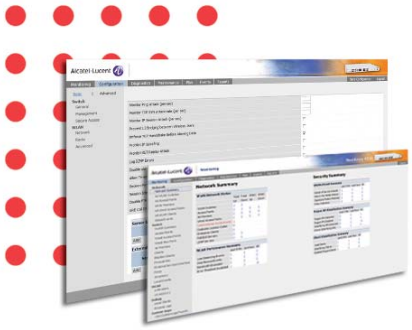
Alcatel-Lucent OmniAccess External Services Interface Module

WIRELESS LAN SOFTWARE

The External Services Interface (ESI) software module provides standards-based extensibility, allowing an Alcatel-Lucent OmniAccess Wireless LAN (WLAN) switch to communicate with external service devices and support advanced interaction with authentication, authorization, and accounting (AAA) services infrastructure.

The ESI selectively redirects interior network traffic, based on policy, to devices that provide in-line network services such as virus protection, network intrusion detection, billing and accounting, content filtering, content transformation and usage auditing.

Advanced Application Programming Interfaces (APIs) provide integration with these external systems as well as with AAA servers. These systems are most effective when they can directly control the authentication and authorization state of wireless clients.



FEATURES	BENEFITS
• Flexible delivery of network services	• Expands network-based services from the DMZ to all interior users, without change to underlying infrastructure • Preserves investment with existing security and service vendors
• Policy-based network traffic inspection	• Directs traffic to external service appliances based on user identity or trust state • Redirects traffic selectively to avoid service device overload
• Open interface	• Provides an open, yet secure interface for integration with best of breed 3rd party devices
• Load-balancing optimization	• Forwards traffic to a pool of service appliances to avoid overloading any one device • Avoids single points-of-failure while ensuring network responsiveness
• Fault-tolerant for mission-critical networks	• Continuous health checking ensures availability of external devices • Load balancing to prevent traffic from being sent to a failed device

FEATURES	BENEFITS
• Flexible deployment options	• Permits deployment under varied network topologies; service appliances may be directly attached to WLAN switches or attached to common intermediary devices
• Extended authorization control using API	• Dynamic modification of user privileges based on metrics such as client behavior • Automatically disconnects users when pre-defined conditions are matched • Interfaces to external systems through RFC 3576 or a flexible XML API
• AAA auto-selection	• Redirects users to different authentication servers based on a fully qualified domain name or realm • Simplifies corporate mergers and consolidations where multiple authentication servers must be integrated

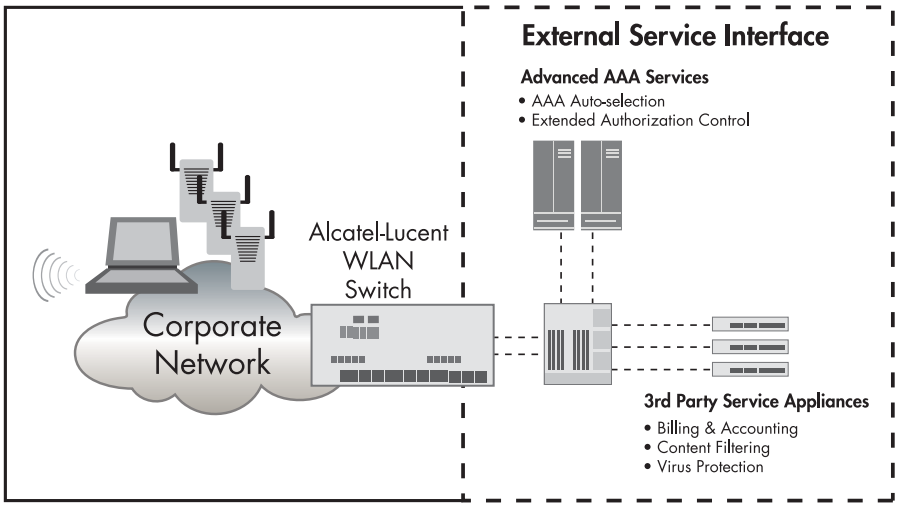
Flexible Delivery of Network Services

As networks transform to support an increasingly mobile workforce, services that were built for fixed networks must be extended to accommodate mobility.

A vast array of network service devices exists in the marketplace today. Typically deployed in a DMZ or at an organization's Internet gateway, these devices provide services such as virus protection, content inspection and filtering, intrusion detection and prevention, content transformation, protocol-based bandwidth shaping and more.

Until now, deploying such services in the interior of the corporate network required placement of network service devices in every wiring closet, where they were placed in line with all network traffic. The OmniAccess Wireless ESI takes a centralized approach, enabling scalable, manageable deployments that minimize both capital and operational costs.

Figure 1 External Service Interface



The OmniAccess WLAN External Services Interface (ESI) software module enables the scalable, seamless extension of WAN DMZ services throughout the network

The ESI module features an open interface, permitting the redirection of traffic to any standard in-line device that supports transparent L2 or routed L3 mode. This allows network managers to use equipment they already own and know, protecting and leveraging their existing investments. The OmniAccess WLAN External Services

Interface (ESI) software module enables the scalable and seamless extension of WAN DMZ services throughout the network.

Policy-based Network Traffic Inspection

Although all "at risk" traffic should be screened, passing all network traffic through network service devices could lead to performance bottlenecks. The OmniAccess WLAN ESI module makes this process more efficient by only forwarding traffic that meets established criteria to service appliances.

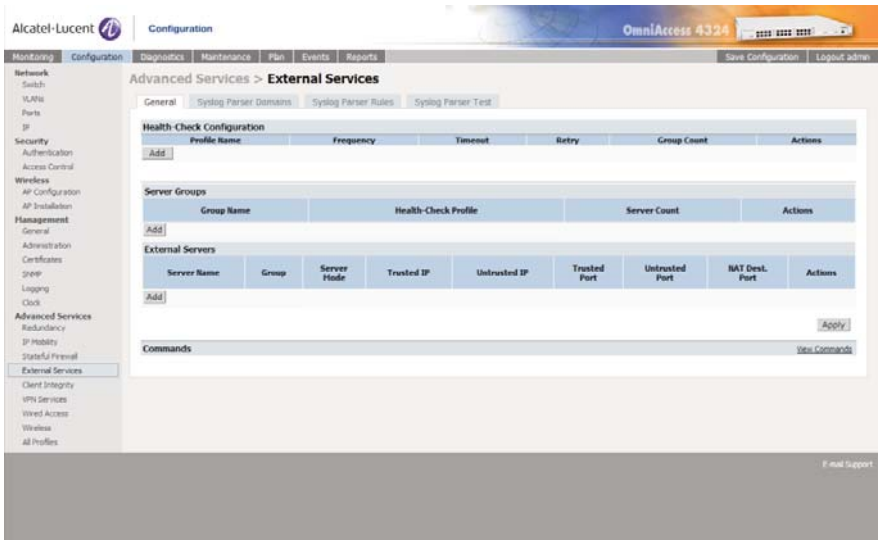
For example, some traffic types, such as Enterprise Resource Planning (ERP) traffic or SQL database transactions, do not carry viruses and do not need to be filtered for virus protection. On the other hand, web, email and file-transfer traffic does require virus filtering. By using the ESI to specify which traffic types are redirected to a network service device, network managers need deploy only enough service capacity for that specified subset of network traffic. Thus, they will not need to deploy as many, if any, additional appliances.

Similarly, the OmniAccess WLAN ESI module can selectively redirect traffic for only certain users or types of users based on authentication or trust state. As an example, enterprises can use endpoint integrity software on employee computers to enforce updates and patches for anti-virus software, personal firewall software and operating systems. If host-based software is up to date on these devices, the network can decide not to perform network-based virus filtering for traffic going to these clients. Alternatively, employees and visitors using their own equipment can be assigned a lower trust level and subjected to strict filtering of all network traffic.

Fault Tolerance for Mission-Critical Networks

The ESI module allows OmniAccess WLAN switches to support health checking and load-balancing of traffic to external devices. Flexible health checking techniques permit the OmniAccess WLAN switches to determine the operational state of external devices without custom software development or vendor lock-in. By health checking a pool of devices, the system can ensure that traffic is not redirected to a device that is down.

Figure 2 External Services Interface configuration screen



Extended Authorization Control Using API

Extended authorization control allows fine-grained control of users from the authentication server. Controls such as automatic disconnection from the network, role re-assignment, and dynamic updates of policies can be enabled.

This functionality is enabled by two Application Programming Interfaces (APIs): IETF standard RFC 3576, and a simple, yet flexible, XML-based API. These APIs both allow external systems to exert user and policy control over an OmniAccess WLAN switch.

Extended authorization control is especially useful in providing guest access, where access can be customized for each visitor, allowing access only to required services and for the exact period of time necessary.

AAA Auto-Selection

The OmniAccess WLAN ESI module now lets enterprises and service providers to provision AAA auto-selection, which redirects users to different authentication servers based on fully qualified domain name (FQDN) or realm. Realms and domains are commonly used in authentication systems. A realm is normally the first part of a username, separated from the actual username by a leading slash. In a Windows Active Directory network, the Active Directory domain is used as the realm. Usernames also often appear in the FQDN format. These addresses appear similar to an email address (e.g., "bob@acme.com").

Enterprise networks can now use this capability to authenticate users from different organizational units. Especially in the case of corporate mergers, it may take months or years to merge the IT infrastructure. The OmniAccess WLAN ESI module makes this integration easy. Realm-based selection of authentication servers allows the users of bothcompanies to use the same network infrastructure while identity information continues to be managed by two different directory services.

TECHNICAL SPECIFICATIONS

Topologies supported
- Transparent (L2)
- Routed (L3)

Load-balancing methods
- Source IP-Destination IP Hash

Health checking
- ICMP Echo
- L2 MAC Frame

External service pools
- 16

Service devices per pool
- 16

To learn more, contact your dedicated Alcatel-Lucent representative, authorized reseller, or sales agent. You can also visit our Web site at www.alcatel-lucent.com.

This document is provided for planning purposes only and does not create, modify, or supplement any warranties, which may be made by Alcatel-Lucent relating to the products and/or services described herein. The publication of information contained in this document does not imply freedom from patent or other protective rights of Alcatel-Lucent or other third parties.

www.alcatel-lucent.com

Alcatel·Lucent