ERICSSON

Operation and Maintenance Description

TECHNICAL PRODUCT DESCRIPTION

13/221 02-AXB 250 10/4-V3 Uen CX

Contents

1 Introduction

This document describes Operation and Maintenance (O&M) functions in the EPG for GSM, WCDMA, and LTE radio access. The EPG allows for simultaneous use of the GGSN, PGW, and SGW logical nodes, and all are connected to the O&M network.

1.1 Scope

This document covers the following issues:

— O&M overview

— Configuration management

— Fault management

— Performance management

— Software management

— VM Migration

— Security Management

— Logs

— Troubleshooting

1.2 Target Groups

This document is intended as an introduction to O&M for network operators, network and service planners, as well as system engineers and administrators. It assumes a basic knowledge of data communication and telecommunication.

2 Overview

The EPG supports the Ericsson Open Interface (EOI) that is based on IETF standard Request for Comments (RFCs). The EPG uses the IETF-based YANG modeling language, which provides the same interface for both platform and EPG application.

The EPG is connected through the O&M network to external management systems, which can consist of Element Management, Network Management System (NMS), and Network Time Protocol (NTP) servers, see Figure 1.

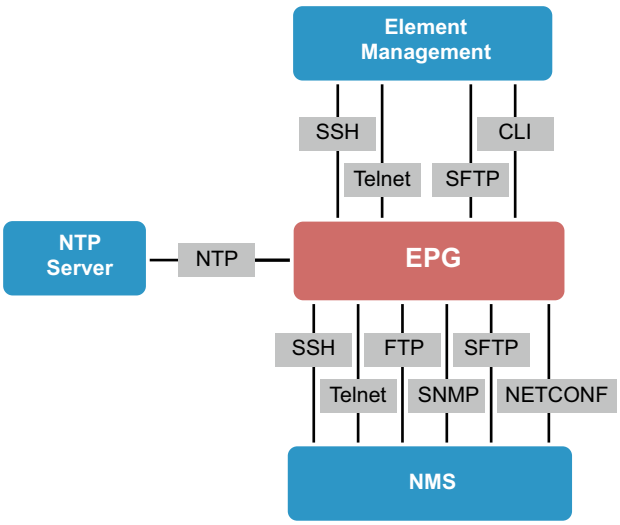

Figure 1 O&M Network Overview

The EPG provides in-band management connections on the Virtual Service-Forwarders (vSFOs).

For out-of-band management, the Ethernet management port on the Node Management Board (NMB) can connect to a management LAN, or any other device that plugs into an Ethernet connection.

For local access, the Console port on the NMB provides a system console using an RJ45 serial cable.

2.1 Element Management

The Ericsson Core Command Line Interface (ECCLI) is used for EPG element management. The ECCLI is accessed using Secure Shell (SSH) or Telnet, through various system ports or a remote network connection, see Section 2 on page 1.

Element management also includes transfer of files using Secure FTP (SFTP).

2.1.1 Command Line Interface

The ECCLI provides tools for configuring, monitoring, and troubleshooting the software, hardware, and network connectivity. It provides interactive help and command completion, and allows the operator to move around in a command to edit and view a buffer containing recently used commands.

The ECCLI handles the platform functions and the EPG application functions. For more information on the ECCLI, refer to EPG Software Configuration Overview.

For a list of all configuration and action commands, refer to EPG YANG Data Model. Detailed descriptions of the action commands can be found in the following documents:

— Action Commands for the GGSN and PGW

— Action Commands for the SGW

— Show Commands for the vRE

Note: CLI-configured limits on node capacity may not be reached due to system load, which depends on, for example, the traffic scenario, traffic distribution and hardware capacities.

Text can be pasted in the ECCLI when configuring EPG services, but the EPG does not support pasting of more than 4kB of text in the ECCLI at once.

The CLI access and the NETCONF access share one user session capacity. The maximum number of user sessions for CLI and NETCONF access is 32.

2.1.2 Life Cycle Status for O&M Elements

Figure 2 describes the life cycle and allowed transitions of the O&M elements in the areas of configuration management, fault management, and performance management.

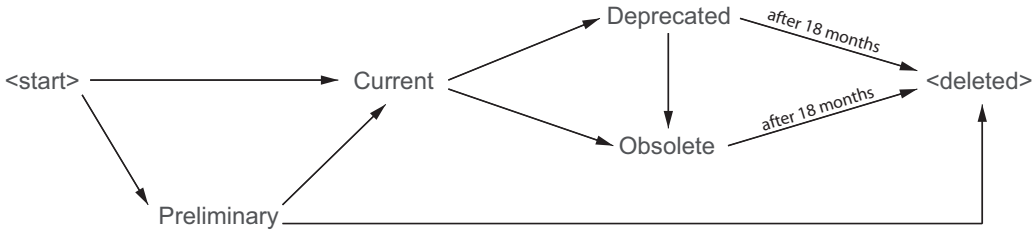

Figure 2 O&M Element Life Cycle

Preliminary The definition of the element is still preliminary such that the element might not work as expected. The properties of this entity may be modified and removed in any way between model versions.

Current/Used The definition of the element is current and valid. From the point where an element is marked as CURRENT, only Backward Compatible changes to its properties should be made between model versions.

Note: CURRENT is substituted by USED in the fault management and performance management.

Deprecated The element has a formal definition that is Backward Compatible and has the same functional behavior as before, but will be removed after 18 months.

Obsolete	The element has a formal definition that is Backward Compatible but has a functionally different behavior compared to when it was CURRENT, and will be removed after 18 months. The element can be used as before, but it might be that, for example, updating the attribute has no effect on the target system.

2.2 Network Management System

The NMS handles subnetwork management for several nodes. An example of an NMS is the Ericsson Network Management (ENM). The O&M protocols used for communication and transfer of data are SNMP, FTP, and NETCONF. FTP is only supported for EPG as an FTP client. SSH also provides support for SFTP, which enables automatic encryption, authentication, and compression of the transmitted data.

The ENM supports fault management, performance management, software management, and Backup and Restore Management (BRM).

2.2.1 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is required to integrate standard network management and monitoring systems. The EPG supports industry-defined standard Management Information Bases (MIBs) as well as private MIB definitions. An example of this is the Ericsson Alarm MIB for handling fault management on the EPG applications.

The EPG supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2c), and SNMP version 3 (SNMPv3).

2.2.2 NETCONF

NETCONF is an Extensible Markup Language (XML)-based management protocol that defines operations for accessing and updating a configuration data store remotely. The NETCONF protocol is driven by the EPG YANG Data Model. The EPG applications can be configured using NETCONF.

Note: The CLI access and the NETCONF access share one user session capacity. The maximum number of user sessions for CLI and NETCONF access is 32.

For more information on how to use NETCONF, refer to NETCONF Interface for YANG.

2.3 Network Time Protocol

The synchronization of time between all nodes in the GPRS and EPS systems is based on NTP. NTP is also used internally to synchronize EPG components with the system clock of the node. All elements are configured to use the Universal

Coordinated Time (UTC) time regardless of the geographical location of the node. In this way, it is possible to compare the time-related information from different nodes that are distributed geographically in different time zones. The NTP is also designed to handle leap seconds.

NTP gives, for a reasonably configured and designed network, a time accuracy between 1 and 50 ms between nodes in the network. For a large and perhaps complexly configured network, the time difference may be greater.

NTP is implemented on the NMB. The NMB takes the role of an internal NTP server for all vSFOs.

The EPG supports NTP versions 1, 2, and 3. NTP operates in client mode only, that is, the EPG can be synchronized to a remote NTP server, but a remote server or node cannot be synchronized to the EPG.

NTP must be configured on the EPG. NTP is assumed to use redundant servers.

For more information on NTP, refer to document Network Time Protocol.

For more information on NTP and time zone configurations, refer to EPG Time Configuration.

2.3.1 Stratum Levels

The NTP protocol is used to distribute time according to a defined stratum schedule. A time source stratum level describes how far from the UTC source it resides. In Figure 3, the stratum levels are depicted. The location of the GPRS and EPS nodes in the stratum hierarchy is indicated as an encircled entity.

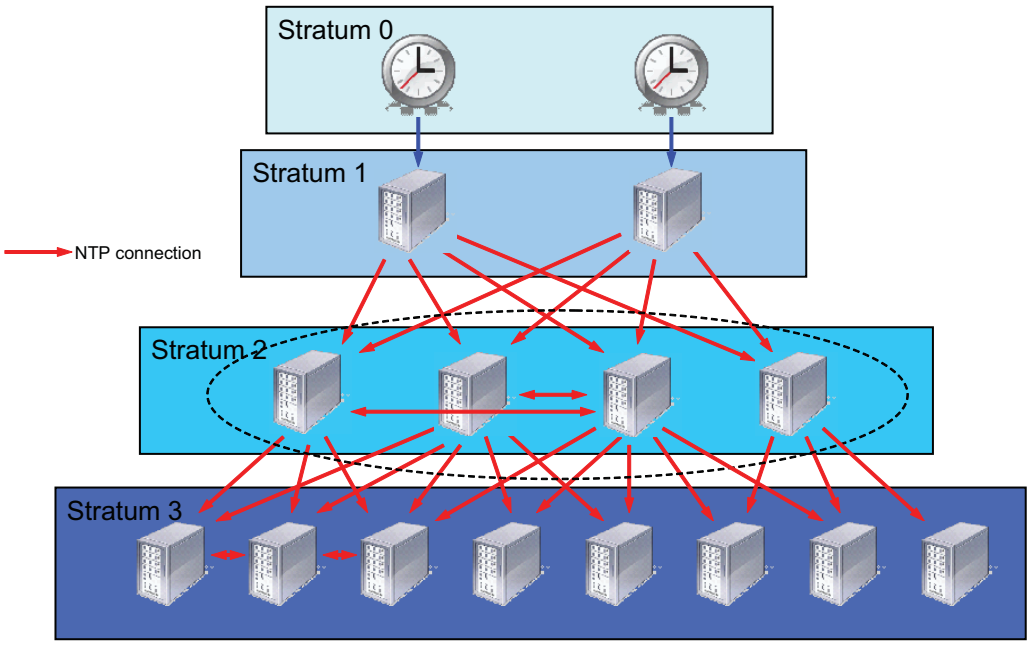

Figure 3 Stratum Levels

An NTP client on a certain stratum level usually has several NTP servers to connect to. The NTP client mainly connects to lower stratum levels, but it can also connect to servers on the same stratum level. NTP has built-in algorithms to compensate for the delay variations encountered in the network. By means of these algorithms and certain criteria, the most reliable and accurate NTP server is then selected for time synchronization. One of the criteria that needs to be fulfilled is that the server clock itself must have been synchronized in the last 24 hours.

Servers that are directly connected to a reference clock are termed stratum 1 servers. In a typical mobile core network, these servers are specialized time servers equipped with Global Positioning System (GPS) receivers. A reference clock connected to a stratum 1 server is referred to as a stratum 0 server. Clients never communicate directly with a stratum 0 server, instead they always go through a stratum 1 server synchronized to a stratum 0 server. Clients of stratum 1 servers are referred to as stratum 2 clients. If they serve time to clients, they are also referred to as stratum 2 servers, and the clients they serve are referred to as stratum 3 clients. This continues similarly to higher numbered strata.

The poll interval for time synchronization varies between a minimum of 64 seconds and a maximum of 1024 seconds (17 minutes). The starting poll interval is always 64 seconds, and, depending on a number of circumstances tracked by the NTP client, the poll interval varies between the minimum and maximum poll interval. There can be a maximum of ten servers per client, which is the highest number that the algorithms in NTP are designed to handle.

2.3.2 Free-running Oscillation

Free-running oscillation of each server internal clock happens when synchronization to a common time source is unreachable. The consequence of free-running oscillation is that the internal server clock slowly drifts over time, due to the internal oscillating source inaccuracy, for example a quarts oscillator, as well as temperature changes in the environment.

This means that end-user billing data transmission can be interrupted by a number of faults causing free-running oscillation, such as a faulty switch.

2.3.3 Security through MD5

The EPG software supports the TCP MD5 authentication option for Border Gateway Protocol (BGP) sessions and Open Shortest Path First (OSPF). MD5 is a message digest algorithm, which is carried as an option in the TCP header of a BGP and OSPF message. The message is not encrypted, but the MD5 protects the validity of the contents of each message. Each peer has a shared secret password that is never sent across the network. The peers use this password to generate and verify the algorithm. MD5 protects against hacker attacks.

3 Configuration Management

The configuration management functions enable the operator to configure and monitor the EPG. The parameters can be set, modified, and displayed from the ECCLI at any given time when the EPG is up and running.

Configuration management can also be done using NETCONF.

Note: The EPG does not support configuration management using SNMP.

For information on configuration management, refer to EPG Software Configuration Overview.

3.1 Equipment Management

The virtual EPG has no direct coupling to the physical hardware it is deployed on. The virtual EPG does not provide any status, alarms, or counters related to the physical hardware. The cloud infrastructure needs to provide this information for the operator. However, the VMs are monitored and can be restarted, blocked, and deblocked.

Each VM in the EPG is assigned a unique index or identifier. The index or identifier is used to configure and manage each VM individually. The vRPs are always the dedicated identifiers vRP1 and vRP2. The vSFOs receive an index between 1-20.

4 Fault Management

The purpose of fault management is to report detected failures and to limit the effect of these failures on the network performance. An NMS, such as ENM is commonly used as the fault management monitoring system. Under SNMP management, the EPG can send SNMP trap notifications to the NMS server. SNMP uses connectionless User Datagram Protocol (UDP) transport, this means no acknowledgement of notifications. The SNMP manager in the NMS server can regularly poll the EPG to verify the status of alarms and alerts. A general rule is that generated alarms are automatically cleared when the error causing the alarm ceases to exist.

For more information on fault management for the EPG applications, refer to Fault Management Description. For more information on fault management for the platform, refer to Fault Management.

5 Performance Management

The performance management function enables the operator to collect information to monitor the behavior of the EPG or of the EPG KPIs. The performance management data are collected by PM jobs. The collected PM data files are stored on the ENM file system.

For more information on performance management, refer to Performance Management Description.

For more information on performance management interface, refer to Performance Management Interface Description.

For more information on counters and gauges, refer to Counters and Gauges for the EPG on Node Level, Counters and Gauges for the EPG on Node Level, Counters and Gauges for the SGW, and Performance Measurement.

5.1 Performance Monitoring with PM Report Files

PM report files are generated in XML format for PM jobs by reporting period or job group. The PM file format is based on the XML schema defined in 3GPP document TS 32.435 V12.0.0 (2014-10). For details, refer to Performance Management Log.

5.2 Performance Monitoring with Action Commands

For performance management, the ECCLI commands can be used to monitor, maintain, and troubleshoot the EPG.

For EPG application, refer to Action Commands for the GGSN and PGW and Action Commands for the SGW.

For virtual EPG, refer to Action Commands for the vRE and Show Commands for the vRE.

5.3 Performance Monitoring with PDC

The Performance Data Collection (PDC) tools are included in the EPG Toolbox, which is introduced in Section 10.1 on page 10. The PDC can be used to obtain some performance indicator readings. The PDC is enabled by default. The PDC also provides the possibility to list counter-values, and calculate PM-related Key Performance Indicators (KPIs). Only a limited subset of counters is accessible through the PDC. For more information, refer to Toolbox Description.

6 Software Management

The virtual EPG is delivered as two software packages:

— Virtual Deployment Package (VDP): It is used for deployment of the virtual EPG

— Install package: It is used for software upgrade of the virtual EPG

The VDP contains the following:

— VM images

— Script and associated configuration template for generating an OVF package

— Script and associated configuration template for scaling

For more information, refer to Deploying Virtual EPG and Software Upgrade for Virtual EPG.

6.1 Software Upgrade

A software upgrade is a major functional change of the software applied between different main product releases.

A main product release is a collection of releases indicated by a number plus ".0", such as 1.0. 2.0, 3.0.

The software upgrade is handled internally by the EPG, and requires no interaction with the cloud system. For example, new VM images corresponding to the new software level do not need to be uploaded to the cloud system for the upgrade.

For more information, refer to Software Upgrade for Virtual EPG.

6.2 Backup and Restore

When a backup is performed, all software, configuration, and files, except charging data and log files, are backed up. Restoring is a fallback procedure that uses the backup to bring the EPG configuration back to the same state as when the dump was saved.

For information on backing up and restoring the virtual EPG, refer to Backing Up and Restoring the EPG.

7 VM Migration

The current existing cloud infrastructures are likely not able to migrate the virtual EPG VMs with short enough VM interruption. The virtual EPG is designed for telecom grade resilience. Therefore, it quickly initiates takeover or failover if a VM becomes unresponsive. Time-outs on higher levels, for example, SCTP and BFD can also trigger various recovery procedures. Therefore, it is recommended to migrate the virtual EPG only after traffic is off-loaded or redirected to another EPG.

8 Security Management

In addition to local authentication, the EPG can be configured to use RADIUS or Terminal Access Controller Access-Control System (TACACS+) authentication, or both, to validate operators who attempt to access the EPG using Telnet. The EPG supports secure protocols such as SSH, Secure Copy (SCP) protocol, and SFTP.

For more information on security functions, refer to Security and Security Management.

9 Logs

The EPG provides logs that record event information about the system operation, performance, and alarms. The logged information can be used for statistics and tracing purposes. For more information about logging, refer to EPG Logs.

10 Troubleshooting

The EPG provides toolbox and features for troubleshooting the EPG software.

For more information on troubleshooting procedures for the EPG, refer to Troubleshooting the EPG Software.

10.1 EPG Toolbox

The toolbox is a collection of tools for facilitating maintenance and troubleshooting of the EPG. For more information, refer to Toolbox Description.

10.2 Event-Based Monitoring

The Event-Based Monitoring (EBM) feature can be configured to collect data on specified mobility and session events. The collected information can be used as additional performance data. For more information on EBM, refer to Event-Based Monitoring.

10.3 Integrated Traffic Capture

Integrated Traffic Capture (ITC) is used to capture control plane traffic on all Control Processing Boards (CPBs) and user plane traffic on all Packet Processing Boards (PPBs) simultaneously.

For more information on ITC, refer to Integrated Traffic Capture.

10.4 UE Trace

The UE Trace feature allows the EPG to record detailed information about signaling information that the EPG sends out, and payload. UE Trace is used for troubleshooting, monitoring, and optimization operations. UE Trace can be used separately on the control plane and user plane for one or more selected UE devices. The network operator identifies the selected UE device by using the International Mobile Subscriber Identity (IMSI).

For more information on UE Trace, refer to UE Trace.

For more information on UE Trace log files, refer to UE Trace Log.

For more information on how to convert log files to plain text or PCAP format for UE Trace on Control Plane, refer to Toolbox Description.