping, Mirroring, and Monitoring

Remote Port Mirroring (RPMIR) extends the port mirroring functionality by enabling remote port mirroring across multiple switches in the network. The traffic for this mirroring session is carried across these switches through the user specified RPMIR VLAN, which is dedicated for the mirroring traffic configured across all these switches. No other traffic is allowed on this VLAN.

Ingress, egress, or bidirectional traffic can be mirrored. The mirrored traffic from the source port is tagged onto the RPMIR VLAN through the mirror to port (MTP) in the source switch, and then forwarded over the intermediate switch ports that are carrying the RPMIR VLAN to the destination switch.

Port Mapping is a security feature that controls communication between peer users. Each session is comprised of a session ID, a set of user ports, and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports. In a port mapping session with user port set A and network port set B, the ports in set A can only communicate with the ports in set B. If set B is empty, the ports in set A can communicate with the rest of the ports in the system.

A port mapping session can be configured in the unidirectional or bidirectional mode. In the unidirectional mode, the network ports can communicate with each other within the session. In the bidirectional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any sessions configured in the bidirectional mode.

To create a port mapping session either with the user ports, network ports, or both the user ports and network ports, use the port-mapping user-port network-port command. For example, to create a port mapping session 8 with a user port on slot 1 port 2 to port 5 and a network port on slot 2 port 3, for example, enter:

-> port-mapping 8 user-port 1/2-5 network-port 2/3

One can create a port mapping session with link aggregate network ports. For example, to create a port mapping session 3 with network ports of link aggregation group 7 to 9, enter:

-> *port-mapping 3 network-port linkagg 7*

-> *port-mapping 3 network-port linkagg 8*

-> *port-mapping 3 network-port linkagg 9*

For other supported port mapping capabilities and its syntax refer to the **Network Configuration** or **CLI User** guides.

Application Fingerprinting

The AOS Application Fingerprinting (AFP) application attempts to detect and identify a remote application by scanning the payload of its IP packets and matching them against predefined bit patterns (application signatures). Once the application is identified, AFP collects the source and destination information and applies QoS or generates an SNMP Trap.

The OmniSwitch sFLOW mechanism is used one port at a time for a given interval, and within the interval, packets are copied to the switch CPU at a controlled rate:

- Application Fingerprinting operates in three different modes:
- Monitoring Mode: The specified application signatures are monitored on a per-port basis. No action is taken if there is a match.
- QoS Mode: If there is a match, pre-configured QoS policy action is applied to the ingress
- IP flow
- UNP Mode: If there is a match, pre-configured QoS policy action is carried out on the IP flow only if the source MAC/VLAN of the IP flow matches with the pre-configured UNP profile

Using this implementation of AFP, an administrator can obtain more detailed information about protocols running on a specific device or make sure that certain QoS actions are automatically applied wherever an application might be running.

Note: Refer to the Specifications Guide for the AOS 8.x version for verified supported AFP specifications.

Applications Visibility

To enable better security practices when deeper application visibility and network control is required including deep packet inspection (DPI) in an OmniSwitch 6860E and OmniAccess Stellar wireless.

APs, a network administrator needs to enable this functionality through OmniVista under the Network Application Visibility Devices Management application. The **Application Visibility Devices Management Screen** displays information about all network switches and Stellar AP Series Devices (AP Groups) that support application visibility. In addition to the name, IP address, and operational status of each device, the screen indicates whether an Application Visibility Profile has been assigned to the device. From that screen, one can display more detailed information and/or enable/disable automatic Signature File updates. For additional configuration options, refer to the OmniVista online help from within each of the OmniVista application screens.

Enabling Learned Port Security

Learned Port Security (LPS) provides a mechanism for authorizing source learning of MAC addresses on Ethernet and Gigabit Ethernet ports. LPS does not support link aggregate and tagged (trunked) link aggregate ports.

Benefits of using LPS to control source MAC address learning:

- A configurable source learning time limit that applies to all LPS ports
- A configurable limit on the number of MAC addresses allowed on an LPS port
- Dynamic configuration of a list of authorized source MAC addresses
- Static configuration of a list of authorized source MAC addresses
- Two methods for handling unauthorized traffic: Stopping all traffic on the port, or only blocking traffic that violates LPS criteria

By default, LPS is disabled on all switch ports. To enable LPS on a port, use the port-security command.

When LPS is disabled on a port, MAC address entries for that port are retained in the LPS table. The next time LPS is enabled on the port, the same LPS table entries are again active. If there is a switch reboot before the switch configuration is saved the dynamic MAC address entries are discarded from the table.

User Network Profile (UNP)

Static or dynamic User Network Profile (UNP) features provide network administrators with the ability to define and apply network access control to specific types of devices by grouping, such devices according to specific matching profile criteria. This allows network administrators to create UNPs from a unified framework of operation and administration (OmniVista 2500 premises-based and OmniVista Cirrus cloud-based) NMS.

UNP is not limited to creating profiles for only certain types of devices. However, the following classification methods implemented through UNP functionality and profile criteria provide the ability to tailor profiles for specific devices (physical or virtual):

- MAC-based and 802.1X-based authentication using a RADIUS-capable server
- Redirection for Captive Portal authentication
- Redirection to OmniVista ClearPass Policy Manager (CPPM) and Unified Policy Access Manager (UPAM) for Bring Your Own Devices (BYOD) user device registration, UNP assignment, and policy list assignment
- Switch-wide classification rules to classify users based on port and device attributes (for example, source MAC, Group ID, IP address). No authentication required.
- Default UNP classification for traffic not classified through other methods
- Basically, UNP functionality is used to define profile-based VLANs to which network devices are assigned. The profile can allow, deny, or require actions by users or machines on the network. Because membership to a VLAN is based on UNP profile criteria, devices assigned to the VLAN or service are not tied to a specific port or switch. This flexibility allows device mobility within the network while maintaining network security.

Configuring UNP involves defining profiles and setting UNP global and port-based parameters. When a UNP (VLAN-based) profile is created, default values are applied for the profile parameters (for the detailed syntax and configuration examples, refer to the “UNP Profile Defaults” in the Network Configuration Guide).

The UNP functionality at the network access is supported in the OmniSwitch 6860/6860E, 6865, 6560 and 6465 with the current version of AOS 8.5R1 or newer software, as well as, the OmniAccess Stellar wireless access points. A new UNP functionality is also supported in the OmniSwitch 6450/6350 with software release AOS 6.7.x or later. The OmniVista 2500 or OmniVista CIRRUS can be used to easily and dynamically provision UNPs with easy-to-follow workflows in both UPAM and Unified Access applications.

Note: Refer to the Specifications Guide for the AOS 8.x version for verified supported UNP specifications for each of the AOS switch platforms. It is recommended to use a single workflow in OmniVista to configure OmniSwitches and OmniAccess Stellar wireless APs through a single 'pane-of-glass'.

Augmented intelligence and device fingerprinting enabled networks

The device profiling and fingerprinting feature builds an inventory list which is dynamically populated with devices information through communication with an external cloud-based database of industry recognized device signatures. That information can be leveraged to provision UNPs that can be enforced at the access layer to further protect an OmniSwitch and Stellar wireless network.

The OmniVista NMS device fingerprinting/ profiling application tool is an enabler to help create containers for those unsolicited, unplanned, headless IoT devices to ensure secure network access through the definition and automatic application of UNPs. With this solution, all stakeholders must cooperate in keeping the IoT devices software security-patched, and use strong passwords to help maintain a clean, mobile, and secure network infrastructure. For configuration options and application of this feature, refer to the "Augmented Intelligence and Device Fingerprinting Enabled Network" application note.

5. Reporting a suspected Security Vulnerability

We acknowledge the importance for our customers to rely on secure products and solutions. Therefore, it is our goal to ensure that ALE products are developed with all appropriate security principles as basis. We follow a comprehensive security program that combines:

- Secure software development best practices, processes, and tools
- Rigorous product security requirements
- Periodic validation and quality of security testing before release

Individuals or organizations that are experiencing technical security issue with an ALE product or solution are strongly encouraged to contact the ALE PSIRT by following these steps:

1. Obtain the ALE PSIRT PGP public key, this will ensure the confidentiality of the communication. Confidentiality is a key point at this step to protect the security of our customers in regards with our responsible disclosure policy.
2. Complete the vulnerability summary report (VSR)
3. Send the completed report to the email address: psirt@al-enterprise.com
4. Consider sending the report email with the reporting organization's public PGP key and by encrypting the message with the ALE PSIRT PGP public key (scroll to bottom of page of key retrieval).

ALE PSIRT works with third-party coordination centers such as CERT-IST, NVD, US-CERT to manage vulnerabilities notices reported on third-party software embedded or used in ALE products and solutions. The reports are referred to with a unique CVE number (Common Vulnerabilities and Exposures After). Each issued CVE is analyzed by ALE teams to provide an adjusted risk score that reflect s the effective impact on our products.

Conclusion

Security awareness training is a requirement for all employees which inadvertently can leave the network administration open to misuse. ALE offers training classes to enhance the network personnel's skills.

In addition, ALE provides a number of user manuals including; the OmniSwitch User Guides for detailed CLI syntax and other security configuration options. Following is a listing of the user guides referenced throughout this document:

1) AOS Switch Management Guide: This guide will help users understand the switch's directory structure, the command line interface (CLI), configuration files, basic security features, and basic administrative functions. The features and procedures in this guide will help form a foundation that will allow you to configure more advanced switching features later in the network provisioning process.
2) AOS Network Configuration Guide: Read this guide when your switch is up and running and you are ready to familiarize yourself with the software functions. When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, Spanning Tree, and network routing protocols. The OmniSwitch AOS Network Configuration Guide contains overview information, procedures, and examples on how standard networking technologies are configured on the OmniSwitch.
3) AOS CLI Guide: Details the CLI syntax and usage including examples.
4) Advanced Routing Guide: This configuration guide includes information about configuring the following Layer 3 features
    - ¬ Open Shortest Path First (OSPF) protocol
    - ¬ Border Gateway Protocol (BGP)
    - ¬ Multicast routing boundaries
    - ¬ Distance Vector Multicast Routing Protocol (DVMRP)
    - ¬ Protocol-Independent Multicast (PIM)—Sparse Mode, Dense Mode, and Source-Specific Multicast
5) AOS Specification Guide: This guide lists all verified features and tested specification tables for the specified AOS release version.
6) OmniVista Online User Guide: OmniVista help user guide can be found in the context-sensitive on-line help within the network management applications. The on-line help user guide can be assessed while configuring OmniVista features by simply clicking on the help "?" on the upper right-hand corner of the OmniVista browser window.

The network administrator will reference a combination of those user guides to configure the OmniSwitch features through CLI or Stellar WLAN via OmniVista. Each guide serves its purpose as summarized above. Other user guides for the hardware, fiber optic transceivers, and Data Center specific features are also available to support those functions.

In conclusion, it is recommended to provision OmniVista for monitoring and configuring the network-wide features. OmniVista, in most cases, can eliminate the use of the AOS user guides; however, the user guides are digitally available for specific switch troubleshooting and individual switch configurations. For Stellar WLAN enterprise deployments, it is recommended that they be 100% provisioned through OmniVista with very little to no CLI interface requirements.

Alcatel·Lucent Enterprise