Release Notes

OmniAccess 5510 USG

Release 3.0

These release notes accompany release 3.0 software for the OmniAccess 5510 USG hardware (OmniAccess 5510 ADSL Annex A/Annex B Unified Services Gateway, OmniAccess 5510 SR Unified Services Gateway, and OmniAccess 5510 TE Unified Services Gateway). They provide important information on individual software features and hardware modules. Since much of the information in this release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

Related Documentation

This release notes should be used in conjunction with the OmniAccess 5510 USG hardware. The following are the titles and descriptions of the user manuals that apply to the OmniAccess 5510 USG.

User manuals can be downloaded at:
http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

- ***OmniAccess 5510 Unified Services Gateway Getting Started Guide***
  Describes the hardware and software procedures for getting an OmniAccess 5510 USG up and running.
- ***OmniAccess 5510 Unified Services Gateway Hardware Users Guide***
  Complete technical specifications and procedures for the OmniAccess 5510 USG chassis, power supplies.
- ***OmniAccess 5510 Unified Services Gateway CLI Configuration Guide***
  Includes network configuration procedures and descriptive information on all the major software features and protocols available on the OmniAccess 5510 USG in the base software package.
- ***OmniAccess 5510 Unified Services Gateway CLI Command Reference Guide***
  Complete reference to all commands supported on the OmniAccess 5510 USG. Includes syntax definitions, default values, and examples.
- ***OmniAccess 5510 Unified Services Gateway Web GUI Users Guide***
  Describes the basic configuration of the OmniAccess 5510 USG using the Web Graphical User Interface (GUI) tool - Unified Services Gateway Configuration Manager (USGM).

System Requirements

Memory Requirements

- OmniAccess 5510 USG Release 3.0 requires 256 MB RAM, 256 MB internal storage media and 16 MB boot flash on the base system. This is the standard configuration shipped.

- Configuration files and the compressed software images including web management software (USGM) images are stored in the internal storage media.

Software Requirements

The software versions listed in this section are the minimum required, except where otherwise noted.

- Firmware version - fw-5510-2.0.npm
- ALU apps version - alu-apps.5510.3.0.0.97.0.npm

Supported Hardware/Software Combinations

The following table shows the hardware supported in release 3.0:

Alcatel-Lucent Marketing Number	Part Number	Release 3.0
OmniAccess 5510-AA USG	902695-90	Supported
OmniAccess 5510-AB USG	902768-90	Supported
OmniAccess 5510-SR USG	902697	Supported
OmniAccess 5510-TE USG	902696	Supported

To determine the OmniAccess 5510 USG hardware configuration, use the '**show chassis**' command. The following is an example of the show chassis command on the OmniAccess 5510-ADSL Annex A and OmniAccess 5510-ADSL Annex B USG:

```
ALU(config)# show chassis

        Physical inventory at Wed Jul  7 14:01:31 2010
        System started approximately Wed Jul  7 14:00:33 2010
        Uptime is 0 days 0 hours 0 minutes 58 seconds
        Current temperature is  42.5 Celsius

OA5510 - OA5510 ADSL ANNEX A (active)
        Part number: 902695-90
        Module type: 00002003
        Serial number:  L0286699
        Revision: D01
        FRU#: 902695-90
        Format: 3
        Base MAC (MAC bank 1): 00:e0:b1:dd:d1:1e
        ADSL Loader version: 1.2


ALU(config)# show chassis

        Physical inventory at Wed Jul  7 13:57:44 2010
        System started approximately Fri Jul  2 18:43:08 2010
        Uptime is 4 days 19 hours 14 minutes 36 seconds
        Current temperature is  53.5 Celsius

OA5510 - OA5510 ADSL ANNEX B (active)
        Part number: 902768-90
        Module type: 00002004
        Serial number:  K5180823
        Revision: D01
        FRU#: 902758-90
        Format: 3
        Base MAC (MAC bank 1): 00:e0:b1:da:30:c8
        ADSL Loader version: 1.2
```

To view the version information of the running package and flash image, use **show version** command.

```
ALU(config)# show version

Alcatel-Lucent Software, Version 3.0.0, Build 81
 Copyright (c) 2003-2010 by Alcatel-Lucent Inc.
 Built on Mon Jun 28 13:21:55 IST 2010

 Flash version – 2.0
```

Hardware Supported

The following hardware is supported subject to the feature exceptions and problem reports described later in this release notes.

Note. See *OmniAccess 5510 Unified Services Gateway Hardware Users Guide* for more information on the OmniAccess 5510 USG hardware features.

OmniAccess 5510 Unified Services Gateway

OmniAccess 5510 USG is designed to provide most commonly used network services such as routing, switching, wide area network (WAN) connectivity, network security with firewall, and related services using a non-modular platform providing Ethernet switching and a single WAN interface.

OmniAccess 5510 USG is a fanless 1U fixed chassis containing 4 10/100 Switched Ethernet ports, 1 10/100 Ethernet port, and either a T1E1 port/Universal Serial Port (USP)/ADSL Annex A or Annex B port.

OmniAccess 5510 USG Ports

ADSL Port

Asymmetric Digital Subscriber Line (ADSL) takes its name from the comparatively high bandwidth downstream with low bandwidth upstream. It works over the same copper already installed by the telephone companies for voice traffic and is “always on” as compared to dial up services.

The distinguishing characteristic of ADSL is that the volume of data flow is greater in one direction than the other, that is, it is asymmetric. ADSL supports applications with "asymmetric" traffic demand such as web surfing, file downloads, and telecommuting. Providers usually market ADSL as a service for people to connect to the Internet in a relatively passive mode: able to use the higher speed direction for the "download" from the Internet but not needing to run servers that would require bandwidth in the other direction. Advantage of ADSL is that it allows users to have telephone conversations and transfer data simultaneously.

Alcatel-Lucent OmniAccess 5510 USG is available in both Annex A and Annex B flavours of ADSL. Annex A supports ADSL over POTS (Plain Old Telephone System) and Annex B supports ADSL over ISDN (Integrated Services Digital Network).

T1E1 Port

The T1E1 port supports American and European (International) digital transmission standards. The T1E1 port can support data rates of 1.544 or 2 Mbps depending on the type of connectivity.

USP (Universal Serial Port)

The serial interface or USP provides a single WAN serial interface. The serial interface can support V.35 and X.21 at 2.048 Mbps bidirectional, and RS-232 in DTE mode at 256Kbps bidirectional. V.35, X.21 and RS-232 are well known communication protocols over synchronous serial lines.

- **V.35 Interface**
  The V.35 interface was originally specified by CCITT as an interface for 48 Kbps line transmissions. It has been adopted for all line speeds above 20 Kbps. V.35 is a mixture of balanced and common earth signal interfaces. The control lines including DTR, DSR. DCD, RTS, and CTS are single wire common earth interfaces. The data and clock signals are balanced signals.
- **X.21 Interface**
  The physical interface between the DTE and the DCE is defined in ITU-T recommendation as X.21. The DCE provides a full-duplex, bit-serial, synchronous transmission path between the DTE and the local PSE. It can operate at data rates from 600 bps.
- **RS-232 Interface**
  RS-232 is specified by Electronic Industries Association. It specifies signal voltage, timing, function, a protocol for information exchange, and mechanical connectors. Signal function includes signal for ground, data interchange, flow control, control of the remote modem, modem status and control signals. For synchronous communication, these signals provide timing information for the transmitter and receiver, which may operate at different baud rates.

10/100 Switched Ethernet Ports

The 10/100 Switched Ethernet ports provide Layer-2 switching functions. The L2 ports are 4 RJ-45 interfaces. These interfaces can auto-negotiate, transmit, and receive data packets at the rate of 10/100 Mbps.

10/100 Fast Ethernet Port

The Fast Ethernet port provides layer-3 connectivity and can auto-negotiate, transmit, and receive data packets at the rate of 10/100 Mbps.

USB Port

This port is used to connect a USB device for software upgrades, backup, and restoring data.

Software Features Supported

The following software features are supported, subject to the feature exceptions and problem reports described later in this release notes:

Feature Summary

Feature	Platform	Software Package
AAA		
Local Authentication	**all**	**base**
RADIUS	**all**	**base**
TACACS+	**all**	**base**
Filter and Firewall		
Stateful Packet Inspection and Filtering	**all**	**base**
Denial-of-Service Attack Prevention	**all**	**base**
Network Address Translation (NAT)	**all**	**base**
ALGs (TFTP, FTP, DNS, RTSP, SIP)	**all**	**base**
GRE	**all**	**base**
Intrusion Detection / Intrusion Prevention		
Detection Mode	**all**	**base**
Prevention Mode	**all**	**base**
Group-based IDS/IPS	**all**	**base**
LAN Protocols		
STP	**all**	**base**
Bridging	**all**	**base**
Integrated Routing and Bridging	**all**	**base**
Multicast Protocols	**all**	**base**
PIM –SM	**all**	**base**
IGMP v1, v2	**all**	**base**
Network Services		
DHCP Server	**all**	**base**
DHCP Relay	**all**	**base**
TFTP Server	**all**	**base**
TFTP Client	**all**	**base**
DNS Client	**all**	**base**
FTP Client	**all**	**base**
SSH Server/Client	**all**	**base**
HTTP/HTTPS Server	**all**	**base**
Telnet Client/Server	**all**	**base**
License Manager	**all**	**base**

Quality of Service (QoS)		
Egress Queues	**all**	**base**
Traffic Policing	**all**	**base**
Weighted Fair Queuing	**all**	**base**
WRED	**all**	**base**
Priority Egress Scheduling	**all**	**base**
Egress Shaping	**all**	**base**
DSCP/TOS Marking	**all**	**base**
Auto QoS (diffserv, voice)	**all**	**base**
Hierarchical Queuing	**all**	**base**
Qos Pre-classify (QoS policies on tunneled/encrypted packets)	**all**	**base**
QoS Marking/Policing	**all**	**base**
QoS on FR, MLPPP	**OmniAccess 5510-SR USG OmniAccess 5510-TE USG**	**base**
Routing		
RIPv1/RIPv2	**all**	**base**
OSPF	**all**	**base**
BGP	**all**	**base**
Policy Based Routing	**all**	**base**
VRRP	**all**	**base**
Virtual Routing and Forwarding (VRF)	**all**	**base**
System Management and Logging		
CLI (Console, Telnet, SSH)	**all**	**base**
USGM (HTTP, HTTPS)	**all**	**base**
USGM Wizards (Firewall, VPN, QoS)	**all**	**base**
SNMP (v1, v2, v3)	**all**	**base**
Syslog Forwarding	**all**	**base**
Standard & Custom MIBs	**all**	**base**
Ping, Traceroute	**all**	**base**
Hitless Component Upgrades	**all**	**base**
VPN (IPsec)		
Site-to-site VPN Tunnels	**all**	**base**
Tunnel Interfaces	**all**	**base**
DES, 3DES, AES Encryption	**all**	**base**
MD-5 and SHA-1 Authentication	**all**	**base**
IKE with Pre-shared Key	**all**	**base**
PKI	**all**	**base**
NAT Traversal	**all**	**base**
Perfect Forward Secrecy (DH Groups)	**all**	**base**
Multiple Peer Support	**all**	**base**
DPD (Dead Peer Detection)	**all**	**base**
WAN Features and Protocols		
HDLC	**OmniAccess 5510-SR USG OmniAccess 5510-TE USG**	**base**

Frame Relay	**OmniAccess 5510-SR USG** **OmniAccess 5510-TE USG**	**base**
PPP	**OmniAccess 5510-SR USG** **OmniAccess 5510-TE USG**	**base**
PPPoE	**all**	**base**
MLPPP	**OmniAccess 5510-SR USG** **OmniAccess 5510-TE USG**	**base**
Link Fragmentation and Interleaving (LFI) over FR and MLPPP	**OmniAccess 5510-SR USG** **OmniAccess 5510-TE USG**	**base**

New Software Features and Enhancements

The following software features are new with the 3.0 release, subject to the feature exceptions and problem reports described later in this release notes:

Feature	Platform	Software Package
Network Services		
DHCP Client	**all**	**base**
DDNS Client	**all**	**base**
TR-069 Client	**all**	**base**
Quality of Service (QoS)		
L2 QoS	**all**	**base**
ATM QoS	**OmniAccess 5510-AA/AB USG**	**base**
Intrusion Detection / Intrusion Prevention		
Snort engine upgraded to version 2.8.5	**all**	**base**
Filter and Firewall		
L2 Filter	**all**	**base**
Hosted SIP ALG	**all**	**base**
System Management and Logging		
Factory Default Configuration	**all**	**base**
VPN (IPsec)		
IPsec VPN Server	**all**	**base**
DMVPN	**all**	**base**
Network Services		
Time bound licenses (for IPsec)	**all**	**base**
WAN Features and Protocols		
OAM	**all**	**base**
BCP	**all**	**base**
ADSL - Multiple PVC	**OmniAccess 5510-AA/AB USG**	**base**
Multiple Encapsulation over ATM Adaptation Layer 5 (MER/1483 Bridged mode/1483 Routed mode PPPoA/PPPoE)	**OmniAccess 5510-AA/AB USG**	**base**

Feature Descriptions

Authentication Features

AAA (Authentication, Authorization, and Accounting) is a system in IP-based networking to control the resources that users have access to and to keep track of the user activity over a network.

Local Authentication

Allows a user to be authenticated against the local database.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a standard protocol that provides centralized authentication and accounting services for remote users. The OmniAccess 5510 USG can be configured to authenticate remote users against a RADIUS server.

TACACS+

TACACS+ is a protocol that can be used to communicate with a TACACS+ authentication server. The OmniAccess 5510 USG can be configured to authenticate remote users against a TACACS+ server.

Firewall

Firewall is a network element that uses software intelligence to filter traffic between trusted and untrusted zones. Firewalls can monitor the flow of traffic, and decide to either permit or deny the communication that is being attempted.

Stateful Packet Inspection and Filtering

A stateful packet filter records the status of all connections and allows only those packets that are associated with a current connection.

Packet Filtering

This is a simple firewall solution that is usually implemented on devices like routers that filter packets. The packet-headers are inspected when going through the firewall. Packets are analyzed against a set of rules. Depending on these rules, the packet is either accepted or denied.

Stateful Inspection

This is an advanced implementation of packet filtering that inspects packets at higher network layers, up to the application layer. Such filters interpret transport-level information (such as TCP and UDP headers) to analyze and record all current connections.

Denial-of-Service

A Denial-of-Service (DoS) attack is a malicious attempt by one or many users to limit or completely disable the availability of a service. The OmniAccess 5510 USG provides an effective way to prevent these attacks against their networks. The OmniAccess 5510 USG employs rate limiting and rule based filtering to prevent these attacks.

Network Address Translation (NAT)

NAT mechanism translates un-registered "private" IP addresses used in an internal network to a real "registered" IP on external networks such as the Internet. The OmniAccess 5510 USG supports three types of NAT: Port Translation, Static NAT, and Dynamic NAT.

Application Layer Gateway

An ALG has the capability to conduct stringent packet inspection and thereby augment the security infrastructure. Besides using a specialized program for each type of application or service that needs to pass through the firewall, the OmniAccess 5510 USG can look for altered data, potentially harmful traffic, data appropriateness, and also has the capability to log these. The OmniAccess 5510 USG can perform ALG functions for the following protocols: TFTP, FTP, DNS, RTSP, and SIP ALG.

GRE

Generic Routing Encapsulation (GRE) is a simple, stateless protocol that allows for the tunneling of traffic. IP is used as transport for GRE. GRE tunnels can be used to form VPNs, connecting remote sites using private IP addresses via a public network. Typically, GRE tunnel is run between the customer edge routers and are transparent to the rest of the network. GRE tunnels are used to carry non-IP traffic (like IPX, Appletalk, DECnet from legacy networks) over an IP backbone.

Hosted SIP ALG

OmniAccess 5510 USG supports hosted SIP ALG with and without pin-holing. A mechanism where the gateway (OmniAccess 5510 USG) does IP layer natting and SBC does ALG is referred as Hosted SIP ALG (on the gateway side). The gateway must be able to open up pinholes for SIP session and RTP session.

Intrusion Detection

Alcatel IPS/IDS is a network security system designed to identify intrusive or malicious behavior via monitoring of network activity. The IDS identifies suspicious patterns that may indicate an attempt to attack, break in, or otherwise compromise a system. IDS can be network-based or host-based, passive or reactive, and can rely on either misuse detection or anomaly detection.

Detection Mode

In detection mode, IDS detects the attack and alarm is generated.

Prevention Mode

Packets are dropped. It sends resets depending on the configuration and group level and rule level prevention information is maintained in Snort.

Group-Level Detection

In group level, different actions can be taken for different group attack packets. One group can have detection as action while others can have prevention.

LAN Protocols

STP

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

Bridging

Bridging occurs at layer 2, the link layer, which controls data flow, handles transmission errors, provides physical addressing, and manages access to the physical medium.

Integrated Routing and Bridging

The L2 port on OmniAccess 5510 USG system is a VLAN-aware Ethernet switch. However, for routing across VLANs or between traffic on the L2 port and other ports, there has to be a mechanism to detect traffic that is to be routed, and subject it to normal IP packet processing activities such as filters, NAT, IPsec, FIB lookup, and so on. Hence a L2 port will then be capable of taking part in both bridging and routing at the same time. This technology is called IRB on OmniAccess 5510 USG.

Multicast Protocols

Multicast is an efficient way to deliver traffic from one sender to many potential receivers.

PIM-SM

Protocol Independent Multicast (PIM) protocols route multicast packets to multicast groups. PIM is protocol independent because it can leverage whichever unicast routing protocol is used to populate unicast routing table.

PIM-SM is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a RP per group, and optionally creates shortest-path trees per source. It defines a Rendezvous Point (RP) that is then used as a registration point to facilitate the proper routing of packets.

IGMP v1, v2

IGMP (Internet Group Management Protocol) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers. Multicast routers use IGMP to learn which groups have members on each of their attached physical networks.
The OmniAccess 5510 USG supports IGMPv2 as default IGMP version. As IGMPv2 is backward compatible, it works well with IGMPv1 host as well.

Network Services

DHCP Server

DHCP is a protocol used to configure an IP device connected in a network. The configuration parameters include - IP address, DNS information, default route and so on. With dynamic addressing, a device can have a different set of network parameter values every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic host configuration simplifies network administration because the software keeps track of host configuration rather than requiring an administrator to manage the task. This means that a new network device can be added to a network without the hassle of manually configuring it. Many ISPs (Internet Service Providers) use dynamic IP addressing for dial-up users. The DHCP server in OmniAccess 5510 USG provides DHCP clients with an IP address along with other network and boot information, based on the DHCP request received from the client.

DHCP Relay

Alcatel-Lucent DHCP relay feature eliminates the need for a DHCP server on every LAN, because DHCP requests can be relayed to a single remote DHCP server. DHCP Relay Agent acts as an intermediary between clients and servers by listening for client DHCP broadcast requests and forwarding them on to the server. In addition, the Relay Agent receives the server's response and passes the response back to the client. The relay agent allows the client and server to reside on different subnets. Enabling DHCP server on OmniAccess 5510 USG automatically disables DHCP relay.

TFTP Server/Client

TFTP (Trivial File Transfer Protocol) is a simplified version of FTP that allows for the transfer of files to and from a device. The TFTP client/server package on OmniAccess 5510 USG allows the system to act as either a TFTP client or server for downloading files. Currently, uploading of files to the TFTP server running on OmniAccess 5510 USG is not supported.

DNS Client

The DNS Client functionality on OmniAccess 5510 USG allows for resolution of host names to IP addresses, and vice-versa.

DHCP Client

DHCP is a protocol used to configure an IP device connected in a network. The configuration parameters include IP address, DNS information, default route, and so on. DHCP uses client-server architecture. DHCP client gets IP address for its broadcast interface and other essential network configuration information (like DNS server, TFTP server) from the DHCP server.

DDNS Client

DDNS is a service that provides the capability for a network device to perform DDNS updates to ensure that an IP host DNS name is correctly associated with its IP address. In general, WAN IP address is dynamic, and it becomes very difficult to access the network device with WAN IP whenever there is any change in the IP address. DDNS updates the WAN IP address in DNS server, so, it facilitates to access device from WAN side by using the unique domain name.

TR-069 Client

TR-069 (or Technical Report 069) from the Broadband forum provides a bi-directional configuration and provisioning mechanism between customer-premises equipment (CPE) and Auto Configuration Servers (ACS) using SOAP/ HTTP. The CPE WAN Management Protocol (CWMP) is an application-layer protocol that provides discovery, configuration, image management and diagnostics.

OmniAccess 5510 USG supports two modes of TR-069 configuration.
Manual mode - All the required parameters for ACS are to be configured manually using the respective CLI commands.

Automatic mode in zero-touch mode (Auto-configuration - ACS Auto-Discovery and dynamic service provisioning) - Auto-discovery feature enables TR-069 client to automatically discover URL of its assigned ACS, user name and the password.

Secure Shell (SSH)

The Secure Shell feature provides a secure mechanism that allows you to log in to a remote system, to execute commands on a remote device, and to move files from one device to another. Secure Shell provides secure, encrypted communications even when your transmission is between two untrusted hosts or over an unsecured network.

License Manager

Some of the features on the OmniAccess 5510 USG are license enabled. Hence they require a license to function. These licenses regulate the availability of a licensable feature at all times. These licenses are contained in a set of license files that will describe the features authorized to run on the OmniAccess 5510 USG. License Manager helps in managing these license files.

Quality of Service (QoS)

QoS generally involves prioritization, queuing, and shaping of network traffic. A network monitoring system must typically be deployed as part of QoS to insure that networks are performing at the desired level. QoS supports voice and data service simultaneously on OmniAccess 5510 USG. This includes controlled resource sharing by providing bandwidth guarantee for different classes. It also provides features that make QoS configuration simpler by means of Auto QoS commands.

OmniAccess 5510 USG supports both ingress and egress QoS processing. Ingress packets are classified using common classifiers, and exploit the one-pass classification feature on OmniAccess 5510 USG. QoS can be configured on Fast Ethernet, ATM, Tunnel and VLAN interfaces.

Supports L2 QoS. An interface can have both L2 and L3 policy map attached in the ingress direction, and only L2 or L3 policy map attached in the egress direction.

Egress Queues

Interface Egress Queues come into effect at the interface level and hold the packets that are in excess of the available bandwidth and are yet to be transmitted out in the network. The maximum length of queue is configurable within a specified range.

Traffic Policing

Dropping or marking packets in order to make traffic stay below a configured bandwidth. Thus defined, a traffic policing do not remove traffic burst, but controls the size of the peak.

Policing is done using Token Bucket Algorithm. A token bucket is a formal definition of a rate of transfer. It has two mandatory parameters like mean rate, burst size and can have optional parameter of peak rate and excess burst size. The traffic received on a flow that is to be policed is examined. The rate of the traffic is compared to a configured token bucket and action is taken based on the result. When sufficient number of tokens is available then the arriving traffic is said to confirm and then the corresponding number of tokens are removed from the bucket. If there are not enough tokens, then the traffic is said to exceed.

Weighted Fair Queuing

It is a packet scheduling technique allowing guaranteed bandwidth services.

WRED

WRED (Weighted Random Early Detection) is also a congestion avoidance technique. WRED combines the capabilities of the RED algorithm with the IP precedence/DSCP feature to provide preferential traffic handling of higher priority packets. It can selectively discard lower priority traffic when the interface begins to get congested and provide differentiated performance characteristics for different classes of service.

WRED can also be configured to ignore the IP precedence when making drop decisions so that non weighted RED behavior is achieved. WRED can provide separate thresholds and weights for different IP precedences, which can provide different quality of service with regard to packet dropping for different packet types.

Priority Egress Scheduling

The process of identifying which packet is to be selected for further action.

Egress Shaping

Egress Shaping is the process of delaying packets before they go out to make the traffic confirm to a configured maximum rate. The main intention of shaping the traffic is to define the traffic to flow with in an envelop.

The main objective of the traffic shaper is to allow the traffic in to the network at a controlled rate from different sources so that the network resources are optimally utilized for better performance. Typically, this is achieved by applying a Token Bucket Filter at the egress of an interface. Tokens will be generated per each flow at a sustained rate (configured as CIR) and are emptied as and when the packets are transmitted.

DSCP/TOS Marking

DSCP refers to the 6 bits in the ToS byte in the IP header. Marking refers to setting the IP DSCP/IP Precedence or ToS flags on the matched packet. This is used to select the Per Hop Behavior that a packet experiences through the network.

Auto QoS (diffserv, voice)

Auto QoS is a feature that enables user to configure QoS on OmniAccess 5510 USG with minimal effort. Normally, QoS configuration involve definition of class, match list association with the class, definition of policy, class association with the policy and defining class traffic attributes like bandwidth, police, shape, etc. This entire configuration might be cumbersome for user to configure. Auto QoS commands creates QoS configuration - automatically classifies traffic, applies the required traffic attributes for each of the classes based on the class needs. Auto QoS configuration also automatically applies the policy on to the interface. These configurations are not editable.

Hierarchical Queuing

Hierarchical Queuing provides a mechanism of controlled sharing of excess bandwidth in a hierarchical fashion. One can configure the hierarchical policy, which supports currently three level of packet classification. QoS manager will check all the constraint of the HPC and will maintain the database. Hierarchical Queuing is not supported on ATM interface.

Qos Pre-classify (QoS policies on tunneled/encrypted packets)

It classifies the packet based on the pre_tunnel ip-header and stores the classification index. This index is later used by QoS to classify the packet based on the inner tunnel header.

QoS on FR

One of Frame Relay's main benefits is that it makes a pool of bandwidth available to many VCs. However, there is a danger that some applications consume all of the available bandwidth leaving nothing or only small amount of bandwidth to other applications. To prevent this, FR interface has to be configured with QoS. The purpose of QoS is to provide fair access to the network's bandwidth by all the user applications and ensure that the key applications are not starved of required bandwidth.

ATM QoS

ATM networks are thought to transmit data with varying characteristics. Different applications need various QoS. Some applications like telephony may be very sensitive to delay or rather insensitive to loss, whereas others like compressed video are quite sensitive to loss. In this situation, it becomes important to ensure that time-critical applications do not suffer. This can be achieved by configuring QoS.

Routing Protocols

RIPv1\RIPv2

RIP uses User Datagram Protocol (UDP) data packets to exchange routing information. The routing information updates are sent at regular time intervals (by default, 30 seconds in Alcatel-Lucent’s implementation). If the router does not receive any updates from a neighboring router for a time interval known as the valid timer, it marks all routes from the neighboring router as invalid. And if there is still no sign of life from the neighboring router after the router’s flush timer has expired, all the routes are removed.

RIP uses hop count as metric and the max metric is 15. A metric of 16 means the network is unreachable; a metric of 0 means the network is directly connected.

A default route can be received from another RIP router or it can source the default route itself. In both the cases, the default route is advertised to other RIP routers via RIP. A default route can be sourced either with the default-information originate command or from another routing protocol via redistribution.

OSPF

OSPF is an IGP (Interior Gateway Protocol) developed by the OSPF working group of the IETF (Internet Engineering Task Force). OSPF was designed expressly for the IP networks. OSPF supports IP subnetting and tagging of externally derived routing information. Packet authentication and sending and receiving packets using IP multicast are also supported in OSPF.

Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed. OSPF multicasts the updated information only when a change has taken place.

Instead of counting the number of hops, OSPF bases its path descriptions on "link states" that take into account additional network information. OSPF also lets the user assign cost metrics to a given host router so that some paths are given preference. OSPF supports a variable network subnet mask so that a network can be subdivided.

BGP

BGP is an inter-Autonomous System routing protocol. The primary function for a BGP speaking system is to exchange network reachability information (NLRI) with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASs). This is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and some policy decisions at the AS level may be enforced.

BGP neighbors form a TCP connection between one another. They exchange messages to open and confirm the connection parameters.

Policy Based Routing

Branch offices need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional forwarding and routing algorithms. PBR is useful in deployments, where administrative issues dictate that traffic be routed through specific paths. By using PBR, customers can implement policies that selectively cause packets to take different paths.

PBR provides the ability to route traffic based on attributes other than the destination IP address. Attributes like source IP address, protocol type can be used to define policies and apply them to an interface.

VRRP

VRRP allows routers on a LAN to back up a static default route with a virtual router. VRRP dynamically assigns responsibility for a virtual router to a physical router (VRRP router) on the LAN. The virtual router is associated with an IP address (or set of IP addresses) on the LAN. A virtual router master is elected to forward packets for the virtual router’s IP address. If the master router becomes unavailable, the highest priority backup router will transition to the master state.

VRF

VRF-CE (Virtual Routing and Forwarding Customer Edge) is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-CE uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. A Layer 3 interface can belong to only one VRF at any time. Interfaces in a VRF can be either physical or logical such as VLANs.

System Management and Logging

CLI (Console, Telnet, SSH)

Alcatel-Lucent's Command Line Interface (CLI) is a text-based configuration interface that allows users to configure applications and to view statistics. Each CLI command applicable to the OmniAccess 5510 USG is defined in the CLI Reference guide. All command descriptions listed in the Reference Guide include command syntax definitions, defaults, usage guidelines, example screen output. The CLI uses single-line text commands that are similar to other industry standard switch interfaces and can be accessed via the console, Telnet, or SSH.

USGM - Unified Services Gateway Configuration Manager (HTTP, HTTPS)

The OmniAccess 5510 USG can be monitored and configured using USGM, Alcatel-Lucent's web-based device management tool. The USGM application is embedded in the OmniAccess 5510 USG and is accessible via the supported web browsers. USGM contains modules for configuring all software features in OmniAccess 5510 USG as well as configuration wizards for Firewall, VPN, and QoS configuration.

SNMP (v1, v2, v3)

The Simple Network Management Protocol (SNMP) is an application-layer protocol that allows communication between SNMP managers and SNMP agents on an IP network. Network administrators use SNMP to monitor network performance and to solve network problems. SNMP provides an industry standard communications model used by network administrators to manage and monitor their network devices. OmniAccess 5510 USG supports SNMP v1, v2 and v3 versions.

Syslog Forwarding

Forwarding syslog protocol compliant log messages to multiple hosts is allowed. It is possible to specify up to a maximum of 16 servers.

Ping, Traceroute

Ping and traceroute are common IP tools for testing IP connectivity.

Hitless Component Upgrades

Hitless component upgrade feature involves upgrading of one or more services without disrupting other services. There is no noticeable downtime during this upgrade, and only the services involved are replaced and restarted.

Factory Default Configuration

OmniAccess 5510 USG supports factory default configuration. In scenarios where OmniAccess 5510 USG is managed in a centralized management system, it is desirable to have a zero touch deployment. OmniAccess 5510 USG may just be connected to network lines and powered on, and the rest of configuration should be managed by the centralized location. This requires OmniAccess 5510 USG to boot with predefined configuration from the factory. Such a configuration is stored in factory default configuration. Whenever OmniAccess 5510 USG boots up for the first time, it always loads with this factory default configuration.

VPN

VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

IPsec Tunnel Interface

The OmniAccess 5510 USG provides support for IPsec in a tunnel mode with encryption, intended for secure site-to-site communications over an untrusted network. IPsec as a tunnel interface is required so that pre/post encryption or decryption policies for QoS, Filters, and ACLs can be applied.

- Traffic classifier will be route based rather than policy based, which means that routing can control what traffic needs to be secure.
- Tunnel failover can be handled by having traffic routed through another tunnel interface.
- Allows for configuration of dynamic routing protocols over the tunnel.

IPsec VPN Server

IPsec VPN Server is key requirement for SMB deployment where gateway is supposed to act as VPN gateway also. OmniAccess 5510 USG supports Alcatel-Lucent IPsec Client version 10.0. Uses RADIUS to authenticate Alcatel-Lucent IPsec Client.

Dynamic Multipoint Virtual Private Network (DMVPN)

DMVPN forms site-to-site VPN in hub and spoke configuration. In typical deployments, branch offices are spokes and central office is a hub. Financial institutions, transport service providers and medical institutions are few of the common deployment sites where hub and spoke model is used. OmniAccess 5510 USG supports spoke functionality of Dynamic MultiPoint VPN technology. Uses NHRP client services and multi-Point GRE (Generic Routing Encapsulation) tunnel for DMVPN.

WAN Protocols

HDLC

Layer 2 of the OSI model is the data link layer. One of the most common layer 2 protocols is the High-level Data Link Control (HDLC) protocol. In fact, many other layer 2 protocols are based on HDLC, particularly its framing structure. OA5510-TE supports only Cisco HDLC

Frame Relay

FR is a WAN protocol that operates at the physical and data-link layers of the OSI reference model. This protocol was originally designed for use across ISDN interfaces but today it is used over a variety of other network interfaces as well.

PPP

The PPP protocol emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, network protocol multiplexing, link configuration, link quality testing, error detection and option negotiation for such capabilities as network layer address and data compression. PPP supports these functions by providing an extensible LCP and a family of NCPs to negotiate optional configuration parameters and facilities. PPP supports IP through IPCP.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet), is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. Ethernet networks are packet-based and have no concept of a connection or circuit and also lack basic security features to protect against IP and MAC conflicts and rogue DHCP servers. By using PPPoE, users can virtually "dial" from one machine to another over an Ethernet network, establish a point to point connection between them and then securely transport data packets over the connection. OmniAccess 5510 USG supports PPPoE client functionality on the Fast Ethernet and ADSL ports.

MLPPP

MLPPP is an extension to PPP.

- OmniAccess 5510 USG supports RFC 1990 (MLPPP Protocol) without necessarily conforming to all the optional items mentioned in the specification.
- Specifically, the system supports the logical aggregation, into a configured MLPPP bundle of Serial interfaces, etc. This bundle behaves like a virtual IP interface.
- Multiple MLPPP bundles may be statically configured on the system. MLPPP protocol negotiation or data reaching the system on an unconfigured interface are dropped. Bundles cannot be deleted, but can be shutdown and thereby made unusable.
- Without any QoS configuration applied on the MLPPP bundle, the packet distribution across the MLPPP member links within a bundle is handled in a weighted round robin fashion, the weight being the bandwidth of the links.
- Authentication optionally happens at each member link, and is supported through PAP, CHAP or EAP as configured.
- IP routing protocols as well as policies such as ACL, NAT, IDS, IPsec, QoS and so on may be applied on the bundle.
- The default MTU is 1500 on an MLPPP bundle interface. That makes the MRRU (Maximum Received Restructured Unit) value to 1506 that accounts for the six extra bytes of the MLPPP

header. If there are interoperability issues with the peer, the MRRU value of the peer MLPPP interface has to be adjusted accordingly.

LFI

Link Fragmentation and Interleaving (LFI) is a Layer 2 technique in which all the Layer 2 frames are broken into small, equal-size fragments, and transmitted over the link in an interleaved fashion.

Link Fragmentation and interleaving feature for MLPPP and FR supports the transport of real-time (voice) and other (data) traffic on lower-speed PPP and FR links without causing excessive delay to the real-time traffic. The feature enables delay-sensitive real-time packets and packets that are not real-time data, to share the same link by fragmenting the long data packets into a sequence of smaller data packets (fragments). The fragments are interleaved with the real-time packets. On the receiving side of the link, the fragments are reassembled and the packet reconstructed. This method of fragmenting and interleaving helps guarantee the appropriate Quality of Service (QoS) for the real-time traffic

OAM

OAM (Operations, Administration, and Maintenance) describes the monitoring of network operation by network operators. OAM is generally utilized for detecting and localizing network faults, examining and reporting network status, monitoring network performance, and provisioning and configuring user parameters. Supports Ethernet OAM functionality on Fast Ethernet interface and BCP enabled T1E1 serial interface on OmniAccess 5510 USG.

BCP

Bridging feature on OmniAccess 5510 USG helps in carrying same VLAN tag across the interfaces, carrying multiple network protocols data seamlessly and avoids complexity of a router configuration. MAC Address, VLAN ID and 802.1p information remain intact while forwarding through WAN interfaces. Supports PPP, MLPPP, WAN Ethernet, FR, HDLC interfaces. Supports MAC based classification, MAC filtering, and QoS for bridge traffic.

ADSL - Multiple PVC

OmniAccess 5510-AA/AB USG supports multiple PVCs per ATM port with choice of different encapsulations over each PVC. PVCs will be configurable via sub-interfaces. Each sub-interface on the main ATM interface can be associated with an ATM PVC. Each PVC is an independent logical interface having its own attributes like encapsulation, IP address, security policies and routing policies.

Multiple Encapsulation over ATM Adaptation Layer 5

Each sub-interface on the main ATM interface can have its own encapsulation. OmniAccess 5510-AA/AB USG supports LLC-SNAP and VC-MUX mechanisms to transport connectionless routed and bridged packets over ATM Virtual Circuits. PPPoE, MAC Encapsulated Routing (MER), 1483 Bridged mode, 1483 Routed mode and PPP over ATM (PPPoA) are the encapsulation types that are supported. The default encapsulation on ATM sub-interface is MER.

Supported Traps

The following traps are supported in 3.0:

Trap Name	Platforms	Description
aluEGChassisTempTooHigh	All	The aluEGChassisTempTooHigh is generated when the chassis temperature (displayed in the “show chassis”output) goes above the upper threshold limit of 45^0C.
aluEGMemoryUsageTooHigh	All	The aluEGMemoryUsageTooHigh is generated when the primary memory usage in the chassis goes above the threshold limit of 95%.
linkDown	All	The linkDown trap is generated when the system recognizes that one of the communication links represented in the agent's configuration has gone down.
linkUp	All	The linkUp trap is generated when the system recognizes that one of the communication links represented in the agent's configuration has come up.
coldStart	All	The coldStart trap is generated when the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.
warmStart	All	The warmStart trap is generated when the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.
authenticationFailure	All	An authenticationFailure trap is generated when the sending protocol entity is the addressee of a protocol message that is not properly authenticated.
dsx1LineStatusChange	OmniAccess 5510-TE USG	A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes.
frDLCIStatusChange	All	The frDLCIStatusChange trap is generated when the indicated virtual circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states. If, however, the reason for the state change is due to the DLCMI going down, per-DLCI traps are not be generated.
aluEGPPPLinkUp	All	The PPPlinkUp trap is generated when the system recognizes that one of the PPP communication links represented in the agent's configuration has come up.
aluEGPPPLinkDown	All	The PPPlinkDown trap is generated when the system recognizes that one of the PPP communication links represented in the agent's configuration has gone down.
aluEGPkgUpgradeStatusTrap	All	Trap aluEGPkgUpgradeStatusTrap informs about status of a software / firmware upgrade.
ieee8021SpanningTreeNewRoot	All	The ieee8021SpanningTreeNewRoot notification indicates that the sending agent has become the new root of the Spanning Tree; the notification is sent by a bridge soon after its election as the new root. For example, upon expiration of the topology change timer,

		immediately subsequent to its election.
ieee8021SpanningTreeTopologyChange	All	A ieee8021SpanningTreeTopologyChange is sent by a bridge when any of its configured ports transitions from the learning state to the forwarding state, or from the forwarding state to the blocking state. The notification is not sent if a ieee8021SpanningTreeNewRoot notification is sent for the same transition.
aluEGClockMgtTrapSynchroOperChange	All	Notify all changes in the state of the system clock synchronization. Notification is sent when: - Type of source, or destination or VRF changes - Synchronization mechanism is stopped by administrator. It is not sent when: - Poll interval is changed.
dot1agCfmMepHighestPrDefect	All	A MEP (Maintenance Association End Point) has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP has a persistent defect, it may or may not generate a fault alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. If a defect with a higher priority is raised after a fault alarm has been issued, another fault alarm is issued. The management entity receiving the notification can identify the system from the network source address of the notification, and can identify the MEP reporting the defect by the indices in the OID of the dot1agCfmMepHighestPrDefect variable in the notification: dot1agCfmMdIndex - Also the index of the MEP's Maintenance Domain table entry (dot1agCfmMdTable). dot1agCfmMaIndex - Also an index (with the MD table index) of the MEP's Maintenance Association network table entry (dot1agCfmMaNetTable), and (with the MD table index and component ID) of the MEP's MA component table entry (dot1agCfmMaCompTable). dot1agCfmMepIdentifier - MEP identifier and final index into the MEP table (dot1agCfmMepTable).
tmnxDot1agCfmMepLbmTestComplete	All	The tmnxDot1agCfmMepLbmTestComplete indicates that a loopback test has been issued and results are ready.
tmnxDot1agCfmMepLtmTestComplete	All	The tmnxDot1agCfmMepLtmTestComplete indicates that a linktrace test has been issued and results are ready. The dot1agCfmMepTransmitLtmSeqNumber indicates the transaction identifier to use to retrieve the linktrace results.
tmnxDot1agCfmMepEthTestComplete	All	The tmnxDot1agCfmMepEthTestComplete indicates that an Eth-test has been issued and results are ready. The tmnxDot1agCfmMepCurrByteCount indicates the number of bytes contained in the frame's Test TLV, and the tmnxDot1agCfmMepCurrFailedBits and tmnxDot1agCfmMepCurrCrcFailures indicate the

		failure state of the test. Zero (0) values for the latter two objects indicate a successful test.
tmnxDot1agCfmMepDMTestComplete	All	The tmnxDot1agCfmMepDMTestComplete indicates that a One-Way-Delay-Test (OWDT) frame, or a Two-Way-Delay-Test (TWDT) response was received. For an OWDT frame, traps are raised only when a delay threshold of three seconds is exceeded.
tmnxDot1agCfmMepAisStateChanged	All	The tmnxDot1agCfmMepAisStateChanged notification is generated when a MEP enters or exits an AIS state.

Restrictions

- **3G Wireless WAN Interface and Hardware Crypto Engine**
  3G Wireless WAN Interface and Hardware Crypto Engine features are not supported in the Release 3.0. Nevertheless, these features are described in the technical documentation. Also, sales and marketing documents may introduce these features as available in the product. These two features will be supported in the Release 3.x maintenance software version.

- **4135 IP conference set**
  4135 IP conference set is not supported on OmniAccess 5510 USG.

- **TR-069 Client**
  Tests are performed with “Motive 5580” server. Depending on the server in use, it may be necessary to analyse any TR-069 client compatibility issue.

- **Web GUI - USGM**
  Some features may not be fully configurable via the Web GUI tool - Unified Services Gateway Configuration Manager. Use the CLI wherever applicable.

- **Dynamic Multipoint Virtual Private Network (DMVPN)**
  Currently, OmniAccess 5510 USG supports DMVPN interoperability with Cisco IOS Version 12.4 (18b). We do not support interoperability with any CISCO IOS version that has NHRP phase 3 implementation (like Cisco IOS Version 12.4(24)T2, Version 15.0(1)M1).

- **Software and Upgrade Requirements on OmniAccess 5510-AA/AB USG**
  Release 3.0 contains significant additions to the ADSL feature set on OmniAccess 5510-AA/AB USG. The changes in the implementation may lead to migrational issues while upgrading the OmniAccess 5510-AA/AB USG from Release 2.3.2 to Release 3.0. For any migrational issues, see the appendix chapter “Software and Upgrade Requirements on OmniAccess 5510-AA/AB USG” in the CLI Configuration Guide.

Unsupported CLI Commands

The following CLI commands are not supported in this release of the software:

Software Feature	Unsupported CLI Commands
Fast Ehternet	**flowcontrol** {**receive**|**send**}
NOE	[*<1-65535>*] **match** [**any**|**all**] <*match-list name*>... **service alcatel-tftp** **udp any any type noe** **nat-ip** <*ip-address*> **reserve-port-range** <*2048-65536*> <*2048-65536*> **show firewall alg noe statistics** **show firewall alg noe subaddress-mapping** [<*phone-ip-address*> |<*phone-mac-address*>] **show firewall alg noe debug-counters** **clear firewall alg noe subaddress-mapping** [<*phone-ip-address*>| <*phone-mac-address*>] **clear firewall alg noe statistics**
MLFR	[**no**] **debug frame-relay mlfr**

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Alcatel-Lucent Technical Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

PR	Description	Workaround
crms00235810	Once the "list" is attached to a client object, any change in the list will not be reflected in the client.	Create a new client object with the new list. Detach the client profile from the interface, attach the new client object to the profile and attach the client profile again to the interface.
crms00244974	When multiple tunnels (five or more) are configured, tunnel interface does not come up on OmniAccess 5510 USG after the peer is reloaded.	Detach and attach the IPsec profile.
crms00251519	Dynamically changing the ACS URL on OmniAccess 5510 USG requires a reboot to take effect.	ACS URL can be changed only through ACS server and cannot be changed through DHCP options or CLI command.
crms00251632	Client VPN tunnel goes down within few hours (six hours or more) of traffic.	If the client VPN connection goes down, reconnect the client.
crms00233635	ATM main interface goes down and comes up when encapsulation is changed from from MER to IPOA during traffic flow.	There is no known workaround at this time. System should auto recover and work fine after the flap.
crms00225473	When configuring /31 IP address for a non point-to-point encapsulation type, following error message is seen "Error - Invalid address in setting IP Address"; which should be treated as "/31 IP address is not applicable for a non point-to-point encapsulation type".	None.
crms00202796	Sometimes, dynamically installing or uninstalling licenses does not automatically enable IPsec tunnels.	Detach and attach the crypto map and the IPsec profile when the license is installed or uninstalled.
crms00231717	'No' commands to delete IPsec client object and client profile not available.	There is no known workaround at this time.
crms00232870	There is no support for options like 60, 43 on DHCP server to support all the features of NOE-SIP phones.	There is no known workaround at this time.
crms00233641	RTP traffic not recognized and one way voice observed when filter applied with non 5060 port and type RTP match-list.	Use DSCP bits in the match-list rule to classify the RTP traffic.
crms00243002	ConnectionStatus field on ACS always in "Connected" state when FastEthernet link is "down".	There is no known workaround at this time.

crms00250414	Segmentation fault occurs if maximum characters are exceeded when entering value for “tftp server” in the DHCP pool.	The workaround is not to use the maximum characters when configuring this option.
crms00228113	On disabling the Fast Ethernet multicast interface, the PIM hello packet with zero holdtime is not generated.	There is no known workaround at this time.
crms00257130	DHCP relay does not work if the outbound interface is an unnumbered interface.	There is no known workaround at this time.
crms00254973	Multiple dynDnsfs core got dumped while testing DDNS with maximum URL length.	There is no known workaround at this time.
crms00253744	"clear ip filter statistics {<filter-name> |<interface-name>} {in|out|both}" is not working.	There is no known workaround at this time.
crms00250687	"show ip nhrp" on the receiving spoke does not display information about its peer spoke.	There is no known workaround at this time.
crms00250040	“show interfaces brief” still shows the line protocol status for ATM main interface.	There is no known workaround at this time.
crms00249069	Links continue to show up in 'show spanning-tree' output even after removal of VLAN configurations from the interface.	There is no known workaround at this time.
crms00248418	L2 QoS is reflected as IP QoS in 'show internal interface' output.	There is no known workaround at this time.
crms00242216	“show running-config” does not show the configured IP address when the encapsulation is changed from PPPOE to PPPOA.	Issue “show” command for the specific interface.
crms00235523	"Policy detach unsuccessfull" message is generated while detaching SNAT from the ATM sub-interface though policy has been detached.	There is no known workaround at this time.

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
Europe	+33-388-55-69-29
Asia Pacific	+65 6240 8484
Other International	818-878-4507

Email: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.esd.alcatel-lucent.com.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each chassis.

Severity 1 Production network is down resulting in critical impact on business - no workaround available.

Severity 2 Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 Information or assistance on product feature, functionality, configuration, or installation.