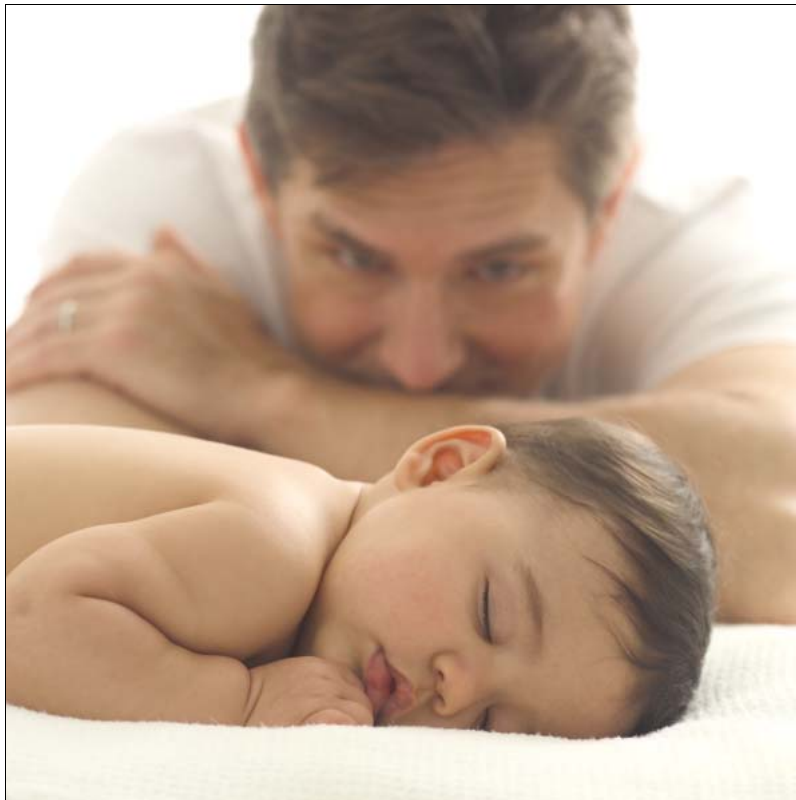


ESA Glossary of Terms and Acronyms

Ericsson SNMP Agent 16.0

GLOSSARY



Copyright

© Ericsson AB 2004-2016. All Rights Reserved.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing.

Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

Ericsson is the trademark or registered trademark of Ericsson AB. All other products or service names mentioned in this document are trademarks of their respective companies.



Contents

1	About This Document	1
1.1	Purpose	1
1.2	Target Group	1
1.3	Prerequisites	1
2	Glossary	3





1 About This Document

1.1 Purpose

The purpose of this document is to present and describe the abbreviations, concepts and terminology used in and that are related to the Ericsson SNMP Agent (ESA).

1.2 Target Group

This document is intended for all users using the ESA documentation library.

1.3 Prerequisites

-





2 Glossary

3GPP

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that brings together a number of telecommunications standards bodies. The establishment of 3GPP was formalized in December 1998. For more information see <http://www.3gpp.org>.

AAL

See *Active Alarm List*.

Abstract Syntax Notation One

The *Abstract Syntax Notation One (ASN.1)* is a formal language for abstractly describing messages to be exchanged among an extensive range of applications involving the Internet, intelligent network, cellular phones, ground-to-air communications, electronic commerce, secure electronic services, interactive television, intelligent transportation systems, Voice Over IP, and others. Due to its streamlined encoding rules, ASN.1 is also reliable and ideal for wireless broadband and other resource-constrained environments. Its extensibility facilitates communications between newer and older versions of applications.

ACC

See *Alarm Clear Control*.

Active Alarm List

The *Active Alarm List (AAL)* is a list presenting the currently active alarms, that is, alarms that have been raised, but not cleared.

Advanced Encryption Standard

The *Advanced Encryption Standard (AES)* is a block cipher of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.

AES

See *Advanced Encryption Standard*.

AFC

See *Alarm Flooding Control*.

Agent Extensibility Protocol

The *Agent Extensibility Protocol* (or AgentX) is a computer networking protocol that allows to manage Simple Network Management Protocol objects defined by different processes via a single master agent. Agents that export objects via AgentX to a master agent are called subagents. The AgentX standard does not only define the AgentX protocol, but also the procedure by which those subagents process SNMP protocol messages.

For more information, see RFC 2741.

AgentX

See *Agent Extensibility Protocol*.

Akka Technology

The Akka Technology is used for clustered ESA. ESA is using Akka's cluster functionality, actor handling, scalability and fault detection.

Alarm Clear Control

The *Alarm Clear Control (ACC)* option in the ESA suppresses all the "alarm clear" traps that are sent without a corresponding "alarm raise" being sent before.

Alarm Flooding Control

The *Alarm Flooding Control (AFC)* option in the ESA makes it possible to avoid raising an identical, already active and not yet cleared alarm, being repeated over and over again. This option spares the NMS from being flooded with identical alarms.

Alarm Persistency

The *Alarm Persistency* capability makes the ESA holding the alarms persistent (active) after an ESA or node restart when operating in Cluster Mode. Also see *Cluster Mode*.

Alarm Redundancy

The *Alarm Redundancy* capability makes the ESA holding the alarm data redundant by replicating the data over several nodes when operating in Cluster Mode. Also see *Cluster Mode*.

API

See *Application Programming Interface*.

Application Programming Interface

An *Application Programming Interface (API)* is the specific method prescribed by a computer operating system, or by an application program, by which a programmer writing an application program can make requests of the operating system or another application.



ASN.1

See *Abstract Syntax Notation One*.

Basic Encoding Rules

Basic Encoding Rules (BER) are ASN.1 encoding rules for producing self-identifying and self-delimiting transfer syntax for data structures described in ASN.1 notations. BER is a self-identifying and self-delimiting encoding scheme, which means that each data value can be identified, extracted and decoded individually. You view it as a kind of "binary" XML. Currently effort is being made to join these two technologies, such as the XML Encoding Rules (an alternative to BER), ASN.1 Schema (an alternative to XML Schema), ASN.1 SOAP (to exchange XML with PER on web services). BER is defined in ITU-T X.690 and ISO 8825-1.

BER

See *Basic Encoding Rules*.

Cluster Mode

The *Cluster Mode* capability provides multiple ESAs on multiple nodes to work as one single unit. From an external view the ESAs in Cluster Mode represents the multiple nodes as a single node. Also, see *Alarm Persistency*, *Alarm Redundancy* and *High Availability*.

Comma Separated Values

In computers, a *Comma Separated Values (CSV)* file contains the values in a table as a series of ASCII text lines, organized so that each column value is separated from the value of the next column by a comma, and each row starts a new line.

An example:

```
Smith,Will,1972,123-4567
Robert,Julia,1962,232-3232
Ford,Harrison,1956,987-6543
```

A CSV file is a way to collect the data from any table, so that it can be conveyed as input to another table oriented application. A CSV file is sometimes referred to as a "flat file".

Community String

The SNMP *Community string* is like a user identification or password that allows access to the information of a device published on the SNMP interface. An NMS sends the community string along with all its SNMP requests. If the community strings match, the device responds with the requested information. If the community strings do not match, the device simply discards the request and does not respond.

SNMP Community strings are used only by devices which support the SNMPv1 or SNMPv2c protocols. SNMPv3 uses security name and password authentication, along with an encryption key.

CSV

See *Comma Separated Values*.

Data Encryption Standard

The *Data Encryption Standard (DES)* is a cipher (a method for encrypting information).

DES

See *Data Encryption Standard*.

Document Type Definition

A *Document Type Definition (DTD)* is a specific definition that follows the rules of the Standard Generalized Markup Language (SGML). A DTD is a specification that accompanies a document and identifies what the funny little codes (or markup) are that separate paragraphs, identify topic headings, and so forth, and how each is to be processed. By mailing a DTD with a document, any location that has a DTD “reader” (or “SGML compiler”) is able to process the document and display or print it, as intended. This means that a single standard SGML compiler can serve many different kinds of documents that use a range of different markup codes and related meanings. The compiler looks at the DTD and then prints or displays the document accordingly.

DTD

See *Document Type Definition*.

Ericsson SNMP Agent

The *Ericsson SNMP Agent (ESA)* is a SNMP agent, sending SNMP alarms and receiving SNMP requests for reading/writing data in published MIBs on the system where it is installed. ESA is a full featured SNMP agent with a SNMP architecture, handling a master agent and several sub agents. It allows flexible cooperation with potential already existing SNMP agents. Also, the ESA provides many features for the system designer for integration of SNMP functionality in completely new systems, without existing SNMP agents, as well as in mature systems, with SNMP agents already installed.

The ESA provides the user with functionalities for both Fault Management and Performance Management.

ESA

See *Ericsson SNMP Agent*.



ETSI

See *European Telecommunications Standards Institute*.

European Telecommunications Standards Institute

The *European Telecommunications Standards Institute (ETSI)* is a non-profit organization that establishes telecommunications standards for Europe. ETSI guidelines are voluntary and almost always comply with standards produced by international bodies.

ETSI initiatives touch on the following areas: aeronautical radio, API, ATM, electromagnetic compatibility, electronic signature, Generic Addressing and Transport protocol, maritime radio, service provider access, Telecommunications Management Network (TMN), TETRA, VoIP, and xDSL.

ETSI's structure includes a general assembly, a board, a technical organization, and a secretariat. Its technical organization has primary responsibility for devising standards.

ETSI is headquartered in southern France. It currently (2003) has 789 members from 52 countries and five continents. Membership is open to any firm with an interest in European telecommunications. Each member pays an annual fee to join ETSI.

Extensible Markup Language

The *Extensible Markup Language (XML)* is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

For example, computer makers might agree on a standard or common way to describe the information about a computer product (processor speed, memory size, and so forth) and then describe the product information format with XML. Such a standard way of describing data would enable a user to send an intelligent agent (a program) to each computer maker's web site, gather data, and then make a valid comparison. XML can be used by any individual or group of individuals or companies that wants to share information in a consistent way.

Fault Management Resource Identifier

Each service instance in Solaris 10 SMF is named with a *Fault Management Resource Identifier (FMRI)*. The FMRI includes the service name and the instance name. For detailed information about FMRI, please read the Solaris 10 manuals from Oracle.

FIFO

See *First In, First Out*.

First In, First Out

The *First In, First Out* principle is a way of organizing and managing data relative to time and prioritization. This expression describes the principle of a queue processing technique or servicing conflicting demands by ordering process by first-come, first-served behavior: The data leave the queue in the order they arrive.

FM

Fault Management.

FMRI

See *Fault Management Resource Identifier*.

Graphical User Interface

A *Graphical User Interface (GUI)* is a graphical (rather than purely textual) user interface to a computer.

GUI

See *Graphical User Interface*.

HA

See *High Availability*.

High Availability

The *High Availability* capability provides multiple ESAs to cooperate and handling a switch over when it comes to handling the O&M operations in case the active ESA goes down when operating in Cluster Mode. Also see *Cluster Mode*.

IA

The *Information Agent (IA)* in the ESA provides ESA and system information on the SNMP interface.

IETF

See *Internet Engineering Task Force*.

International Organization for Standardization

The *International Organization for Standardization (ISO)* is an international standard-setting body composed of representatives from national standards bodies. Founded on February 23, 1947, the organization produces world-wide industrial and commercial standards, the so-called ISO standards.

International Telecommunications Union – Telecommunication



The *International Telecommunications Union – Telecommunication (ITU-T)* (for Telecommunication Standardization Sector of the International Telecommunications Union) is the primary international body for fostering cooperative standards for telecommunications equipment and systems. It was formerly known as the CCITT and is located in Geneva, Switzerland.

Internet Engineering Task Force

The *Internet Engineering Task Force (IETF)* is the body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFCs).

Internet Protocol

The *Internet Protocol (IP)* is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connection-less protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3 – the Networking Layer.

IP

See *Internet Protocol*.

ISO

See *International Organization for Standardization*.

ITU-T

See *International Telecommunications Union – Telecommunication*.

Java Cryptography Extension

The *Java Cryptography Extension (JCE)* is an officially released Standard Extension to the Java Platform. JCE provides a framework and implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.

Java Management Extensions

The *Java Management Extensions (JMX)* is a Java technology that supplies tools for managing and monitoring applications, system objects, devices and service oriented networks. Those resources are represented by objects called MBeans (Managed Beans).

JCE

See *Java Cryptography Extension*.

JMX

See *Java Management Extensions*.

JRE

Java Runtime Environment.

JVM

Java Virtual Machine.

Management Information Base

A *Management Information Base (MIB)* is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.

MIB

See *Management Information Base*.

Network Management System

A *Network Management System (NMS)* is an entity that handles the ISO network management model's five functional areas; Fault Management (FM), Configuration Management (CM), Performance Management (PM), Security Management (SM), and Accounting Management (AM). The functional areas have the following features. FM – detect, isolate, notify, and correct faults encountered in the network, CM – configuration aspects of network devices such as configuration file management, inventory management, and software management, PM – monitor and measure various aspects of performance so that overall performance can be maintained at an acceptable level, SM



– provide access to network devices and corporate resources to authorized individuals, and AM – usage information of network resources.

NMS

See *Network Management System*.

Object Identifier

An *Object Identifier (OID)* is, basically, a string of numbers. It is allocated in a hierarchical manner, so that, for instance, the authority for “1.2.3” is the only one that can say what “1.2.3” means. OIDs are used in a variety of protocols. The formal definition of OIDs comes from the ITU-T recommendation X.208 (ASN.1). The encodings – how you can transfer an OID as bits on the wire – is defined in X.209.

OID

See *Object Identifier*.

Open Systems Interconnection

An *Open Systems Interconnection (OSI)* pertains to the logical structure for communications networks standardized by the ISO. Adherence to the standard enables any OSI-compliant system to communicate with any other OSI-compliant system, for a meaningful exchange of information.

Operational Support System

An *Operational Support System (OSS)* is a set of programs that help a communications service provider to monitor, control, analyze and manage a telephone or computer network. See also *Network Management System*.

OSI

See *Open Systems Interconnection*.

OSS

See *Operational Support System*.

PDU

See *Protocol Data Unit*.

PM

Performance Management.

PMA

Performance Management Agent.

Protocol Data Unit

A *Protocol Data Unit (PDU)* is information that is delivered as a unit among peer entities of a network, and that may contain control information, address information, or data. In layered systems, a PDU is a unit of data that is specified in a protocol of a given layer and that consists of protocol-control information of the given layer, and possibly user data of that layer. The following PDUs are assigned to communicate within the given, specific, layers. LPDU – data link layer, NPDU – network layer, and TPDU – transport layer.

Proxy

A *Proxy*, or *Proxy server*, is a server between a client application, such as a web browser, and a real server. The proxy intercepts all requests to the real server, on the OSI application layer, to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Remote Method Invocation

The *Remote Method Invocation (RMI)* is a way that a programmer, using the Java programming language and development environment, can write object oriented programming in which objects on different computers can interact in a distributed network. The object can include information that will change the service that is performed in the remote computer.

For example, when a user at a remote computer fills out an expense account, the Java program interacting with the user could communicate, using RMI, with a Java program in another computer that always had the latest policy about expense reporting. In reply, that program would send back an object and associated method information that would enable the remote computer program to screen the user's expense account data in a way that was consistent with the latest policy. The user and the company both would save time by catching mistakes early. Whenever the company policy changed, it would require a change to a program in only one computer.

Remote Monitoring

The *Remote Monitoring (RMON)* is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information. RMON became a draft standard in 1995 as RFC 1757.

Request For Comment

See *Internet Engineering Task Force*.

**Response file**

A *Response file* is a configurable file that replaces manual input during a silent (unattended) installation.

RFC

See *Request For Comment*.

RMI

See *Remote Method Invocation*.

RMON

See *Remote Monitoring*.

SAS

See *Subagent AAL Synchronization*.

Secure Hash Algorithm

The *Secure Hash Algorithm (SHA)* is a group of hash algorithms used in cryptography.

Security Name

The *Security Name* identifies the user that is used when generating the notification if the USM security model is used. It identifies the SNMP community used when generating the notification if the v1 or v2c security models are used.

Service Management Facility

The *Service Management Facility (SMF)*, introduced in Solaris 10, provides an infrastructure that augments the traditional UNIX start-up scripts, init run levels and configuration files. For detailed information about SMF, please read the Solaris manuals.

Service Network Framework

The *Service Network Framework* was a concept used by Ericsson to integrate service network systems easily with each other. The MIBs used in the ESA originates from that framework.

SHA

See *Secure Hash Algorithm*.

Simple Network Management Protocol

The *Simple Network Management Protocol (SNMP)* is the protocol governing network management and the monitoring of network devices and their

functions. It is not necessarily limited to TCP/IP networks. SNMP is described formally in the IETF RFC 1157.

The *Simple Network Management Protocol version 1 (SNMPv1)* is described in RFC 1065 (Structure and identification of management information for TCP/IP-based internets), RFC 1066 (Management information base for network management of TCP/IP-based internets), and RFC 1067 (A simple network management protocol).

The *Simple Network Management Protocol version 2 (SNMPv2c)* is described in RFCs 1901 to 1908, and is widely considered the de facto SNMP v2 standard.

The *Simple Network Management Protocol version 3 (SNMPv3)* is described in RFCs 3411 to 3415 and 3584.

SMF

See *Service Management Facility*.

SMI

See *Structure of Management Information*.

SNF

See *Service Network Framework*.

SNMP

See *Simple Network Management Protocol*.

SNMP v1

See *Simple Network Management Protocol*.

SNMP v2c

See *Simple Network Management Protocol*.

SNMP v3

See *Simple Network Management Protocol*.

SSM

See *System Service Monitor*.

Structure of Management Information

The *Structure of Management Information (SMI)* defines the rules for describing management information. The SMI specifies that all managed objects should have a name, a syntax, and an encoding. The name is the OID, the syntax defines the data type of the object (for example, “integer” or “string”). A subset



of ASN.1 definitions are used for the SMI syntax. The encoding describes how the information associated with the managed object is formatted as a series of data items for transmission on the network. Another ISO specification, called the Basic Encoding Rules (BERs), details SMI encodings. The SMI for SNMPv2 includes the RFCs 1443 (Textual Conventions) and 1444 (Conformance Statements). The SNMPv2 SMI also defines security (1.3.6.1.5) and SNMPv2 (1.3.6.1.6), which are new branches of the Internet MIB tree.

Subagent AAL Synchronization

The *Subagent AAL Synchronization (SAS)* is a function in the ESA that provides the possibility to synchronize the AAL in the ESA with other AALs that already exists in the system.

System Service Monitor

The *System Service Monitor (SSM)* provides real-time, enterprise-wide system and application monitoring. It is an SNMP sub agent included in the ESA, accurately measuring the availability and performance of host systems and applications running on those systems. As such, it proactively monitors changing conditions about system configuration, status, and performance, as well as applications and file systems, and automatically notifies about detected problems. The SSM is configurable, to be adapted to the needs of a system or a user.

TCP

See *Transmission Control Protocol*.

Transmission Control Protocol

The *Transmission Control Protocol (TCP)* is a set of rules (a protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into, for efficient routing through the Internet.

UDP

See *User Datagram Protocol*.

User Datagram Protocol

The *User Datagram Protocol (UDP)* is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the TCP and, together with the IP, is sometimes referred to as UDP/IP. Like the TCP, UDP uses the IP to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end, and does not provide sequencing of the packets that the data arrives in.

This means that an application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

User-based Security Model

The *User-based Security Model (USM)* is a default security model defined by SNMP v3 framework (RFC 3414). It provides different types of security levels using various authentication and privacy protocols.

USM

See *User-based Security Model*.

VACM

See *View-based Access Control Model*.

View-based Access Control Model

The *View-based Access Control Model (VACM)* is a default access control model defined by SNMP v3 framework (RFC 3415). It is possible to restrict a particular group in accessing an OID in the MIB using VACM.

VIP

See *Virtual IP address*.

Virtual IP address

The *Virtual IP address* is an IP address assigned to multiple domain names, servers or applications residing on a single server instead of connected to a specific server or network interface card (NIC) on a server. Data packets are sent to the VIP address which are routed to actual network interfaces.

Windows Service

Previously called NT service, the core function of a *Windows service* is to run an application in the background. A few things make them different from a Windows application. A Windows service can be started at boot-up, before any user logs in to the system, or the user might be required to start it manually. Windows services have their own processes, and hence run very efficiently. Normally, a Windows service will not have a user interface for the simple reason that it can be run even if no one is logged into the system, but there can be a user interface.

XML

See *Extensible Markup Language*.

XML Schema



An *XML Schema*, also known as an *XML Schema Definition*, is a Recommendation of the World Wide Web Consortium (W3C), specifies how to formally describe the elements in an XML document. This description can be used to verify that each item of content in a document adheres to the description of the element in which the content is to be placed.

In general, a schema is an abstract representation of an object's characteristics and relationship to other objects. An XML schema represents the interrelationship between the attributes and elements of an XML object, for example a document or a portion of a document.

XSD

See *XML Schema*.