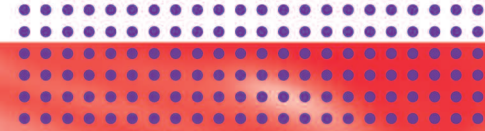


Software básico inalámbrico de Alcatel-Lucent OmniAccess

SOFTWARE DE LAN INALÁMBRICA



Incluido de serie con todos los conmutadores LAN inalámbrica de Alcatel-Lucent OmniAccess (WLAN), el software inalámbrico básico proporciona un control sin precedentes sobre todo el entorno inalámbrico con servicios avanzados y de conmutación LAN inalámbrica centralizada.

El conjunto de funciones básicas del software WLAN de Alcatel-Lucent OmniAccess, que se detalla a continuación, incluye autenticación sofisticada y cifrado, protección frente a los AP no autorizados, movilidad sin fisuras con itinerancia rápida, gestión de RF y herramientas de análisis, configuración centralizada, seguimiento de ubicación, etc.

El software básico de LAN OmniAccess se puede complementar con módulos opcionales, entre los que se incluyen Protección contra intrusiones inalámbricas, Firewall acorde con políticas, Servidor VPN, Integridad de clientes, AP remoto, Interfaz de servicios externos y Cifrado de L2 avanzado xSec.



F U N C I O N E S

- Control de acceso, cifrado y autenticación seguros
- Movilidad sin fisuras
- Gestión de RF, planificación de RF y solución de problemas

V E N T A J A S

- Autenticación 802.1X con WPA, WPA2 y 802.11i
- Motor de cifrado basado en hardware programable y ampliable a los estándares de seguridad más recientes
- Portal cautivo basado en Web para autenticación basada en explorador SSL
- Detección, clasificación y contención automáticas de los puntos de acceso no autorizados
- Los tiempos de cambio de itinerancia de 2-3 milisegundos permiten handoffs (traspasos) muy rápidos para las aplicaciones sensibles a los retrasos
- Proxy IP móvil y proxy DHCP permiten que los usuarios se desplacen sin problemas entre APs y conmutadores WLAN
- Gestión automática de radio (ARM) para la configuración automática y sencilla de todos los parámetros de RF
- Estudio del emplazamiento en directo para controlar y mostrar en tiempo real la interferencia y la cobertura de RF
- Diseño, planificación y colocación automáticos de los AP y monitores de RF basados en requisitos de capacidad, cobertura y seguridad
- Las herramientas de captura de paquetes proporcionan instantáneas detalladas de todo el entorno inalámbrico

F U N C I O N E S

- Alta disponibilidad de gestión de redes
- Compatibilidad con QoS, VoIP y seguimiento de localización

Autenticación, cifrado y control de acceso seguros

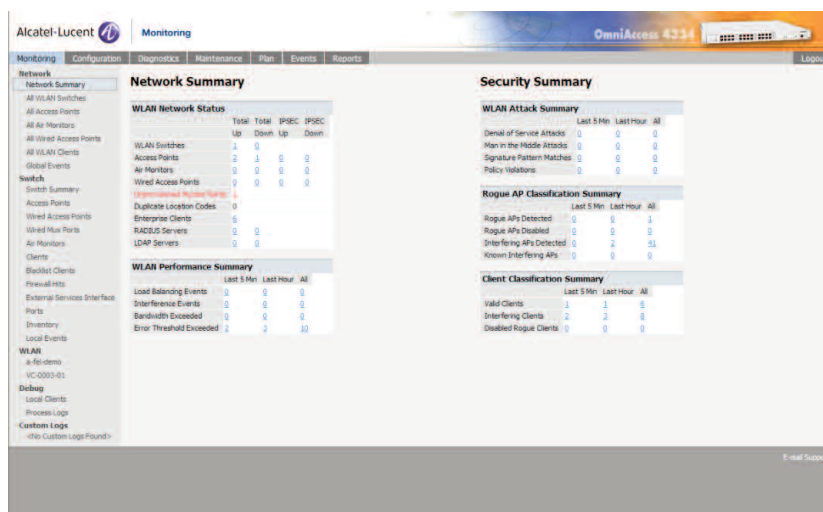
El software WLAN de OmniAccess proporciona funciones líderes en el sector que protegen el espacio, los dispositivos, los usuarios y los datos de la red inalámbrica de la empresa. Es compatible con una amplia gama de métodos de autenticación, entre los que se incluyen los protocolos WPA2 y 802.11i estándar en el sector, ampliamente reconocidos como de última generación en la seguridad inalámbrica. El software WLAN de OmniAccess proporciona tecnologías de cifrado de capa 2 más recientes y, gracias a su procesador de cifrado de hardware programable, el conmutador WLAN de OmniAccess se puede actualizar de forma inmediata para admitir estándares de cifrado emergentes.

Para los clientes sin WPA, VPN u otro software de seguridad, el sistema inalámbrico OmniAccess admite un portal cautivo basado en Web que proporciona una autenticación basada en explorador estándar. La autenticación del portal cautivo se cifra mediante SSL (Secure Sockets Layer) estándar en el sector y puede admitir tanto a usuarios registrados con un nombre de usuario y una contraseña como a usuarios invitados que sólo proporcionan una dirección de correo electrónico. A través de la integración con sistemas finales, el portal cautivo puede proporcionar una solución segura de acceso a invitados, lo que permite que al personal de recepción

V E N T A J A S

- Todos los conmutadores WLAN y los AP se controlan y gestionan de forma centralizada
- Conjuntos de conmutadores WLAN que utilizan VRRP
- La tolerancia a fallos de RF automática evita los puntos muertos de radio y proporciona una copia de seguridad de AP
- Compatible con 802.11e, WMM y 802.1p
- Control de admisión de llamadas y control de RF sensible a la voz
- Ubicación de cualquier dispositivo 802.11 con visualización en tiempo real

Figura 1



emitir credenciales de autenticación para los visitantes y realizar un seguimiento de éstas.

Para protegerse frente a los dispositivos inalámbricos no autorizados, los algoritmos de clasificación de AP de WLAN de OmniAccess permiten que el sistema distinga de forma precisa entre los AP "no autorizados" amenazantes instalados en la red local y los AP "de interferencias" cercanos. Una vez clasificados como no autorizados, estos AP se deshabilitan automáticamente tanto en las redes inalámbricas como en las cableadas. También se notifica a los administradores la presencia de dispositivos no autorizados, junto con la ubicación física exacta en un plano de plantas para facilitar su eliminación de la red.

Movilidad sin fisuras

El software WLAN de OmniAccess proporciona conectividad inalámbrica sin fisuras mientras el usuario se desplaza por la red. Con tiempos de cambio de itinerancia de 2 a 3 milisegundos, las aplicaciones persistentes y sensibles a los retrasos, como las aplicaciones de voz y Citrix experimentan un rendimiento ininterrumpido. El software WLAN de OmniAccess integra funciones de proxy IP móvil y proxy DHCP que permiten que los usuarios se desplacen entre las subredes, los AP y los conmutadores WLAN sin necesidad de un software cliente especial. Gracias a la agrupación de VLAN, la condición de usuario de VLAN se equilibra para mantener un rendimiento de red óptimo cuando se mueven por la red grupos grandes de usuarios.

Gestión y planificación de RF y solución de problemas

La función de gestión automática de radio (ARM) de WLAN de OmniAccess elimina el trabajo de invitado en los despliegues de AP. Una vez desplegados los AP, estos empiezan inmediatamente a controlar su entorno local en busca de interferencias, ruidos y señales que se reciben de otros AP. Esta información se envía de nuevo al conmutador WLAN central, que puede así controlar los niveles de potencia y la asignación de canal óptimos para cada AP de la red.

Una vez desplegada la red, la función de estudio del emplazamiento en directo de WLAN de OmniAccess proporciona una visualización a color en tiempo real del entorno de RF que muestra la fuerza de la señal, la cobertura y la interferencia. El estudio de emplazamiento en directo permite la planificación de capacidad y cobertura WLAN y evita la necesidad de realizar estudios de emplazamiento manuales caros y frecuentes.

Al trabajar con los puntos de acceso y los monitores inalámbricos de OmniAccess para explorar de forma constante todos los canales de las bandas de 2,4 Ghz y 5 Ghz, el software inalámbrico de OmniAccess recoge datos estadísticos agregados y sin procesar por estación, canal y usuario. Todas las estadísticas se pueden mostrar en las herramientas de solución de problemas intuitivas inalámbricas de OmniAccess y también están disponibles a través de SNMP para su integración fácil en las aplicaciones de análisis y gestión de otros fabricantes. La captura de paquetes en directo está disponible para permitir la conversión de cualquier AP o monitor inalámbrico de OmniAccess en un dispositivo de captura de paquetes, capaz de devolver los marcos de nivel 802.11 en directo a las estaciones de control como Ethereal, Air Magnet Laptop Analyzer o WildPackets

AiroPeek NX. Con esta información detallada, los administradores pueden resolver rápidamente los problemas de los usuarios, determinar los principales interlocutores inalámbricos y diagnosticar los AP congestionados.

Compatibilidad con QoS, VoIP y seguimiento de localización

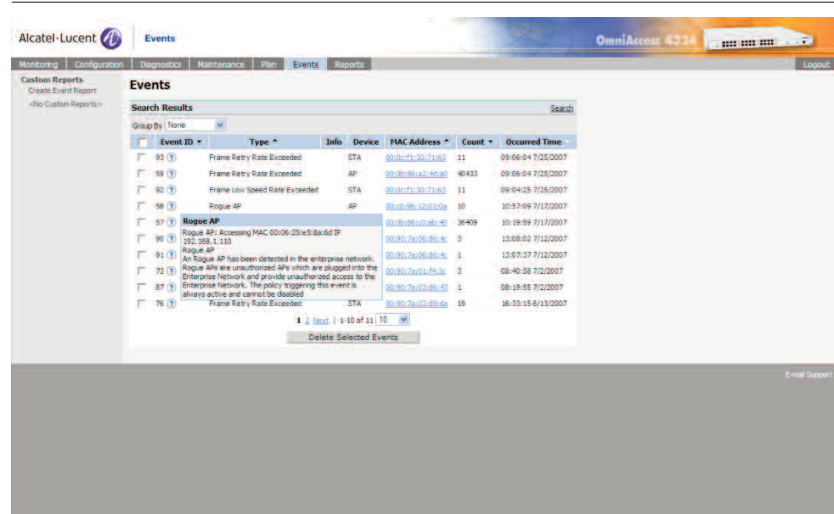
La compatibilidad con 802.11e y WMM garantiza una QoS inalámbrica para aplicaciones sensibles a los retrasos con asignación entre etiquetas 802.11e y colas de hardware internas. Los conmutadores WLAN de OmniAccess también admiten la asignación de etiquetas 802.1p y DiffServ para colas de hardware de la QoS con cable. Las capacidades de QoS de capa 2 se han mejorado para la capa 3+gestión de flujo y DiffServ mediante el módulo adicional Firewall acorde con políticas.

Para voz sobre despliegues de WLAN (VoWLAN), la clasificación de flujos de voz (VFC) automática e inalámbrica de OmniAccess identifica y da prioridad de forma automática a las llamadas de voz

para garantizar la transmisión de latencia baja. El control de admisión de llamadas gestiona las asociaciones de dispositivos de voz y las llamadas de descolgado activas para garantizar una disponibilidad del ancho de banda en las llamadas de voz en cada AP. Con el fin de ofrecer un rendimiento ininterrumpido, la monitorización de RF sensible a la voz garantiza que los AP no establezcan un ciclo con el modo de control opcional cuando un cliente está cerca.

El software WLAN de OmniAccess incluye la visualización de localización avanzada y el seguimiento de los dispositivos 802.11z. La triangulación de localización basada en firma por RF permite que los administradores localicen físicamente cualquier dispositivo o usuario 802.11 con una precisión de un metro. Con las funciones de seguimiento de localización en tiempo real inalámbricas de OmniAccess se pueden localizar de forma continua varios dispositivos y realizar un seguimiento simultáneo de los mismos.

Figura 2



The screenshot shows the 'Events' page in the Alcatel-Lucent OmniAccess 4334 management interface. It features a search results table with columns for Event ID, Type, Info, Device, MAC Address, Count, and Occurred Time. The table lists several events, including 'Frame Retry Rate Exceeded', 'Rogue AP', and 'Rogue AP Accessing MAC 00:06:25:e5:8a:d3'. A 'Delete Selected Events' button is visible at the bottom of the table.

Event ID	Type	Info	Device	MAC Address	Count	Occurred Time
93	Frame Retry Rate Exceeded	STA	00:0c:12:01:43	11	09-06-04 7:05:2007	
99	Frame Retry Rate Exceeded	AP	00:0c:12:01:43	40433	09-06-04 7:05:2007	
82	Frame Low Speed Rate Exceeded	STA	00:0c:12:01:43	11	09-04-25 7:05:2007	
98	Rogue AP	AP	00:0c:12:01:43	10	02:57:09 7:17:2007	
97	Rogue AP	00:0c:12:01:43		36409	01:19:19 7:17:2007	
80	Rogue AP Accessing MAC 00:06:25:e5:8a:d3 (22:268.2.110)	00:0c:12:01:43		3	13:08:02 7:12:2007	
81	Rogue AP	00:0c:12:01:43		1	13:07:37 7:12:2007	
73	An Rogue AP has been detected in the enterprise network. Rogue APs are unauthorized APs which are plugged into the Enterprise Network and provide unauthorized access to the Enterprise Network. The policy triggering this event is always active and cannot be disabled.	00:0c:12:01:43		3	08:40:58 7:02:2007	
87	Frame Retry Rate Exceeded	STA	00:0c:12:01:43	1	08:18:55 7:02:2007	
76	Frame Retry Rate Exceeded	STA	00:0c:12:01:43	19	16:33:15 6/13/2007	

Autenticación, cifrado y control de acceso seguros

TIPOS DE AUTENTICACIÓN

- IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAPTTLS, EAP-FAST)
- RFC 2548 - Atributos RADIUS específicos del proveedor de Microsoft
- RFC 2716 - PPP EAP-TLS
- RFC 2865 - Autenticación RADIUS
- RFC 3576 - Extensiones de autorización dinámica para RADIUS
- RFC 3579 - Compatibilidad de RADIUS con EAP
- RFC 3580 - Directrices IEEE 802.1X para RADIUS
- RFC 3748 - Protocolo de autenticación extensible
- Autenticación de direcciones MAC
- Autenticación del portal cautivo basado en Web

SERVIDORES DE AUTENTICACIÓN

- Base de datos interna
- LDAP/ SSL LDAP segura
- RADIUS
- TACACS+
- Interoperabilidad probada con los servidores de autenticación de otros fabricantes: Microsoft Active Directory, Microsoft IAS RADIUS
- Servidor, Servidor Cisco ACS Server, Servidor Funk Steel Belted RADIUS, servidor RSA ACE, Infoblox, Interlink RADIUS
- Servidor, FreeRADIUS, A-10 Networks IDSentrie

TIPOS DE CIFRADO

- WEP: 64 y 128 bits
- WPA-TKIP, WPA-PSK-TKIP, WPA-AES, WPA-PSK-AES
- WPA2/802.11i: WPA2-AES, WPA2-PSK-AES, WPA2-TKIP, WPA2-PSK-TKIP
- Secure Sockets Layer (SSL) y TLS: RC4 128-bits y RSA 1024- y 2048-bits
- Hardware programable ampliable a los nuevos mecanismos de cifrado
- Detección de AP no autorizados: Sí
- Clasificación de AP no autorizados: Sí
- Contención de AP no autorizados: Con cables e inalámbricos

Movilidad sin fisuras

- Itinerancia rápida: 2-3 mseg dentro del conmutador; 10-15 mseg entre conmutadores
- Itinerancia entre subredes y VLAN: Sí
- Compatible con teléfonos Mobile IP: Sí
- Proxy Mobile IP: Sí
- Proxy DHCP: Sí
- Agrupación VLAN: Sí

Gestión y planificación de RF y solución de problemas

- Gestión adaptativa de radio (ARM): Sí
- Varios ESSID por AP: Hasta 16
- Calibración automática de AP: Sí
- Autorrecuperación en torno a los AP que fallan: Sí
- Equilibrio de carga — número de usuarios: Sí
- Equilibrio de carga — basado en el uso: Sí
- Control de acceso AP basado en temporizador: Sí
- Herramienta de implantación y planificación de RF: Sí
- RMON inalámbrica/captura de paquetes: Sí
- Complementos para las herramientas de análisis de otros fabricantes: Ethereal, AiroPeek, AirMagnet
- Extensiones de 802.11h a 5 GHz para Europa: Sí
- 802.11d Dominios regulatorios adicionales: Sí

Gestión de redes y alta disponibilidad

- Configuración basada en Web: Sí
- Línea de comandos: Consola, telnet, SSH
- Syslog: Sí
- SNMP v2c: Sí
- SNMP v3: Sí
- MIB privado Aruba: Sí
- MIB-II: Sí
- Configuración centralizada de conmutadores WLAN locales 128
- Actualización de imagen centralizada para conmutadores WLAN y todos los AP: Sí
- VRRP: Sí
- Compatibilidad con centros de datos redundantes: Sí

Calidad de servicio, compatibilidad con VoIP y seguimiento de localización

- Compatible con 802.1p: Sí
- Compatible con 802.11e: Sí
- T-SPEC/TCCLAS: Sí
- WMM: Sí
- Monitorización/control de RF sensible a voz: Sí, basado en sesiones
- Control de admisión de llamadas: Sí
- Clasificación de flujos de voz automática (VFC): SIP, SVP, SCCP
- U-APSD (Unscheduled Automatic Power Save Delivery, ahorro de energía no programado): Sí
- IGMP Snooping para suministro multicast eficaz: Sí
- Control y seguimiento de localización en tiempo real: Sí
- API de seguimiento de localización para integración externa: Sí

Conmutación general

- RFC 1812 - Requisitos para routers IP versión 4 RFC 1519 CIDR
- RFC 1256 - IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 - Requisitos de host
- RFC 768 - UDP
- RFC 791 - IP
- RFC 792 - ICMP
- RFC 793 - TCP
- RFC 826 - ARP
- RFC 894 - IP sobre Ethernet
- RFC 1027 - Proxy ARP
- RFC 2338 - VRRP
- RFC 2516 - Protocolo de punto a punto sobre Ethernet (PPPoE)
- IEEE 802.1D - 1998 protocolo de árbol de expansión (STP) IEEE 802.1Q -1998 redes de área local conectadas virtuales

Inalámbrico

- IEEE 802.11a/b/g 5GHz, 2,4 GHZ, 2,4 GHz Alta velocidad
- IEEE 802.11d Dominios regulatorios adicionales
- IEEE 802.11e Calidad de servicio
- IEEE 802.11h Extensiones de la potencia de transmisión y espectro para 5GHz en Europa
- IEEE 802.11i Mejoras de la seguridad MAC

VLAN

- IEEE 802.1Q Etiquetado de VLAN
- VLAN basadas en puerto

Políticas y calidad de servicio

- IEEE 802.1D-1998 (802.1p) Prioridad del paquete
- IEEE 802.11e Mejoras de la calidad del servicio
- RFC 2474 - Servicios diferenciados

Análisis del tráfico y la gestión

- RFC 2030 - SNMP, Protocolo de tiempo de la red simple v4
- RFC 854 - Servidor y cliente Telnet
- RFC 783 - Protocolo TFTP (revisión 2)
- RFC 951, 1542 - BootP
- RFC 2131 - Protocolo dinámico de configuración de host
- RFC 1591 - DNS (operación del cliente)
- RFC 1155 - Estructura de la información gestionada (SMIv1)
- RFC 1157 - SNMPv1
- RFC 1212 - Definiciones de MIB concisas.
- RFC 1213 - Base de información de gestión para gestión de redes de Internet basado en TCP/IP - MIB-II
- RFC 1215 - Convención para definir las alertas para su uso con SNMP
- RFC 1573 - Evolución de interfaces
- RFC 2011 - Base de información de gestión de SNMPv2 para el protocolo de Internet que utiliza SMIv2
- RFC 2012 - Información de gestión de SNMPv2
- RFC 2013 - Información de gestión de SNMPv2

- RFC 2578 - Estructura de la información de gestión versión 2 (SMIv2)
- RFC 2579 - Convenciones textuales para SMIv2
- RFC 2863 - MIB del grupo de interfaces
- RFC 3418 - Base de información de gestión (MIB) para gestión del protocolo simple de gestión de redes (SNMP)
- RFC 959 - Protocolo de transferencia de archivos (FTP)
- RFC 2660 - Protocolo de transferencia de hipertexto seguro (HTTPS)
- RFC 1901 - 1908 SNMP v2c, SMIv2 y MIB-II revisado
- RFC 2570 - 2575 SNMPv3, autenticación, cifrado y seguridad basada en el usuario
- RFC 2576 - Coexistencia entre SNMP versión 1, versión 2 y versión 3
- RFC 2233 - Interfaz MIB
- RFC 2251 - Protocolo ligero de acceso a directorios (v3)
- RFC 1492 - Protocolo de control de acceso, TACACS+
- RFC 2865 - RADIUS (Remote Authentication Dial-In User Service, Servicio de usuario de acceso telefónico de autenticación remota).
- RFC 2866 - Tarificación de RADIUS
- RFC 2869 - Extensiones de RADIUS
- RFC 3576 - Extensiones de autorización dinámica para RADIUS remoto
- RFC 3579 - Compatibilidad con RADIUS para el protocolo de autenticación extensible (EAP)
- RFC 3580 - IEEE 802.1X para RADIUS (Remote Authentication Dial In User Service, Servicio de usuario de acceso telefónico de autenticación remota).
- RFC 2548 - Atributos RADIUS de Microsoft
- RFC 1350 - Protocolo TFTP (revisión 2)
- Servidor Secure Shell (SSHv2)
- Registro de configuración
- Múltiples imágenes, múltiples configuraciones
- BSD Protocolo de registro de sistema (SYSLOG, System Logging Protocol), con varios servidores Syslog.

Seguridad/cifrado

- RFC 1661 - Protocolo de punto a punto (PPP)
- RFC 2406 - Carga de seguridad IP encapsulada (ESP)
- RFC 2661 - Protocolo de túnel de capa dos "L2TP"
- RFC 3193 - L2TP garantizado con IPsec
- RFC 2451 - Algoritmos de cifrado en modo ESP CBC
- RFC 2403 - Uso de HMAC-MD5-96 en ESP y AH
- RFC 2401 - Arquitectura de seguridad para el Protocolo Internet, RFC
- RFC 2408 - Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP)
- RFC 2409 - El intercambio de claves en Internet (IKE)
- RFC 2405 - El Algoritmo de cifrado DES-CBC en ESP con IV explícito
- RFC 2403 - Uso de HMAC-SHA-1-96 en ESP y AH
- RFC 3602 - Algoritmo de cifrado AES-CBC y su uso con IPsec
- RFC 4017 - Requisitos del método del Protocolo de autenticación extensible (EAP) para LAN inalámbricas
- RFC 3706 - Método de detección de puntos inactivos de intercambio de claves de Internet (IKE) basado en tráfico
- RFC 3947 - Negociación de paso NAT en el IKE
- RFC 3748 - Protocolo de autenticación extensible (EAP)
- RFC 3079 - Claves derivadas para su uso con cifrado punto a punto de Microsoft (MPPE)
- RFC 4137 - Máquinas de estado para el autenticador y el par del Protocolo de autenticación extensible (EAP)
- RFC 2716 - Protocolo de autenticación extensible PPP EAP TLS
- RFC 2246 - Protocolo TLS (SSL)
- RFC 2407 - El Dominio de Interpretación de Seguridad IP en Internet para ISAKMP
- RFC 3948 - Encapsulación de UDP de paquetes IPsec
- Borrador de Internet - EAP-TTLS
- Borrador de Internet - EAP-PEAP
- Borrador de Internet - EAP-POTP
- Borrador de Internet - XAuth para ISAKMP

Para obtener más información, consulte con su representante exclusivo de Alcatel-Lucent, revendedor autorizado o agente comercial. También puede visitar nuestro sitio Web en www.alcatel-lucent.com.

La finalidad del presente documento es meramente informativa y no pretende crear, modificar o completar ninguna de las garantías que pudiera ofrecer Alcatel-Lucent para cualquiera de los productos y/o servicios en él descritos. La publicación de la información incluida en el presente documento no implica que no existan patentes ni otros derechos de protección de Alcatel-Lucent u otras marcas.

www.alcatel-lucent.com

Alcatel, Lucent, Alcatel-Lucent y el logotipo de Alcatel-Lucent son marcas comerciales de Alcatel-Lucent. Las demás marcas registradas pertenecen a sus respectivos propietarios. Alcatel-Lucent no se responsabiliza de la exactitud de la información aquí expuesta, que puede ser modificada sin previo aviso.
© 2008 Alcatel-Lucent. Reservados todos los derechos. ES - 4288342 Rev. B 3/08