Alcatel-Lucent
Femto Security Gateway (Brick)

Product Description

Document Number: BCR/ALFM/INF/025110
Document Issue: V01-02/ EN
Document Status: Standard
Date of Issue: 15/JUNE/2009

About Alcatel-Lucent

Alcatel-Lucent (Euronext Paris and NYSE: ALU) provides solutions that enable service providers, enterprises and governments worldwide, to deliver voice, data and video communication services to end-users. As a leader in fixed, mobile and converged broadband networking, IP technologies, applications, and services, Alcatel-Lucent offers the end-to-end solutions that enable compelling communications services for people at home, at work and on the move. For more information, visit Alcatel-Lucent on the Internet: **Error! Hyperlink reference not valid.**

Notice

The information contained in this document is subject to change without notice. At the time of publication, it reflects the latest information on Alcatel-Lucent's offer, however, our policy of continuing development may result in improvement or change to the specifications described.

Trademarks

Alcatel, Lucent Technologies, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Contents

LIST OF FIGURES

LIST OF TABLES

PUBLICATION HISTORY

Release	Date	Contact	Comments
BCR2.1		Isabel Pampliega	New document
BCR2.2	V01 September 2008	Kevin Pendleton	New sections: 2.2 Operation and Maintenance 2.3 Installation Update for release BCR 2.2
BCR2.2	V01-02 June 2009	Susana Gonzalez	Updated Section 2.2.7 Alcatel-Lucent Security Management Server

1 INTRODUCTION

1.1 Overview

This document provides a high level description of Alcatel-Lucent VPN Firewall Brick 1200 HS or Security Gateway, used in the BSR Femto Solution Architecture.

For further information about any Alcatel-Lucent products please refer to your local representative.

The Product Description provides information on the Security Gateway (Brick) including:

- General information about the Brick device hardware and functions
- Illustrations of the Brick device hardware components
- Operations and Maintenance
- Technical Specifications

1.2 Scope of this Document

Although this document provides information on Alcatel-Lucent VPN Firewall Brick 1200 HS or Security Gateway functions, it cannot be considered as a detailed feature list or a Plan of Record (PoR). This information is provided in dedicated documents on a per software release basis (e.g. BCR 2.2 Feature Planning Guide).

This document is focused in the BCR 2.2 BSR Femto Reference Architecture.

2 ALCATEL-LUCENT SECURITY GATEWAY (BRICK)

2.1 Functions

The Security Gateway or Alcatel-Lucent Brick implements the logical functionality of the firewall(s), IPSec router(s), Base Station Router Voice Gateway (BVG) and Base Station Router Packet Gateway (BPG) in the BSR Femto Solution.

Figure 1 - Alcatel-Lucent VPN Firewall Brick 1200 HS (Femto Security Gateway

The Brick device is a high-speed packet-processing appliance, primarily oriented towards providing security functions. The Brick is offered supporting different physical interface combinations. The Brick device product line provides LAN-level Ethernet interfaces, in both 10/100 copper as well as Gigabit fiber and/or copper ports via Small Form-factor Pluggable (SFP) ports.

Internally, the device has only a solid-state NVRAM disk to store local policy and configuration. The cooling fan is the only continuously moving part. This allows the Brick device to have an extremely long hardware mean time between failures (MTBF). The Brick device does not run as an application on top of a commercial operating system ; rather, it runs as the kernel of a small, highly application-specific operating system developed by Bell Labs. The Brick device operating system is an evolution of Lucent's Inferno operating system , designed for small embedded security applications.

The Brick OS has no user logins or file system permissions to be overridden, as well as no insecure communication processes (such as Telnet or HTTP) to be broken via a stack smash or buffer overflow.

Brick devices are available in a variety of hardware models; the models differ solely in throughput, capacity, and physical interface types. Currently, 10/100 copper Ethernet and Gigabit fiber-optic (multimode) and Gigabit copper interfaces are available.

The Brick supported functions are described in more detail in the paragraphs below.

2.1.1 IPSec Gateway

The purpose of the IPSec Gateway is to provide IPSec tunnel endpoints to all BSR Femtos of the cluster. IPSec tunnels are setup in coordination with the AAA server based on shared secret mechanism or USIM authentication.

The mapping is one IPSec tunnel for each BSR Femto by default. Optionally, two tunnels are made available, one for high priority traffic, the other for low priority traffic.

Having this centralized IPSec router avoids the need to implement IPSec on all the network elements.

The following traffic passes through the tunnel between the BSR Femto and the Brick:

- All signaling traffic to/from the operator's network elements.
- IuCS' user plane packets
- IuPS' user plane packets and
- Control signaling for the BVG and BPG functions

2.1.2 Firewall

The Brick acts as a firewall between the BSR Femtos and the operator's network. As a firewall its purpose is to isolate the operator's network from potential harmful traffic. All signaling traffic between the operator's network and the managed IP network is carried in IPSec tunnels and will pass through this firewall.

2.1.3 BSR Voice Gateway (BVG)

The BSR Voice Gateway (BVG) is a functional element in the BSR network for support of Circuit Switched voice and data.

The BVG acts as a concentrator for IuCS user plane traffic providing a single IP address towards the MSC

Only Iu-CS user plane traffic passes through the BVG; Iu-CS signaling traffic passes through the BSR Signaling Gateway (BSG) The BSG and BVG present a single logical RNC interface to the MSC representing the entire BSR Femto cluster.

Both the BSR Femto and BVG support the proprietary Dynamic Port Address Translation (DPAT) protocol to allow multiple BSRs to share an "RNC address". The RNC Address provided to the MSC by the BSR Femto is referred to as the Virtual RNC Address (VRA) of the BVG and a UDP port number. In turn the BVG provides the BSR Femto a single Virtual MSC Address (VMA) and a UDP port number. The VRA and VMA could be the same or they can be different.

2.1.4 BSR Packet Gateway (BPG)

The BPG acts as a concentrator for the Internet interface for a BSR Femto cluster, presenting a single IP address towards the SGSN from a "virtual RNC" represented by the BPG. It performs address translation to enable routing to/from the many BSR Femtos.

Traffic passes to the SGSN directly from the BPG, while signalling is handled by the BSG. Together the BSG and BVG present a single "virtual" RNC interface to the SGSN representing the entire femto-cell cluster.

The BPG shall support a Network Address Translation scheme to allow multiple BSR Femtos to share a "Virtual RNC Address" (VRA) towards the SGSN and to allow multiple "Virtual SGSN Addresses" (VSA) to represent a virtual SGSN towards the femtos.

The BPG will support a minimum of 20 VSA and one VRA. The number of supported VSAs being provisionable.

2.2 Operation and Maintenance

2.2.1 Introduction

The Bricks can be managed remotely from the Alcatel-Lucent Security Management Server (ALSMS). One ALSMS can manage up to 20,000 Bricks. ALSMS connects to the Bricks via Ethernet.

2.2.2 Configuration Management

The configuration process consists of the following activities:

- Using the ALSMS, create an instance of the Brick device and enter the required configuration parameters, such as Brick name and IP address
- Create a floppy disk or USB drive containing the configuration information and use the disk to activate the Brick device

As part of the BSR voice and packet gateway features, an administrator can specify the DPAT port number for collection of UDP packets from multiple BSRs, enable/disable a clean-up process for hung-up or failed BSR/BVG port table mappings, and configure a BPG inactivity timer to terminate the binding session between the BSR and Brick device if there has been no user traffic activity for a set amount of time. Additionally, the user may set QoS management settings.

Although not in the reference architecture, the IPSec function can be enabled or disabled for a Brick device via the ALSMS. If it is required to disable the IPSec function, it is recommended that prior commitment by Alcatel-Lucent to validate this architecture is requested.

2.2.3 Performance Management

Traffic statistics of the brick may be monitored at the ALSMS by use of either a tabular or graphical display. The following statistics are shown;

- Data packet throughput into the Brick (Mbits/sec)
- Data packet throughput out of the Brick (Mbits/sec)
- Packets per second into the Brick Packets per second out of the Brick
- New sessions per second into the Brick
- New sessions per second out of the Brick
- Megabit guarantee into the Brick
- Megabit limit into the Brick
- Session limit into the Brick
- Megabit guarantee out of the Brick
- Megabit limit out of the Brick
- Session limit out of the Brick

2.2.4 Fault Management

The ALSMS allows alarm configuration of SMTP and Syslog servers that will be used when an alarm triggers an e-mail or Syslog, admin console, SNMP Manager or to a pager message.

A Trigger scans the ALSMS logs for a set of conditions, when the conditions are matched the action associated with the trigger is taken.

When a trigger detects a set of conditions that are user defined, the action that is associated with this trigger is taken.

Triggers can be set for any of the following conditions.

- Alarm code
- Brick Error
- Brick Failover event
- Brick ICM Alarm
- Brick interface lost
- Brick lost
- Brick Proactive monitoring
- Brick SLA round trip delay alarm
- ALSMS error
- ALSMS proactive monitoring
- LAN to LAN tunnel lost
- LAN to LAN tunnel up
- Local Presence map pool
- QOS Rule Bandwidth exceeded alarm
- QOS Rule Bandwidth guarantees alarm
- QOS Rule Bandwidth Throttling alarm
- QOS Zone Bandwidth Guarantees alarm
- QOS Zone Bandwidth throttling alarm
- Real Secure
- Unauthorized ALSMS login attempt
- User authentication

Any of the following actions can be set based on these triggers

- Direct Page – Page the administrator
- Email – Send email to responsible party
- SNMP Trap – to any SNMP Manager
- Syslog – Sends UDP packet to Syslog server

2.2.5 System Administration

By default, all standalone and primary ALSMS automatically back up their databases and configuration files each night or may be scheduled to any set time as required. Backups for the last seven days are stored on the ALSMS server. There are also options for sending backups to a RAID server or server farm.

After the nightly backup, a copy of the backup is written to the secondary ALSMS. It is to be used in the event that there is a failure on the primary ALSMS.

2.2.6 Remote Access

The ALSMS Remote Navigator application allows you to run the ALSMS application from a remote host instead of the ALSMS console. It is provided on the ALSMS CD-ROM, and may also be retrieved remotely from the ALSMS via a browser.

An Administrator can log into the ALSMS remotely using a host running:

Microsoft®Windows®, Vista™, or Sun®Solaris® operating systems. Interoperability across platforms is supported, so Windows remote clients can access a Solaris® ALSMS, and Solaris® remote clients can connect to a Windows® or Vista™ ALSMS. The following gives the software requirements for both platforms.

2.2.6.1 Microsoft®Windows® or Vista™

The remote host must be running the following software:

- Windows® 2000 Professional, Windows® 2000 Server, Windows® XP Professional, Windows® Server 2003, or Vista™
- Microsoft® Internet Explorer 5.0 or greater
- Adobe Acrobat Reader 4.0 or above, to read the on-line documentation.

2.2.6.2 Solaris® 8, 9, 10

The remote host must be running the following software:

- Solaris® 8, 9, or 10
- Netscape Communicator 4.7 or greater
- Adobe Acrobat Reader 4.0 or above, to read the on-line documentation.

2.2.7 Alcatel-Lucent Security Management Server

Alcatel-Lucent Security Management Server (ALSMS) software provides integrated control over thousands of Brick appliances and IPSec client users from one console.

The window that appears immediately after login is called the Navigator window. This window is your doorway to the SMS. Starting from this window, the user is able to centrally manage the Bricks in the network.

Figure 2 below shows the Navigator window. The window work area is divided into two panels, a Folders panel on the left and a Contents panel on the right.

The Folders panel consists of a set of folders and subfolders organized into a hierarchical tree structure. Inside these folders are listed the devices being managed, the security policies and tunnel endpoints set up and a variety of other system features and components.

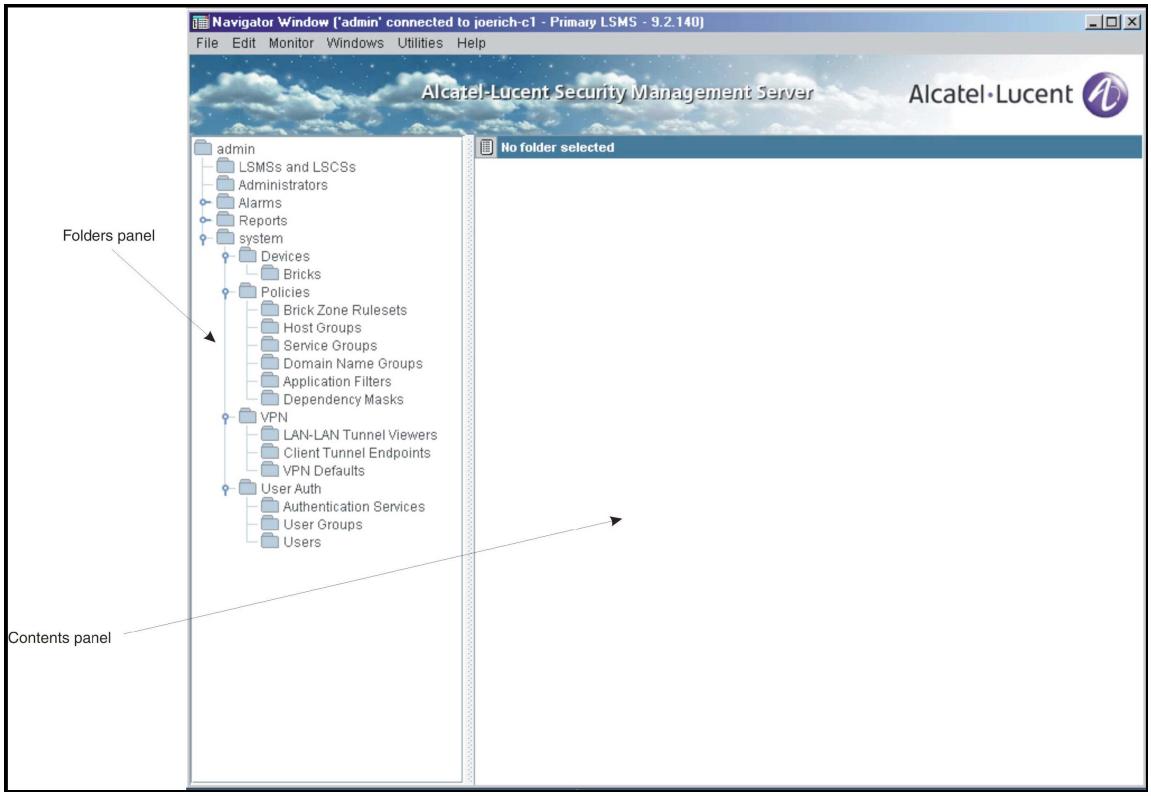

Figure 2 - 2.2.7 Alcatel-Lucent Security Management Server Navigator Window

2.2.7.1 Hardware Requirements

- The Alcatel-Lucent recommended Hardware Platform for the ALSMS Server is the Sun Netra X4250[1], which is NEBS compliant and is available in both AC & DC versions.
- From BCR2.2 it is possible to run the ALSMS on the same hardware platform as the AAA.
- The ALSMS can be deployed either in standalone mode or collocated with the AAA and both modes are are supported for Trial and Commercial deployments.
- The Alcatel-Lucent recommendation is to deploy the ALSMS on the same SUN Netra X4250 Server as the AAA as shown in Figure 3, below.

[1] Existing ALSMS Servers deployed in BCR2.1 on the Sun Netra T2000 will continue to be supported. However all new deployed ALSMS Servers from BCR2.2 should be based on the SUN Netra X4250.

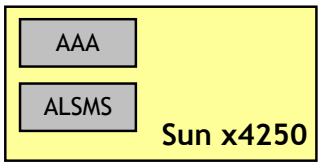

Figure 3: ALSMS collocated on same HW platform as AAA

2.2.7.2 Software Requirements

- Required OS needed for the ALSMS in standalone mode is RHEL5.1
- Required OS needed for the ALSMS collocated with AAA, is RHEL5.1 + Java1.6

2.3 Installation

Installation of the Brick requires no special tools. Physical Installation in the rack is by means of securing front and rear mounting brackets. Optional side mounting brackets may be used depending on the rack mounting requirements. Electrical connection is made via standard connectors.

2.4 Technical Specifications

2.4.1 Hardware

The Security Gateway functions are performed in the Brick 1200 HS platform. The main characteristics of the Brick Model 1200 HS are listed below:

Specification	Detail
Brick Model 1200 HS	Simplex = 1; Duplex = minimum 2 (1 Brick pair in active/standby) This is a carrier grade platform which consists of: 3.6 GHz Processor 2 GB RAM 1 x VPN encryption accelerator It is recommended that the Bricks are deployed in pairs. The number of Brick Pairs deployed per cluster for commercial deployments will vary depending on customer Traffic profile and the number of Femtos deployed.
Ethernet Ports	14 x 10/100/1000 Mbps BaseT Ethernet Ports 6 x GigE optical Ethernet Ports The GigE optical ports are optional. Additional hardware required including SFPs to support. Recommendation is to go with 1000BaseT
Dimensions (Height x Width x Depth)	48.3 cm x 48.3 cm x 8.9 cm / 19" x 19" x 3.5" (2U) Rack Mountable per EIA-310 specification
Weight	Weight: 20 Kg (44 lbs) Shipping Weight: 22 Kg (50 lbs)
Temperature	Operating 0 to 40° C Non Operating -40 to 70° C
Shock	Operating 2.5g at 15 – 20 ms on any axis Non Operating 35g at 15 – 20 ms on any axis
Relative humidity	Operating 5-85% at 40 C (non-condensing) Non Operating 5-90% at 40 C (non-condensing)
Vibration	Operating 5g at 2 – 200Hz on any axis Non Operating 5g at 2 – 200Hz on any axis

Power Supply AC Models	Hot Swappable, Internal Dual AC to DC Power Supply: 500W max Auto-ranging: 100 to 240 VAC, 47 to 63 Hz Consumption: 8A @ 120 VAC; 5A @ 240 VAC
Power Supply DC Models	Hot Swappable, Internal Dual DC to DC Power Supply: 500W max Input Range: -36 to -72 VDC Consumption: 10A @ -48 VDC, 8A@ -60VDC
Cooling	Chassis fan (intake and exhaust), power supply fans
Operating Altitude	Up to 4 000m (13 123 ft)
Mean Time Between Failure	Brick 1200HS AC: 128,820 hours Brick 1200HS DC: 128,833 hours
Certifications	ICSA V4.1 Firewall Certification in process, ICSA V1.2 IPSec Certification in process, FIPS 140-2 Certification in process EAL-4 Certification in process NEBS™ Level 3 (compliant to Telecordia GR1089-CORE and GR-63-CORE) in process for Brick 1200 HS DC version.

Table 1 — Hardware Specification

2.4.2 Regulatory Requirements

Environmental Condition Domain	Reports	Environmental Requirement
Product Safety Approvals		CE
		CB Scheme to EN/IEC 60950-1
		CSA Certified to UL ® 60950-1, 1st Edition (Americas)
		CAN/CSA 22.2 No. 60950-1-03 (Americas)
		CB Scheme to EN/IEC 60950-1 (APAC)
		ACA TS 001 1997 (APAC)
		AS/NZS 3260 1993 with amendments 1, 2, 3 and 4 (APAC)
EMC Approval	Report # TR2006-044-EU	CE
		Directive 2004/108/EC December, 15th 2004
		EN55022/CISPR 22 (Telecommunications ports, conducted emission DC and AC)
		EN55024 / CISPR 24 (Limits & test method and classification)
		EN55024/VCC
		EN300-386, Class B (emission and immunity)
		IEC 61000-3-2 (harmonic current emissions AC mains input port)
		IEC 61000-3-3 (voltage fluctuations and flicker, AC mains input port)
		IEC 61000-4-2 (Electrostatic discharge)
		IEC 61000-4-3 (RF electromagnetic field)
		IEC 61000-4-4 (Fast transient common mode)
		IEC 61000-4-5 (Surges, common and differential mode)
		IEC 61000-4-6 (RF common mode 0,15 – 80 MHz)
		IEC 61000-4-11 (Voltage dips, short interruptions and voltage variations)
		IEC 61000-6-1 (Immunity for residential, commercial and light-

		industrial environments)
		FCC Part 15, Class A (USA)
		ICES-003, Class A (Canada)
		VCCI Class A (Japan)
		AS/NZS – CISPR Pub 22, Class A (APAC)
Power Supply	Report # CB-161547-1851482 as per IEC 60950	ETS 300 132-1
		ETS 300 132-2
Human safety rules	Report # CB-161547-1851482	IEC 60950-1
	Report # CB-161547-1851483	Directive 1973/23/EEC (A1)
	Report # CB-161547-1851484	Directive 1993/68/EEC

Table 2 — Regulatory Compliance

2.4.3 Interfaces

Supported Interfaces	Interface Description	Comments
IuCS' + IuPS' (BSR Femto – Brick)	IuCS' & IuPS' proprietary interfaces from the BSR Femto	IPSec router function on the Brick terminates a secure tunnel from each BSR Femto. All user, signaling and OAM traffic passes through this tunnel.
IuCS'-CP + IuPS'-CP	IuPS'-CP & IuCS'-CP interfaces from the Brick to the BSG	
IuCS-UP (BVG – 3GMSC)	Interface from the BVG to the 3G-MSC	
IuPS-UP (BPG – SGSN)	Interface from the BPG to the SGSN,	Only IuPS o/ATM supported. IuPS-CP will be o/ATM IuPS-UP to be switched via the 77xx to perform the IP over ATM encapsulation.
Itf-Brick	Interface towards the ALSMS	

Table 3 — Interfaces

2.4.4 Redundancy

The Security Gateway (Brick) redundancy shall be supported on a pair of platforms (1200 HS Bricks).

The Brick can operate in one of two modes:

- Simplex Operation – One Brick

- Redundant Operation: A Brick Pair (2 Bricks)[2]

When operating in redundant operation, the two Bricks are connected to the same set of LANs and they share the same identity, including IP address.

From an OAM point of view the two Bricks are treated as a single Brick, the first of the two to boot up becomes the active Brick and the other remains the standby until the active Brick fail.

Fail over from the active to the standby Brick will occur:

- Upon failure of the active Brick
- If the active detects that the standby has better LAN connectivity. The active hears "standby" heartbeats with a greater health and status indicator from the standby Brick (if the yield parameter is set to greater than zero).
- Based on administrator command

2.4.5 Availability

Alcatel-Lucent supports the following features to ensure high availability, eliminating any single point of failure:

- VPN Firewall Brick security appliance to VPN Firewall Brick security appliance active/passive failover with full synchronization
- 400 millisecond device failure detection and activation
- Session protection for firewall
- Link failure detection
- Alarm notification on failover
- Encryption and authentication of session synchronization traffic
- Self-healing synchronization links
- Pre-emption and IP tracking for improved health state checking
- Seamless system upgrade with no downtime for redundant deployments

2.4.6 Diagnostic Tools

- Out of band debugging and analysis via serial port/modem/terminal server
- Centralized, secure remote console to any VPN Firewall Brick
- VPN Firewall Brick security appliance supports Ping, Traceroute, and Packet Trace with filters
- Remote Brick security appliance bootstrapping
- Real-time log viewer analysis tool
- Java-based Navigator for remote access to management system

[2] This is the minimum number of Bricks (Brick pair) required within a cluster to operate in redundant mode. Additional Brick pairs will be added based on the size of the cluster required to support. For bigger size networks additional clusters will need to be setup.

3 REFERENCES & ACRONYMS

3.1 References

For further information on the BSR Femto Solution and the Security Gateway (Brick), please refer to:

[1] UMT/SYS/INF/023452: BCR 2.2 Feature Planning Guide

[2] UMT/OAM/INF/022831: Femto Management Solution high level product overview

[3] BCR/SYS/DD/025509: BCR2.1 Alcatel-Lucent 9365 Base Station Router Femto Reference Architecture

[4] 260-100-022R9.2 Alcatel-Lucent Security Management Server (SMS) Release 9.2 Technical Overview

[5] 260-100-039R9.1 Lucent VPN Firewall Model 1200 Brick User's Guide

3.2 Acronyms

1 - 10

3G	3rd Generation

A - L

ALSMS	Alcatel-Lucent Security Management Server
BPG	BSR Packet Gateway
BSG	BSR Signalling Gateway
BVG	BSR Voice Gateway
CS	Circuit Switched
FMS	Femto Management Solution
GGSN	Gateway GPRS Support Node
HLR	Home Location Register
HNM	Home Network Management
IP	Internet Protocol
IPC	IP Protocol Converter

M - Z

MSC	Mobile Switching Centre
OAM	Operations, Administration and Maintenance
PS	Packet Switched
QoS	Quality of Service
RF	Radio Frequency
SGSN	Serving GPRS Support Node
SFP	Small Form-factor Pluggable
UE	User Equipment
VSA	
VoIP	Voice over IP
W-CDMA	Wideband-Code Division Multiple Access
WMS	Wireless Management System