SGSN-MME 2010 System Administration

Solution to Exercises

Intentionally Blank

Table of Contents

Exercise 1 Basic System Operation

CASE 1: FIND AND SHOW PLMN INFORMATION

OBJECTIVES:

Upon completion of this case the student will be able to find and show the PLMN Identification information on the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation:

Manual pages “PLMN Identification (CLI)”

DISCUSSION

The CLI and OSS - RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

What is this PLMN information used for?

The Public Land Mobile Network (PLMN) is the network to which the Serving GPRS Support Node (SGSN-MME) belongs. PLMN information is communicated to the MS or UE over the air interface to facilitate appropriate attach and update requests to the network.

The MCC and MNC of the PLMN must be specified for the following reasons:

All Routing Area Identities (RAIs) and Cell Global Identities (CGIs) of routing areas and cells in the PLMN contain the same MCC and MNC. The MCC and MNC are used when specifying the RAIs and CGIs. Remember that the IMSI number series is used by an MS/UE to the correct HLR for accurate information on the MS/UE. The IMSI starts with MCC+MNC+MSIN, we can identify which country and which operator a MS/UE belongs to.

The Default Access Point Name (APN) Operator Identifier (ID) is derived from the MCC and the MNC. The Default APN Operator ID is used to identify the network that a particular APN belongs to, as this is appended to the presented APN for DNS resolution.

What happens when you add Country Initials?

When this item is selected it is to specify if the country initials should be shown on the display of the MS or UE, when it is attached to the network.

What is the Default APN Operator ID used for?

The default APN Operator ID is a fully qualified Domain Name System (DNS) name, which is generated out of the MNC and the MCC of the PLMN as follows:

mncMNC.mccMCC.gprs

It is how the PLMN is known in the IP network. The Default APN is added to the APNs DNS name to create a fully qualified DNS name for each APN within a PLMN. E.g. ericsson.com.se.mnc003.mcc240.gprs. This is done so whenever an MS/UE is roaming into another operator's network. This allows for the MS/UE to use the SGSN-MME in the Visiting network, and the GGSN of your home network. When you are using GPRS to access your Corporate LAN (for example), this would be tied to the GGSN of your home network. Therefore there would have to be a roaming agreement between the two operators. Also to secure traffic between the two networks the Gp interface would be established between the two networks.

Further Questions for Discussion during Conclusion

-

CLI Commands

list_plmns

get_plmn [plmn name]

list_cmds

list_sort_cmds

CASE 2: CREATE A PLMN IDENTITY

OBJECTIVES:

Upon completion of this case the student will be able to create a new PLMN identification and its relevant details on the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual pages “PLMN Identification (CLI)”

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

What did your Default APN operator ID becomes?

Group dependent answer - from: mnc*xxx*.mcc*xxx*.gprs

Why can you have more than one PLMN identities?

The SGSN-MME may belong to more than one PLMN in order to support different networks on the same hardware.

What is the difference between the CLI commands set_plmn and create_plmn?

The set_plmn command is used to modify an existing PLMN Identity while the create_plmn is used to add a new PLMN identity.

Further Questions for Discussion during Conclusion

The PLMN identities question should lead to a discussion of the concept of Multiple PLMNs on one SGSN-MME. This being so operators can share networks using the concept of equivalent PLMNs, with the MS / UE receiving a list of up to 5 equivalent PLMNs (MCC+MNC) which is downloaded to MS/UE in the Attach Accept and RA Update Accept messages.

CLI Commands

create_plmn Hplmn Name –mcc *** -mnc *** [- fnn full network name] [-snn

short network name] [-ci]

get_plmn Hplmn name

delete_plmn

CASE 3: SHOW LOCAL SGSN-MME DATA

OBJECTIVES:

Upon completion of this case the student will be able to find on the SGSN-MME, the local SGSN-MME information, such as the SGSN-MMEs' ISDN number and node identity.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual pages of "Local SGSN-MME (CLI)"

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

On the SGSN-MME, what is the CN-ID used for?

The CN-Id variable uniquely identifies a physical SGSN-MME. Within a Public Land Mobile Network (PLMN) the CN-Id is unique, and together with Public Land Mobile Network Identity (PLMN-Id) (Mobile Country Code (MCC)+Mobile Network Code (MNC)) it is globally unique, constituting a global CN-Id.

What is the International ISDN number used for?

To identify the SGSN-MME for SS7 signaling (actually the own calling address of the SGSN-MME, an SCCP addressing function). The ISDN Number is used as source address, a so-called SGSN-MME number, in outgoing Mobile Application Part (MAP) or Base Station System Application Part (BSSAP+) signaling messages towards a Home Location Register (HLR) or Mobile Service Switching Center/Visitor Location Register (MSC/VLR). In Signaling Connection Control Part (SCCP) there must exist a Global Title Translation that matches the ISDN Number. It is not possible to delete the ISDN number. The global title must be written to route the SCCP messages to and from the SGSN-MME node.

What is the name of the network and the interface that access the GPRS backbone IP network that IP network?

Interface - Gn

Further Questions for Discussion during Conclusion

CLI Commands

get_ne

get_sgsn

CASE 4: SHOW SGSN-MME IP SERVICES

OBJECTIVES:

Upon completion of this case the student will be able to view and understand the IP Services provided and configured in the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual Page of “IP Service (CLI)”

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

On the SGSN-MME, what is the Gn-GTP-C used for?

The Gn-GTP-C service is used for all GTP control traffic over the Gn and Gp interfaces.

What is the Gn-GTP-C VPN IP Address ?

Node dependent answer

Further Questions for Discussion during Conclusion

CLI Commands

list_ip_service

list_ip_service_address

CASE 5: GSM SYSTEMS ONLY - ADD A BASE STATION CONTROLLER (BSC) TO THE NETWORK

OBJECTIVES:

Upon completion of this case the student will be able to create and connect a BSC to the network plan on the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual pages of “BSC (CLI)

“GPRS Overview” Description - 13/1551-AXB 250 05/3 Uen B

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

How many SGSN-MME can one BSC be connected to?

One.

At this point you can introduce the SGSN-MME Pool feature. SGSN-MME pool is an optional feature supported for SGSN-MMEs 2010B using Gb over IP.

Further Questions for Discussion during Conclusion

-

CLI Commands

list_bscs

create_bsc [bsc name]

delete_bsc

CASE 6: WCDMA SYSTEMS ONLY - ADD A RADIO NETWORK CONTROLLER (RNC) TO THE NETWORK

OBJECTIVES:

Upon completion of this case the student will be able to create and connect a RNC and LRA to a network plan on the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation:

Manual Pages:

- ”Local Routing Areas WCDMA (CLI)”
- “RNC – General (CLI)”
- “RNC Routing Areas (CLI)”

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

How many LRA’s can be at most associated with one RNC ?

Maximum 800

Further Questions for Discussion during Conclusion

Why are the equivalent PLMNs specified?

The Equivalent PLMN IDs parameter is a list of PLMN Ids. The list is sent to the mobile station to indicate what other PLMNs are to be considered as equivalent to the one stated in the Routing Area (RA). A list of equivalent PLMNs (MCC + MNC) can be downloaded to the UE in the Attach and Routing Area Update Accept messages.

The UE will then treat the PLMN codes, which it has received as equivalent to each other at PLMN selection and cell change. The UE selects an equivalent PLMN at roaming if UE is within the coverage of one of the equivalent PLMNs. It is possible to define a list containing up to 5 Equivalent PLMNs per Routing Area (RA).

CLI Commands

list_rncs

list_wras

create_rnc *RncName* -id *RncId* -pid *PlmnId* -spc *RncSPC* [-rai *Rai*]

create_wra *Rai* [-name *RaName*]

connect_rnc_ra *RncName* -rai *Rai*

delete_rnc [*rnc name*]

CASE 7: GSM SYSTEMS ONLY - ADD A MOBILE SWITCHING CENTRE (MSC) TO THE NETWORK

OBJECTIVES:

Upon completion of this case the student will be able to add an MSC to the network plan on the SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual pages of ”MSC/VLR - General (CLI)”

Manual pages of “MSC/VLRs Location Area (CLI)

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

What did you notice when deleting the MSC?

Unable to delete MSC while it is associated with a LA.

Further Questions for Discussion during Conclusion

-

CLI Commands

list_mscs

create_msc MscVlrName -isdn IsdnNumber

delete_msc [msc name]

disconnect_msc_la Lai -msc MscVlrName

create_msc_la Lai

connect_msc_la Lai -msc MscVlrName

CASE 8: ADD NEW IMSI NUMBER SERIES INFORMATION

OBJECTIVES:

Upon completion of this case the student will be able to configure IMSI series information in the SGSN-MME node.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Manual page of “IMSI Number Series (CLI)”

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

In roaming status, what does the Status “visitor” imply?

Home, indicating subscribers within that IMIS number series range belong to the home PLMN or a PLMN belonging to that SGSN-MME. The status “visitor” implies that the IMSI number series range is for visiting subscribers to the PLMN and the subscriber belonging to another PLMN.

Further Questions for Discussion during Conclusion

For an E.214 address why are you removing and adding digits to the IMSI number series?

The IMSI number series is used as follows to address the HLR of the subscribers:

If the numbering plan is E.212, the IMSI number (according to E.212), is used to address the HLR. If the numbering plan is E.214, the modified IMSI (where a number of digits have been removed and specific digits added) is used to address the HLR.

For E.214 you are changing part of the IMSI number of the subscriber to one IMSI number that will address the HLR.

This is used at GPRS attach procedure.

With this data, what network element are you addressing?

The HLR that contains the subscriber data for that particular IMSI number series.

When is this node addressed?

As part of Mobility management e.g. when attaching to the network.

CLI Commands

list_imsins

create_imsins ImsiNumberSeries -rs RoamingStatus -dn DomainName -np

NumberingPlan [-na NatureOfAddress] [-rd NoOfDigitsToRemove] [-ad

DigitsToAdd] [-misc1 String] [-misc2 String] [-misc3 String] [-phase3

true|false][-qpmg QosPolicyMap] [-qpmw QosPolicyMap]

CASE 9: DISPLAY INFORMATION OF PLUG-IN UNITS

OBJECTIVES:

Upon completion of this case the student will be able to find and display the information of specified PIU in SGSN-MME node.

REFERENCE LITERATURE

The students use the Alex Library for documentation.

Direction for Use “Equipment Management (PXM)”

Manual page of “Plug-in Unit (CLI)”

DISCUSSION

The PXM GUI and CLI provide all Discussion to do the exercises.

Questions in the student text for Discussion

What happen when a PIU used for payload DP is blocked?

For a payload DP the block request is denied if the remaining resources in the Serving GPRS Support Node (SGSN-MME) can't handle the increased load or there is another block ongoing (not finished) or other recovery event is ongoing (initiated and not yet finished).

The -force flag makes it possible to override and block a PIU even if the remaining resources in the SGSN-MME can't handle the blocked PIUs load.

When blocking a PIU used for payload Device Processor (DP), a DP take over is initiated.

How do you know which PIUs are blocked?

list_eq *blocked*

Further Questions for Discussion during Conclusion

CLI Commands

get_active_ncb, get_eq_info -eq *EqID,* get_fsb_info

CASE 10: CHANGE PASSWORD

OBJECTIVES:

Upon completion of this case the student will be able to check which users are currently working on the SGSN-MME, and change the password.

REFERENCE LITERATURE

The students use the Alex Library for documentation Directions for Use,

Manual pages of “User Administration”.

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

How many characters of the password does the system recognize?

Only the first eight characters of the password are significant, that is, the passwords " 12abcdef" and "12abcdefghi" are the same from the systems point of view. At least one must be a non-lower case letter.

Can you change the passwords with CLI?

Yes.

Change your role to system administrator. What happens?

Not allowed

Further Questions for Discussion during Conclusion

The students are logged in as *user1, user2, user3* and *user4* with the role *userRole*. When they try to change their role to system administration, they will find out that this is not possible. This is what was intended when the Action Sets where set for the *userRole.* In this way access restrictions can be generated.

CLI Commands

list_sm_users

passwd

set_sm_roleToUser

CASE 11: SOFTWARE CONFIGURATION

OBJECTIVES:

Upon completion of this case the student will be able to check which Software Configuration is currently loaded on the SGSN-MME and which Software Configuration will be loaded during reload(s).

REFERENCE LITERATURE

The students use the Alex Library for documentation

Directions for Use, “Software Configuration Management”

Manual Pages of “Software Configuration (CLI)”

DISCUSSION

The PXM GUI and CLI provide all Discussion to do the exercises.

Questions in the student text for Discussion

When is the default SC loaded?

If the next restart SC is not stable and another restart is triggered the default SC will be loaded. This is written to the next restart file after a reload has occurred. This SC should be a proven reload Software Configuration.

How do you checkpoint the system to create a new SC?

By clicking on the “checkpointing an active SC” a dialogue box is displayed whereby you enter a logical name for the new SC. The logical name is added to the list of checkpointed SCs below the name of the active release.

How do you ensure your new SC will be used in the next restart of the node?

Select the SC you want to use at the next packet switching node restart. Click the Use for Next Restart button. Then the Next Restart field at the top of the form is updated with the name of the specified SC.

How often is the periodic checkpoint performed?

Node specific answer – default is never

Further Questions for Discussion during Conclusion

Discuss Periodic checkpoint interval – what is actually being checkpointed. After the conclusion it is useful to give a demonstration to the students: (1) Checkpoint the active SC; now the active SC differs from the SC used for the last restart. (2) Set the SC for next restart. (3) Initiate a node restart from the NCB and monitor the restart. The SC used for the next restart has changed to the active SC.

The active SC differs from the SC used for the last restart after Checkpointing. In the “Software Configuration” window further more an SC for a “Default Restart” is listed. Tell them in the conclusion that after a restart with the specified SC for “Next Restart”, a further restart will use the default SC. This prevents the GSN from cyclic restarts. Review restart levels with the students from Chapter 2 theory. The Software Configuration Screen is often very slow to come up. Note that student’s node access will not allow them to configure the SC details.

CLI Commands

get_active_sc

get_booted_sc

get_checkpoint_interval

get_default_sc

checkpoint {[-rel *ReleaseName*] -cpn *CheckpointName*}

listSCs

set_default_sc

set_next_sc { -rel *ReleaseName* [-cpn *CheckpointName*]}

CASE 12: LICENSED FEATURES AND FUNCTIONS MANAGEMENT

OBJECTIVES:

Upon completion of this case the student will be able to check the states of licensed features and make them activated on SGSN-MME node. Also student will be able to check and modify the states of functions.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Operation Directions of “Features and Functions Management”

Manual Pages of “Feature Management (CLI)”

DISCUSSION

The CLI and OSS-RC provide all Discussion to do the exercises.

Questions in the student text for Discussion

Can you modify values of both? How?

The two functions needn’t any license but both are based on SGSN-MME G node. The state values of both can be check and modify with respectively **get_nodeprop** and **set_nodeprop**.

The four license-controlled features need supplementary configuration with CLI command **set_nodeprop**. For example, Gb_PeriodicAuthenticationTimer for **Authentication of Stationary Subscribers,** Charging_Ch-SGSN-MME-Multiple-PLMN for **Multiple PLMN Support** Gn_DefaultAPNGSMNetwork and Gn_DefaultAPNUMTSNetwork for **APN Redirection,** Gb_MS_`inactivity_time_limit` for **Detach of Inactive Subscribers.**

CLI Commands

action_ne_emergency_unlock

get_capacity -name *CapacityName*

get_feature -name *FeatureName*

list_capacity [-ps *PlanState*][-name *CapacityName*][-keyId *LicenseKeyId*][-par *CapacityParameter*]

list_feature [-ps *PlanState*][-name *FeatureName*][-keyId *LicenseKeyId*][-lic *LicenseState*][-state *FeatureState*]

modify_feature -name *FeatureName* [-state *FeatureState*]

get_nodeprop NodePropId

list_nodeprops

set_nodeprop NodePropId -val *Value*

Exercise 2 Alarm and Event Handling

CASE 1: ALARMS

OBJECTIVES:

Upon completion of this case the student will be able to check active and cleared alarms in PXM and OSS-RC on the SGSN-MME node.

REFERENCE LITERATURE

The students use the Alex Library for documentation and OSS-RC help.

Operation Direction, “Alarm Handling”

DISCUSSION

The PXM GUI and OSS-RC provides all Discussion to do the exercises.

Questions in the student text for Discussion

How many and which alarms are existing?

Node specific answer

How can you get detailed information about the alarms?

Answer 1 - Alarm and Event Panels Beneath the alarms or events table there is a panel of text fields. When you select an alarm or event entry from the table above, the information is fully displayed in these text fields.

Answer 2 - Use the pull down menu - Help On Selected Items You can select any alarm or event in any of the tabs to obtain more information. For instance, the explanation, background, proposed solution, and consequences of an alarm or an event are displayed.

Are there any active alarms on the SGSN-MME?

The node keeps a list of all currently active alarms. If the Alarms and Events PXM form is used, the list can be viewed in the PXM window. Node specific answer.

After re-activating deactivated alarms - Do you notice any changes in the alarm list? What about the alarms in the PXM Main Window? The OSS-RC alarms window?

The alarms are now displayed.

How do you differentiate between active and cleared alarms in the "Alarm and Events" window?

If the cause of an alarm is removed, the node automatically removes the alarm from the alarm list. It also logs the cleared alarm in the alarm log. If the node fails to clear an alarm, the alarm can be manually cleared with Alarm Force Clear. Cleared alarms will not be displayed here.

How do you get information about older alarms?

Check the alarm log in the logs

Further Questions for Discussion during Conclusion

-

CLI Commands

list_alarms

list_events

clear_alarms [fault id]

=== sysadm@eqm01s14p2 ANCB ~ # gsh get_fm_filter

Include alarms/events raised since: <not defined>

Include Type Severity Category Name

Yes alarm major qos admAttachCapacityReached

Yes alarm minor qos admAttachLicenseExceeded

Yes alarm major qos admContextCapacityReached

Yes alarm minor qos admContextLicenseExceeded

Yes alarm major communications atmLBCellsMissing

Yes alarm major communications atmLineAlarmIndicationSignal

Yes alarm major communications atmLineRemoteDefectIndication

Yes alarm major communications atmLossOfFrame

Yes alarm major communications atmLossOfPointer

Yes alarm major communications atmLossOfSignal

Yes alarm major communications atmPathAlarmIndicationSignal

Yes alarm major communications atmPathRemoteDefectIndication

Yes alarm major communications atmVCAlarmIndicationSignal

……

[Interrupted printout]

Note: The modify_fm_filter_date CLI command, modifies the parameter Alarm/Event Raised Since of the selected fault manager filter, see Parameter Description SGSN-MME 2010B (G), Parameter Description SGSN-MME 2010B (W) or Parameter Description SGSN-MME 2010B Dual Access. The date and time operands define after which point in time, alarms or events shall have been raised in order to pass the filter. If the date and time operands are left out the time based filtering is set to default. The filtering is done over the Simple Network Management Interface (SNMP).

modify_fm_filter_date [-id FilterId] [-date Date] [-time Time]

i.e

=== sysadm@eqm01s14p2 ANCB ~ # gsh

modify_fm_filter_date -id snmp -date 2010-08-06

=== sysadm@eqm01s14p2 ANCB ~ # gsh get_fm_filter

Include alarms/events raised since: **2010-07-16 00:00**

Include Type Severity Category Name

```
------------------------------------------------

Yes alarm major qos admAttachCapacityReached

Yes alarm minor qos admAttachLicenseExceeded

Yes alarm major qos admContextCapacityReached

Yes alarm minor qos admContextLicenseExceeded

Yes alarm major communications atmLBCellsMissing

……

[Interrupted printout]
```

CASE 2: FAN FAULT

OBJECTIVES

The students will be able to detect, investigate and clear alarms related to fan hardware fault.

REFERENCE LITERATURE

Operation Direction: “Alarm Handling”

Direction for Use: “Alarms and Events (PXM)”

User Guide: “Fault Manager Alarm List Viewer (OSS-RC)”

DISCUSSION

Alarm: **hwFanError**

Event 1

Look in the active alarms, did you find any related to Fan hardware fault? In which magazine did the fault occurred?

Node dependent. Example- Magazine 1. Alarm will indicate error on 1.1 and 1.21

Event 2

What is the cause of the alarm (look in CPI)? What will eventually happen if the all the fans in the magazine fail?

The hwFanError alarm is generated if the Fan Unit attached to the PEB reports an error, due to the fan not spinning, or broken/disconnected fan sensor cable to the PEB. . The alarm will be set/reported from both PEBs since the Fan Unit are connected to both

CASE 3: FAULTY PIU

OBJECTIVES:

Upon completion of this case the students will be able to solve and clear an alarm concerning a faulty PIU on SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library and OSS-RC help for documentation

Directions for Use, “Alarms and Events (PXM)”

User Instructions about Platform Alarms.

DISCUSSION

The PXM GUI and OSS–RC provides all Discussion to do the exercises.

Questions in the student text for Discussion

Look in the active alarms list, which alarm has been raised recently about hardware failures. Give an explanation of what has happened.

DpeHardwareFailure Fault - Alarm/Notification Text - Hardware error detected by DPE.

This is a logical alarm raised by the NCB to indicate, that a hardware unit is no longer responding. The reason for the fault can be either a software fault or real hardware fault.

Figure out what the problem is (look in the user instruction) and find out, how the problem can be solved.

Fault Tracing Direction states – action to be taken:

If the alarm ceases within 4 minutes from its origin and is not raised again a software fault has occurred and no actions need to be taken. A persistent dpeHardwareFailure alarm indicates, that the unit does no longer reply. In this Exercise, onsite investigation is needed to analyze if a hardware replacement is needed.

Solve the problem by replacing the faulty PIU with a good one.

Visit the node and replace / reinsert the faulty PIU

Further Questions for Discussion during Conclusion

-

CLI Commands

list_alarms

CASE 4: LINK FAILURE

OBJECTIVES:

Upon completion of this case the student will be able to solve and clear an alarm concerning a link failure on SGSN-MME.

REFERENCE LITERATURE

The students use the Alex Library for documentation

Directions for Use, “Alarms and Events (PXM)”

User Instructions about E1/T1, SS7 Alarms.

User Instructions about Ethernet link.

DISCUSSION

The GUI provides all Discussion to do the exercises.

Questions in the student text for Discussion

Look in the active alarms list, which alarms have been raised recently about link failure. Ask your instructor which alarm should be solved by your group

pcmE1T1LossofSignal – IBTE/IBS7 PIU used for Gb / NB Gr interface

atmLossofSignal- ATM PIUs used for Iu-C and BB Gr interfaces

ethLinkDown- ETH PIU used for Gn interface

Figure out what the problem is (look in the user instruction) and find out, how the problem can be solved.

Interface $ PCM port P$ has lost receive signal.- This alarm is generated when the E1/T1 interface does not receive any signal. (255 consecutive zeros received.) This could indicate a cable problem or remote peer down.

The SDH/Sonet interface $ has lost receive signal - This alarm is generated when the SDH/Sonet interface doesn't receive any signal. This could indicate a cable problem or remote peer is down.

Ethernet port *magazine*.*slot*.2.1:*port* $ has lost link.- This alarm is generated when the Ethernet port does not receive any signal from the carrier. This could indicate remote peer down or a cable problem.

Solve the problem.

Actions to Be Taken - Perform visual check of interface cable and check remote peer configuration.

Further Questions for Discussion during Conclusion

-

CLI Commands

list_alarms

Exercise 3 Definition of a new role

OBJECTIVES

Upon completion of this exercise the student will be able to:

- Describe the Role Based Access Control (RBAC) which is used on the SGSN-MME
- Use the CPI documentation to find instructions on how to implement a new role
- Define a new role on the SGSN-MME

DESCRIPTION

The exercise will lead step by step into the process of integrating a new role in a SGSN-MME. All documents including the student text and customer product information (CPI) are used to find out about and implement a new role.

BACKGROUND

It is important to security management to understand and handle roles in the SGSN-MME systems. Though roles are relatively simple to create and modify, information and understanding about the action sets available is very important. Where to get this information and how to handle roles on SGSN-MME systems will be explained and practised during this case.

RESOURCES

During the case you may have use of the following resources:

[1] ALEX documentation on SGSN-MME 2010B on e.g. http://cpi.al.sw.ericsson.se/alexserv or available on the Network Element

[2] Student Text

EVENT DEFINITION OF A NEW ROLE

During this event, you will create a new role for a specialized type of access to the SGSN-MME. The role defines the rights – called action sets – a user has to configure and access information using either PXM or CLI commands.

Your boss wants you to integrate a new role for the OSS integration staff. The users need access to some but not all areas of GSN configuration. Please read on before you start creating roles.

First review resource [2] and identify the action set always to include:

oms_sm_user_admin_passive

If you forget to add this action set to your role, what is the consequence for all users connected to this role?

They can't change their own passwords.

Your Boss specified the rights that an OSS user has to work with the node. They are defined in list 1.

List 1: Rights for OSS users to have

- View the IMSI Number Series
- View the EPL IMSI Number Series
- View the NRR IMSI Number Series
- View the PLMN Identification
- View the Equivalent PLMN List
- View the EPL Location Areas
- View the NRR Location Areas

- View and Configure the Event Recording
- View and Set functions in the Alarms and Events PXM form
- View the Local SGSN-MME attributes
- View and Configure the Domain Name System
- View IP configurations using the GPRS CM application
- View information about software configuration
- View and set-up the Measurement Jobs with PXM in the Measurement Types and Measurement Jobs PXM forms or with the corresponding CLI commands

Use the resources [1] and [2] to map the requirements into corresponding action sets. Fill in all action sets you are planning to add to your new role:

- **nwc_coop_routing_area_passive**
- **nwc_epl_imsins_passive**
- **nwc_nrr_imsins_passive**
- **nwc_hplmn_passive**
- **nwc_epl_plmn_passive**
- **nwc_epl_lai_passive**
- **nwc_nrr_lai_passive**
- **ncs_EventRec_passive**
- **ncs_EventRec_active**
- **oms_fm_admin_passive**
- **oms_fm_admin_active**

- **nwc_local_sgsn_passive**
- **vlr_imsins_analysis_passive**
- **dns_slo_passive For view the configuration with dns sortlist CLI**
- **dns_slo_active For configuration of attributes with dns sortlist CLI**
- **ip_passive For viewing IP configuration including DNS**
- **ip_active For modifying IP configuration including DNS**
- **ip_proxy_passive**
- **swcm_slo_passive**
- **oms_pm_passive**
- **oms_pm_active**
- **oms_sm_user_admin_passive**

Now implement your new role on the network element. Use CLI to create the new role. Use a unique name like OSSstaff<#> where <#> is your group number. List the document that describes how to create a new role using CLI:

User Administration (CLI)
112/190 80-CRA 250 56/1 Uen F

Create a new role with CLI commands and note it here including mandatory options.

add_sm_role -role role [-a actions...]
add_sm_action -role Role -a Action...

Exercise 4 Definition of a new user

OBJECTIVES

Upon completion of this Exercise the student will be able to:

- Describe the Role Based Access Control (RBAC) which is used on the GSN
- Use the CPI documentation to find instructions on how to implement a new user
- Define a new user on the SGSN-MME
- Assign groups to the new user

DESCRIPTION

During this case the student will learn and practise how users are created, what administrative information and actions are connected to user management and the default settings used for newly created users on a SGSN-MME.

BACKGROUND

During a node's lifetime, there are plenty of changes regarding the users. New users have to be created in order to permit access for new employees. Also if new services are implemented they might use dedicated accounts for access. So, after a while lots of old accounts are on the system need to be removed again.

The node shall be managed as few as possible using the system administrator account. The default om_admin account should be used only to create other user accounts with different roles related for instance to software updates, patching or configuration management.

RESOURCES

[1] ALEX documentation on SGSN-MME 2010B on e.g. http://cpi.al.sw.ericsson.se/alexserv or available on the Network Element

[2] Student Text

EVENT DEFINITION OF A NEW USER

Which types of user can be defined on the SGSN-MME?

A PXM user created using CLI commands or PXM
A Unix User created only in the Unix OS of the GSN

Explain the difference between these two user types

A PXM user can change parameters and configuration
according to his role in PXM and by CLI commands.
A Unix user exists only in the OS environment but not on
GSN layer. A Unix user has no configuration access on the
node.

Which types of group can be supported on the SGSN-MME?

charging group
security group
gsnuser grup

Explain the difference between these three groups

Charging group allows read and write access to the charging

files.
Security group allows read and write access to the user administration files.
Gsnuser grup allows read and write access to all files, except for the charging and user administration files.

Create a PXM user (use om_admin account). Ask the instructor to login as om_admin for you. Once logged in, assign to the user the role you defined in the case before. Name your user uniquely like "Oper<#>" where <#> is your group number.

Logout and login again a second time with the user account you created. Try to open the Node Properties. What happens?

The user's role has no view permission on node properties.
The request to open node properties is rejected.

Add the action sets for the Node Properties to the role of user you created before. Try to open the Node Properties a second time. What happens this time?

Access is possible.

What is the home directory of the user you created before? Use the Unix configuration files to find this information.

All users' home directories are located in /Core/home/.
This information is found in /etc/passwd file.

What is the default group assigned to the user you created before? Can you read the Unix configuration files?

gsnuser group

No, because you are gsnuser group and can not read /etc/group

Which group has to be added for the user again? Can you read the Unix configuration files?

security group
Yes.

Go to the home directory of the user you created before and check which files were automatically created by Security Management.

Three files are created by default, they are used to initialize
the user's shell.

Delete your PXM user and check the Unix configuration files once again.

The entire home directory is removed.

Delete the role you defined before. You are finished with the Security Management cases. Please stop further processing now and inform the instructor.

Exercise 5 Log Management

OBJECTIVES

Upon completion of this exercise the student will be able to:

- Describe the different available logs and the default log parameters
- Retrieve data from the logs

DESCRIPTION

During this case the student will make him/her-self familiar to the log management functions of a SGSN-MME node. He/She will configure log parameters, lookup parameters of predefined log files and retrieve data from logs using different methods.

BACKGROUND

The SGSN-MME system provides different build in logs containing valuable information to supporters and trouble-shooters. When the system is operational, the logs start growing and need sooner or later administration. Also it is important to understand the implementation of logging on SGSN-MME systems; which information can be retrieved in what log and how can logging be influenced in case it is needed.

RESOURCES

[1] ALEX documentation on SGSN-MME 2010B on e.g. http://cpi.al.sw.ericsson.se/alexserv or available on the Network Element

[2] Student Text

EVENT LOG MANAGEMENT

Name the SGSN-MME built-in Logs and their purpose. Please specify which one is different in SGSN-MME 2010B.

Note: The logs are described in document: Operation and Maintenance Description 66/1551-AXB 250 05 Uen T
ADC log Data is stored in the Automatic Device Configuration (ADC) log each time an unknown Home Public Land Mobile Network (HPLMN) subscriber attaches the GSN, or the International Mobile Station Equipment Identity Software Version (IMEISV) is modified for a known HPLMN subscriber, or an Access Point Name (APN) in Home Location Register (HLR) data is new or modified for a known HPLMN subscriber.
AdmissionControlUsage log Events related to features and capacity licenses, such as changed feature or capacity licenses, exceeded licensed capacities, invalid license-key files, or emergency unlocks, are stored in the AdmissionControlUsage log. (different in SGSN-MME 2010B)
au_data_log Failed MS authentications are stored in au_data_log. Failed MS authentication procedure can be caused due to, for example, SRES failure, MAC failure or synchronization failure. The GSN is able to store the au_data_log for a minimum of 72 hours. Only users belonging to the security group can access this log.
chsLog In postpaid charging, the CDRs are collected in chsLog. Only users belonging to the charging group can access this log.
chsGtpPrimLog In near-real-time charging, the CDRs are grouped into GTP' PDUs. If the connection for transfer of GTP' PDUs to the external billing systems fail or the billing systems do not

respond, the CDRs are after a while stored in chsGtpPrimLog. Only users belonging to the charging group can access this log.
ebs The events collected by the Event-Based Statistics (EBS-S) for OSS-RC feature are stored in the ebs. EBS-S logs successful and unsuccessful events, formatted according to logging criteria.
er_data_log Traffic events are stored in. Traffic event recording is a tool for finding problems in the network and is used for tracking subscribers who complain about problems with their GPRS service.
fm_alarm All occurred alarms and alarm clearings are listed in the fm_alarm log.
fm_event All occurred events are stored in the fm_event log.
Gf_IMEIcheck_log All IMEI_CHECK failures are stored in the Gf_IMEIcheck_log.
Gs_interface_log Mobile status messages sent over the Gs interface, for indicating errors, are stored in the Gs_interface_log.
list_subscribers_result Subscribers registered in the GSN can be listed with the list_subscribers CLI command and are stored in the list_subscribers_result log.
mmi_log All activities on the machine-to-machine interface are stored in the mmi_log.

mobility_event_log All Attach Reject messages due to network failure are stored in the mobility_event_log.
OMS_SM_Log Each action performed by the operator is stored in the OMS_SM_Log. Only users belonging to the security group can access this log.
Performance monitoring logs The measurement data collected by a measurement job is stored in a log, whose name is identical to the name of the measurement job. A maximum of 50 performance monitoring logs can exist at the same time.
session_event_log All MS-initiated Activate PDP Context rejects due to network failure, missing or unknown APN, unknown PDP address, or requested service option not subscribed are stored in session_event_log.

Which CLI command gives all available logs?

list_logs

What is the default path for log files on SGSN-MMEs?

/tmp/OMS_LOGS/
/tmp/OMS_CHARGING

What is the maximum size configured for charging log (chsLog)? How did you find this information?

The value is based on specified SGSN-MME node.

get_log_config chsLog

Download the most recent OMS_SM_Log to your local machine using FTP and use a text viewer to look into the file. How can you find the most recent file? When was your last login? And is it possible to trace back your work in PXM?

Most recent file can be found using the Unix "ls –rtl" command.

Simply the file in the last row is the most recent.

Login and every PXM form opened are logged into this file.

Dive into the location of the logs using the Unix environment. Try to search the most recent alarm log for alarm clearings using Unix tools. Note down the command to use:

grep "clearAlarm" fm_alarm.x | more

Which other useful possibilities you know to process the file using Unix commands?

This can be quite a lot – here are just a few examples:

"sort" can be used to sort the output into any order

"egrep" can be used to search for more complex strings

"nawk" or "awk" can be used to process/reformat changes

Your have finished with the Log Management Case. Please stop further processing and inform the instructor that you have finished.

Exercise 6 GSN Support Application

OBJECTIVES

Upon completion of this exercise the student will be able to:

- Verify that the GSN Support System server and the SGSN-MME are connected
- Create backups of a SGSN-MME system
- Replace a standalone FSB board
- Administrate backups on GSS server

DESCRIPTION

During this case the student will make him/her-self familiar to the GSN Support Application. The student will access to the GSA interface, verify the connection between GSS and SGSN-MME, create an entire system backup and will use a backup to restore one FSB board in SGSN-MME with MkV/VI/VI+ HW. During this procedure the student will learn about the FSB replacement procedure, and handling the GSS server.

BACKGROUND

SGSN-MME boards have a limited live time. As rotating disks are installed in both FSB boards they are subject of disc failures as well as memory or processor faults. In general if no backup is taken from the node, especially when the two FSB boards fail, it will get hard to replace the boards. So having a secure backup of your SGSN-MME is most important for low down times.

As the administrator usually takes care about backup jobs he/she must know the backup and restore procedures.

RESOURCES

[1] ALEX documentation on SGSN-MME 2010B on e.g. http://cpi.al.sw.ericsson.se/alexserv or available on the Network Element

[2] Student Text

[3] Back Up and Restore an SGSN-MME

[4] Replacing a Standalone FSB

EVENT 1 PREPARING THE SGSN-MME FOR BACKUP

The GSS server is built up for initial installation and upgrade of SGSN-MME, also for backup and restore SGSN-MME. And it is possible to serve multiple SGSN-MMEs in parallel. The GSS server does not install any Ericsson SW or HW but store the SW for backup. All logics are in the GSA on SGSN-MME. Different directories in GSS server distinguish the nodes with node name. Use the student text to review the function and implementation of the GSS server.

Make yourself familiar with the GSS by going through the directories below /gsn and identifying the meanings. To do so connect to the GSS server using telnet or ssh. The instructor will tell you all necessary connection parameters.

Note down the most important directories on the GSS server for you:

/gsn/nodes/<nodename> is root path for each SGSN-MME connected to the GSS server.

/gsn/nodes/<nodename>/backups stores backup files for the corresponding SGSN-MME.

/gsn/sw is for the software deliverables.

If logon an SGSN-MME node with Mk IV HW as a root user, how to start GSA on the SGSN-MME node?

Logon as a root to the active NCB via PEB, Gom Board or

Console port of NCB, then start ‘gsa’

If logon an SGSN-MME node with Mk V/VI HW as a root user, how to start GSA on the SGSN-MME node?

Logon as a root to the primary FSB via Console port of FSB, then start ‘gsa’; or to the active NCB via PEB, Gom Board or Console port of NCB, then start ‘gsa’.

Which GSA command checks and verifies that GSS server and the SGSN-MME are connected? How to decide the connection is ok?

info

The IP address, node path and backup directory of the GSS server indicates that the GSS server and the SGSN-MME are connected.

The Dynamic Host Configuration Protocol (DHCP) server needs to be running on the GSS server in order for the SGSN-MME to be able to access the GSS server file system.

On a GSS server with Solaris 10 installed, how to check that the DHCP server on the GSS server is active? In case of the disabled DHCP server, how to start the DHCP server?

svcs network/dhcp-server:default

If the DHCP server is active, the printout should be similar to the following:

STATE STIME FMRI

online Oct_12 svc:/network/dhcp-server:default

If the DHCP server is disabled, the printout should be similar to the following:

STATE STIME FMRI

disabled 14:31:30 svc:/network/dhcp-server:default

/usr/sbin/svcadm enable network/dhcp-server:default

On a GSS server with SUSE Linux Enterprise Server 10 installed, how to check that the DHCP server on the GSS server is active? In case of the disabled DHCP server, how to start the DHCP server?

ps -ef|grep dhcp

/etc/init.d/dhcpd restart

Is there a GSA command for showing all available backups, too? If so note down the full command:

list

Now note down the GSA command to backup and periodically backup the SGSN-MME.

backup [-t tag-name]

periodic_backup <periodic-backup-start-time> [-r <hours>]

[-t <tag-name>] [-l] [-k <job-id>]

-r option can be included to repeat a backup after a specified number of hours

-t option can be included if a tag is to be used as an identifier

-l option is included to list defined background jobs

-k option is included to close a defined periodic backup job

Fetch the OPI document telling how to create a backup. It is found as reference [3]. Study how to create a backup. Then start the procedure. The node root path is already created for you. Please further note that there was no initial installation or restore of the SGSN-MME recently.

You find the tag name to use for the backup in the table below. Ask the instructor for the node name to use.

Group #	Tag name
Group1	Group1BK
Group2	Group2BK

Run all further necessary steps in the OPI to take a backup. During the backup check the file in directory /gsn/nodes/<nodename>/backups/

BACKUP_IN_PROGRESS, which means the backup procedure is ongoing.

./<backup name>/BACKUP_COMPLETE which will be generated when the backup is done.

When you have finished, it’s time for having a coffee break, and inform the instructor that you have finished, please.

EVENT 2 VERIFYING THE BACKUP

After creating a backup it's important to know if the backup taken is really healthy. One possible solution to this question is to restore the backup on the node again. Of course this kind of testing would be both – time consuming and dangerous in case the backup taken was unhealthy for some reason.

The second best solution is to use the GSA to verify the consistency of the backup files. Existence of backup files is checked together with the size of each file. The GSA command "verify" provides the function. An incomplete backup or a backup where files are missing, or are of faulty size, is regarded as corrupt and the backup should be removed and redone.

Execute the verification of your backup.