Oracle® Communications Diameter Signaling Router

Virtual Signaling Transfer Point

Release 8.4
F12308-01
July 2020

ORACLE

Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point, Release 8.4

F12308-01

Contents

List of Figures

List of Tables

1
Introduction

This chapter describes how to obtain help, where to find related documentation, and provides other general information.

1.1 Revision History

The document has been updated for the following features:

- **vSTP AINPQ/INPQ Feature**

1.2 Locate Product Release Software on the Oracle Software Delivery Cloud Site

Oracle Communications software is available for electronic download at the Oracle Software Delivery Cloud site, https://edelivery.oracle.com. Only authorized customers with a valid password may download software from the site.

For directions on downloading the software and other information about using this site, click **FAQ** in the top right corner.

1.3 My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

2
Overview of vSTP

This chapter provides a high level description of the features associated with vSTP.

2.1 vSTP Introduction

The Virtual Signaling Transfer Point (vSTP) application uses signaling experience from both the Oracle Communication EAGLE STP and the vDSR products to build a common signaling platform for unified signaling solutions. The application is installed on virtual machines.

2.2 M3UA Protocol

M3UA seamlessly transports SS7 MTP3 user part signaling messages over IP using SCTP. M3UA-connected IP endpoints do not have to conform to standard SS7 topology, because each M3UA association does not require an SS7 link. Each M3UA-connected IP endpoint can be addressed by an SS7 point code unique from the signaling gateway's point code. vSTP provides M3UA without routing keys.

M3UA does not have a 272-octet Signaling Information Field (SIF) length limit as specified by some SS7 MTP3 variants. Larger information blocks can be accommodated directly by M3UA/SCTP without the need for an upper layer segmentation or re-assembly procedure, as specified by the SCCP and ISUP standards. However, a Signaling Gateway will enforce the maximum 272-octet limit when connected to a SS7 network that does not support the transfer of larger information blocks to the destination.

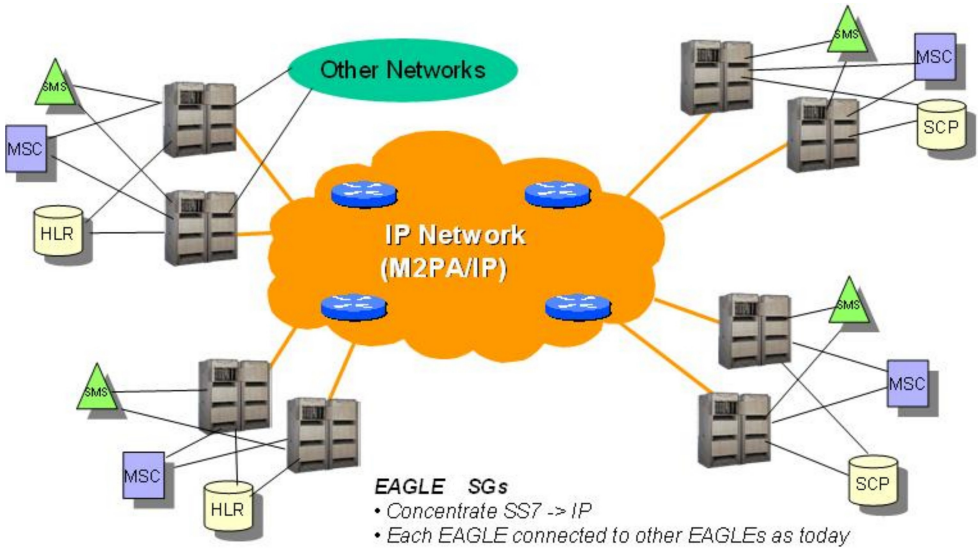
At the Signaling Gateway, M3UA indicates to remote MTP3 users at IP end points when an SS7 signaling point is reachable or unreachable, or when SS7 network congestion or restrictions occur.

2.3 M2PA Protocol

M2PA is used primarily to replace B-, C-, and D-links. When used with A-links, M2PA connects to Service Switching Points, Signaling Control Points, Home Locater Registers and other endpoints. M2PA is a direct replacement for channelized TDM circuits because it provides specific controls for assurance of in-sequence delivery of messages. As such, M2PA is used to connect points that pass call-related data that is time-sensitive, such as ISUP calling data.

Congestion procedures conform to those specified by the ANSI/ITU standards.

Figure 2-1 M2PA Network



2.4 Global Title Translation

The Global Title Translation (GTT) feature is designed for the Signaling Connection Control Part (SCCP) of the SS7 protocol.

The GTT feature uses Global Title Address (GTA) information to determine the destination of the MSU. The Translation Type (TT) indicates which GTT table is used to determine the routing to a particular service database. Each GTT table includes the Point Code (PC) of the node containing the service database, the SubSystem Number (SSN) identifying the service database on that node, and a Routing Indicator (RI). The RI determines if further GTTs are required. GTA and TT are contained in the Called Party Address (CdPA) field of the MSU.

The GTT feature changes the destination PC and the origination PC in the routing label. The GTA information is not altered.

Depending on how the GTT data is configured, the GTT may also change the RI, SSN, or the TT in the CdPA. The gray shaded areas in the following tables show the message fields affected by GTT.

Figure 2-2 ANSI MSU (ANSI Message Signal Unit)

BSN FSN LI	SIO	SIF		
		Routing Label		
	xx xx xxxx NIC PRI SI	DPC OPC SLS NCM NC NI NCM NC NI xx	CGPA Length Address Indicator (x x xxxx x x) Subsystem Point Code (NCM NC NI)	CDPA Length Address Indicator (x RI xxxx xx) Subsystem Point Code (NCM NC NI) Address (Translation Type) (Digits)

Figure 2-3 ITU-I MSU (ITU International Message Signal Unit)

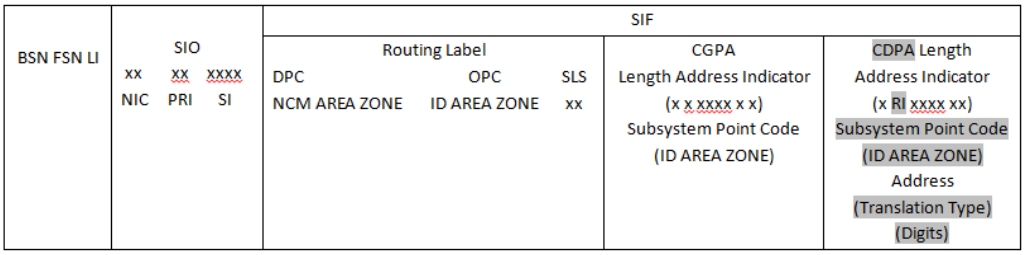


Figure 2-4 14-Bit ITU-N MSU (14-Bit ITU National Message Signal Unit)

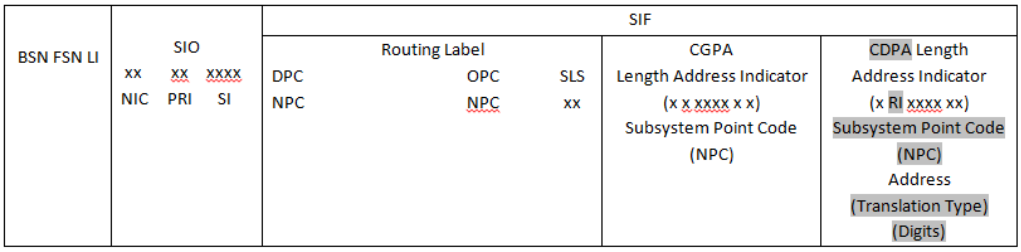
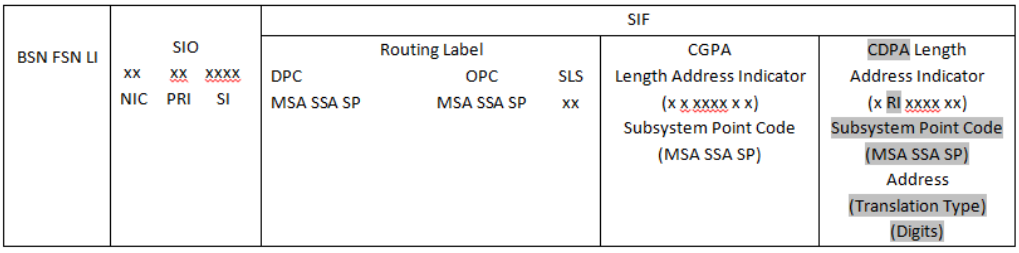


Figure 2-5 24-Bit ITU-N MSU (24-Bit ITU National Message Signal Unit)



2.4.1 GTT Routing

The routing options described in this section allow you to add translations to parameters, code, and components for additional flexibility in routing a message.

TCAP Opcode Based Routing (TOBR)

TOBR provides vSTP with the ability to route messages based on its operation codes. With the TOBR feature, vSTP considers the following information contained in TCAP portion of messages for performing GTT.

- ITU Messages
  - Message/Package type
  - Application context name
  - Operation code
- ANSI Messages

  - Package type
  - Operation code family
  - Operation code specifier
- Message Type support by TOBR for ITU and ANSI
- ITU TCAP
  - Begin
  - Continue
  - End
  - Abort
  - Unidirectional
- ANSI TCAP
  - Unidirectional
  - QueryWithPermission
  - QueryWithoutPermission
  - Response
  - ConversationWithPermission
  - ConversationWithoutPermission
  - Abort

TOBR works based on the following rules:

- If the message/package type is NOT one of those mentioned, vSTP treats it as an unknown message type and does not proceed with the decoding.
- vSTP attempts to decode the TCAP portion of all UDT/UDTS/Unsegmented XUDT/Unsegmented XUDTS queries coming to the SCCP layer for GTT.
- If decoding fails, the message still undergoes GTT using some default values for the TCAP data that denote their absence in the message.
- ACN is used for all supported ITU TCAP messages except ABORT. No attempt to retrieve ACN is made for Abort messages. All other supported messages may have a Dialog portion containing Dialogue Request/Unidirectional Dialogue/ Dialogue Response PDU, from which the ACN is retrieved. If no Dialog portion is detected, then ACN is assumed to be NONE.
- TOBR attempts to find the Operation Code (Opcode) in all supported ITU TCAP messages except ABORT. These messages must contain Invoke or Return Result (Last or Not Last) as the first component. If not, Opcode is assumed to be NONE.
- TOBR attempts to find the Operation Family and Specifier in all supported ANSI TCAP messages (except ABORT) containing an INVOKE component. For all other messages, Family and Opcode are assumed to be NONE.

Flexible Linkset Optional Based Routing (FLOBR)

FLOBR supports Linkset based routing and Flexible routing.

- Linkset based routing routes GTT traffic based on the incoming linkset

- Flexible routing routes GTT traffic based on parameters such as MTP, SCCP, and TCAP in a flexible order on a per translation basis

With the FLOBR feature, you can change the default CdPA GTTSET to point to any GTT set type and find the translation.

FLOBR works based on the following rules:

1. When GTT mode is FLOBR CDPA, CDPA fields in the MSU are used for GTT selector search and the GTT set is taken from the CDPA GTT SET Name configured in the selector entry.
2. When GTT mode is FLOBR CGPA, CGPA fields in the MSU are used for GTT selector search and the GTT set is taken from the CGPA GTT SET Name configured in the selector entry.
3. When GTT hierarchy is FLOBR CDPA and FLOBR CGPA, GTT selectors are searched as defined in 1. If no selector match is found or CDPA GTTSET is not provisioned, GTT selectors are searched as defined in 2.
4. When GTT hierarchy is FLOBR CGPA and FLOBR CDPA, GTT selectors are searched as defined in 2. If no selector match is found or CGPA GTTSET is not provisioned, GTT selectors are searched as defined in 1.
5. If GTT selectors are not found as specified in 1, 2, 3 or 4, then vSTP considers this a translation failure.
6. You can provision a fallback option for each translation in FLOBR to tell it how to route an MSU under the following conditions:
    - Routing when a search fails
    - Routing when the same GTT set name is referred to more than once
    - Limiting the number of database searches to seven (7)
7. When a fallback option is set to No, the GTT fails and the MSU is discarded.
8. When a fallback option is set to Yes, the GTT performs based on the last matched entry.

MAP Based Routing (MBR)

MBR provides vSTP with the ability to route messages based on its MAP components. This can be done by using either IMSI or MSISDN GTT set types, which are linked by OPCODE set type.

MBR works based on the following rules:

- TCAP package types BEGIN, CONTINUE, and END are supported for MAP based routing, so OPTSN with one of the MAP GTT set types are allowed to be provisioned for TOBR GTA entries that have "pkgtype" as BGN, CNT, or END.
- When an MSU is processed by the TOBR GTT translation with the OPTSN as one of these new set types, Eagle decodes the TCAP part and extracts the required TCAP parameter from the MSU. The digits in this parameter are used as the key to search for the translation in the GTT set.
- If Dialogue Portion is present in the message, pick the last byte of the ACN.

> **Note:**
>
> MBR does not validate if the MAP operation is supported with the ACN in the message; it is only decoding the last byte of the ACN to determine the MAP version.

- If Dialogue Portion is not present, the MAP version provisioned with the Opcode translation is used as the MAP version.

2.4.2 GTT Action Feature

The Global Title Translation (GTT) action feature performs additional actions on the incoming/translated Message Signaling Unit (MSU) coming from the GTT. Configure GTT Action, GTT Action Set, and GTA Managed Object (MO) to use these as optional features.

vSTP supports the following types of GTT actions:

- Discard
- UDTS
- TCAP Error
- Forward
- Duplicate
- SFTHROT
- SCPVAL

Discard

The Discard GTT action discards incoming MSU.

UDTS

The Unit Data Service (UDTS) GTT action marks the MSU as discarded and an error response is sent back with an udts error code.

TCAP Error

The Transaction Capabilities Application Part (TCAP) Error GTT action marks the MSU as discarded and an error response is sent back with an tcap error code.

Forward

The Forward GTT action forwards the incoming/translated MSU to a specified point code per configuration. The MSU does not forward to translated point code.

If the Forward GTT action fails, then default actions are performed per configuration:

- Fallback means forward the MSU to translated point code
- Discard an incoming MSU
- Send a UDTS response with an udts error code per configuration
- Send a TCAP error response with an tcap error code per configuration

Duplicate

The Duplicate action sends a copy of incoming/translated MSU to a specified point code per configuration. The MSU does sent to translated as well as duplicate point code.

SFTHROT

The GTT Throttle action is part of SS7 security firewall. It provides support for Egress throttling of GTT messages in vSTP. For more details, see GTT Throttle Action.

SCPVAL

The SCPVAL GTT action along with relevant parameters performs the validation on MAP parameters by comparing the SCCP and MAP digits. For more details see, GTT SCPVAL Action.

2.4.2.1 GTT Throttle Action

The GTT Throttle (SFTHROT) is a GTT Action that performs the Egress throttling of GTT messages in vSTP. This action is part of SS7 security firewall.

This functionality can be achieved by enabling the SFTHROT action.

2.4.2.1.1 Workflow for GTT Throttle Action

The GTT Throttle action works based on the following rules:

1. When an MSU hits a GTT action of the type SFTHROT, the MSU count of that action gets updated.

   > **Note:**
   >
   > The Shared Metric Service (SMS) framework is used to accumulate the total number of MSU count per SFTHROT action.

2. The MSU count is updated only on the Message Processor (MP) on which the message is received for that action. On the other hand, the Threshold configuration for SFTHROT action is across the MPs.

   > **Note:**
   >
   > For each GTT Action, user provisions a threshold value that is the maximum number of MSUs hitting the GTT action per second.

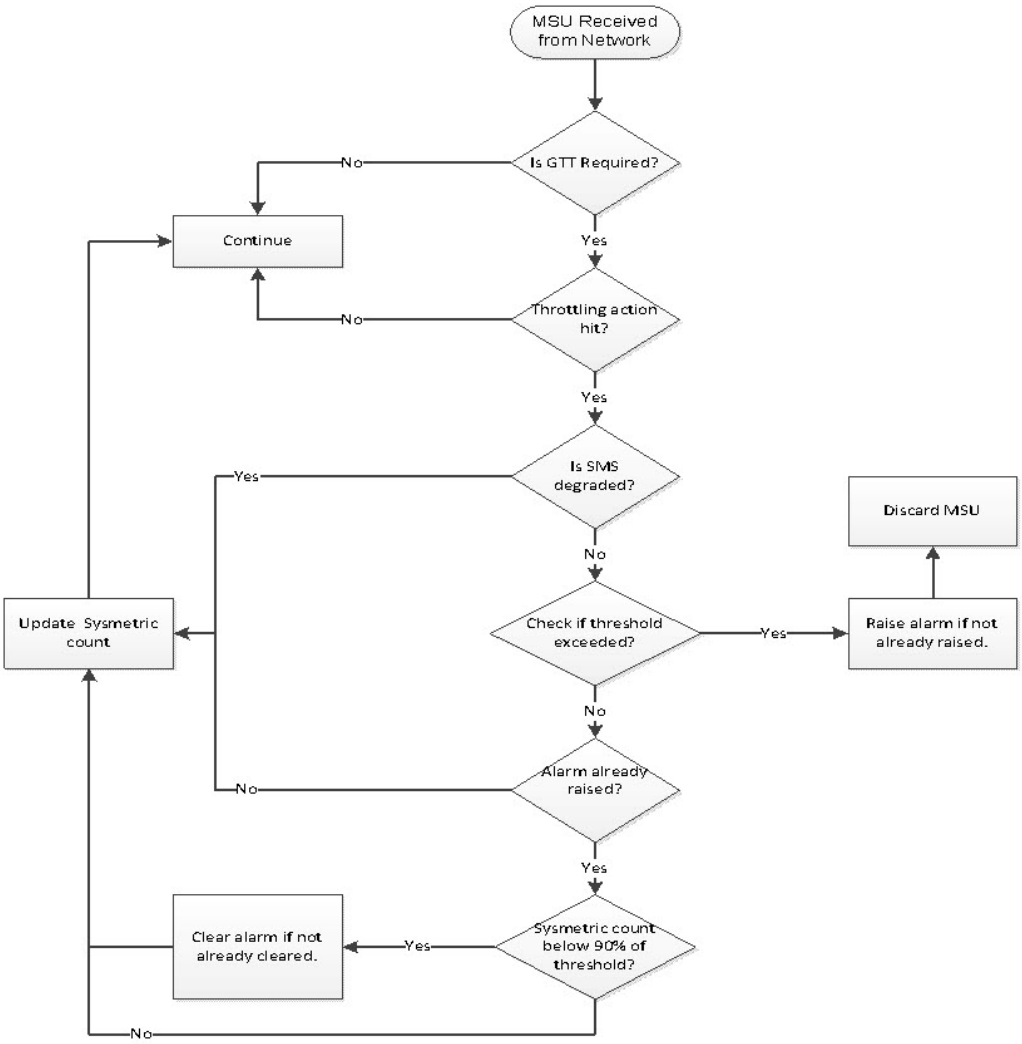
3. Two sysmetrics are registered. The first is for MSU count per MP and second one for cumulative MSU count across the site.
4. Aggregation of the MSU count from all the MPs is done by the MP Leader. There is only one MP leader across the site. It performs the aggregation of MSU counts. Rest of the MPs across the site are known as followers.

5. Whenever a message comes to any MP, it will increment the sysmetric count of that MP known as local sysmetric count. All the follower MPs will send the local sysmetric count data to the MP Leader to get the aggregated value of that action.
6. The MP Leader will receive the data from all the other MPs including it's own local sysmetric count. It will do the aggregation and broadcast the cumulative count to all the MPs.
7. The SMS framework is used to send local sysmetric count to MP leader and receive the aggregated sysmetric count from it. The aggregation of the count is taken care by SMS framework hence, any degradation in SMS service will impact the feature.
8. When GTT message is received for SFTHROT action, then the aggregated sysmetric count is compared with the configured threshold value for that action:
    - If the aggregated sysmetric count value is lesser than the configured threshold value, then the message is allowed and the local sysmetric count value is increased by 1.
    - If the aggregated sysmetric count value is more than the configured threshold value, then the local sysmetric count value does not get increased due to throttling. The GTT message is discarded, discard measurement is pegged for that action, and an alarm is raised.
        a. The alarm will get cleared once the aggregated sysmetric count drops below 90% of the configured threshold value.
        b. As there is no local sysmetric is pegged, the aggregated count will be decreased in next sliding window. Convergence time is 2 sec.
        c. Once the cumulative value drops below the configured threshold, it will allow the GTT messages for that action and the local sysmetric count will be increased.

> **Note:**
>
> For GTT Throttle action, an error margin of +2% to -2% of the provisioned threshold value must be considered. The error margin depends on the cloud infrastructure load & burst pattern of incoming traffic.

The following figure shows the process flow for GTT Throttle action:

Figure 2-6 Process Flow of GTT Throttle Action



2.4.2.1.2 MMI Managed Objects for GTT Throttle Action

MMI information associated with GTT Throttle action is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for GTT Throttle action.

Table 2-1 vSTP SFTHROT Managed Objects and Supported Operations

Managed Object Name	Supported Operations
gttactions	Insert, Update, Delete
gttactionsets	Insert, Update, Delete

gttactions - Insert, Update, Delete

Create a file with the following content:

```
$ cat gttaction.txt
{
            "act": "Sfthrot",
            "actid": "throttle1",
            "defactid": "fallback",
            "threshold": 5
        }
```

> **Note:**
>
> **Threshold** is mandatory for SFTHROT action type. Range is **1** to **4294967295**. Modification is allowed for threshold.

Execute the following command on an active SOAM to insert:

```
 /vstp/gttactions -v POST -r /<Absolute path>/<Fiename>
```

Example output:

```
 /vstp/gttactions -v POST -r gttaction.txt
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute the following command on an active SOAM to update:

```
 /vstp/gttactions -v PUT -r /<Absolute path>/<Fiename>
```

Example output:

```
 /vstp/gttactions -v PUT -r gttaction.txt
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/gttactions/<actid> -v DELETE
```

Example output:

```
 /vstp/gttactions/throttle1 -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.1/vstp/
gttactions/throttle1? for 'DELETE' operation
```

Execute the following command to display:

```
 /vstp/gttactions
```

Example output:

```
 /vstp/gttactions
       {
          "data": [
              {
                  "act": " Sfthrot",
                  "actid": "throttle1",
                  "defactid": "fallback",
                  "threshold": 5
              }
          ],
          "links": {},
          "messages": [],
          "status": true
      }
```

gttactionsets - Insert, Update, Delete

Create a file with the following content:

```
{
    "actsn": "actset1",
    "actid1": "Act1“
}
```

Note:

- At max 1 SFTHROT action is allowed to be provisioned per VstpGTTActionSet entry.
- While provisioning Action Id, ensure it is provsioned in VstpGTTAction Table.

Execute the following command on an active SOAM to insert:

```
 /vstp/gttactionsets -v POST -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactionsets -v POST -r /tmp/ActSet1
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
```

Execute the following command on an active SOAM to update:

```
 /vstp/gttactionsets -v PUT -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactionsets -v PUT -r /tmp/actset1
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/gttactionsets/<Set Name> -v DELETE
```

Example output:

```
 /vstp/gttactionsets/Set1 -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.0/vstp/
gttactionsets/Set1? for 'DELETE' operation
```

Execute the following command to display:

```
 /vstp/gttactionsets
```

Example output:

```
  /vstp/gttactionsets
{
 "data": [
{
    "actsn": "actset1",
    "actid1": "Act1“
}
],
"links": {},
    "messages": [],
    "status": true
}
```

2.4.2.1.3 GTT Throttle Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to GTT Throttle action:

Alarm/ Event ID	Name
70418	Sccp Egress Tps Threshold Crossed

For more details related to Alarms and Events, refer to Alarms and KPIs Reference document.

Measurements

The following table lists the measurements specific to GTT Throttle action:

Measurement ID	Measurement Name
21721	VstpThrottleActionMsgRatePeak
21722	VstpThrottleActionMsgRateAvg
21723	VstpThrottleActionMsgDiscard

For more details related to measurements, refer to Measurement Reference document.

2.4.2.1.4 Dependencies

The GTT Throttle action support for vSTP has no dependency on any other vSTP operation.

2.4.2.1.5 Troubleshooting

In case of error scenario, check the incoming traffic. The incoming traffic must be 100% or above the provisioned threshold value for respective actid with SFTHROT action.

2.4.2.2 GTT SCPVAL Action

The SCCP MAP Validation (SCPVAL) is a GTT Action that performs validation check on the of vSTP map parameters. This action is part of SS7 security firewall.

For example, in vSTP few of the map parameters must be same as either SCCP CdPA or CgPA. The GTT SCPVAL action do this validation check with a comparison between SCCP parameters and the map digits.

> **Note:**
>
> The SCPVAL action is applicable only for the following messages coming to the vSTP:
>
> - MO-FSM (MAP version 2 or 3)
> - MT-FSM (MAP version 3)

The SCPVAL action has the following set of parameters to execute the functionality:

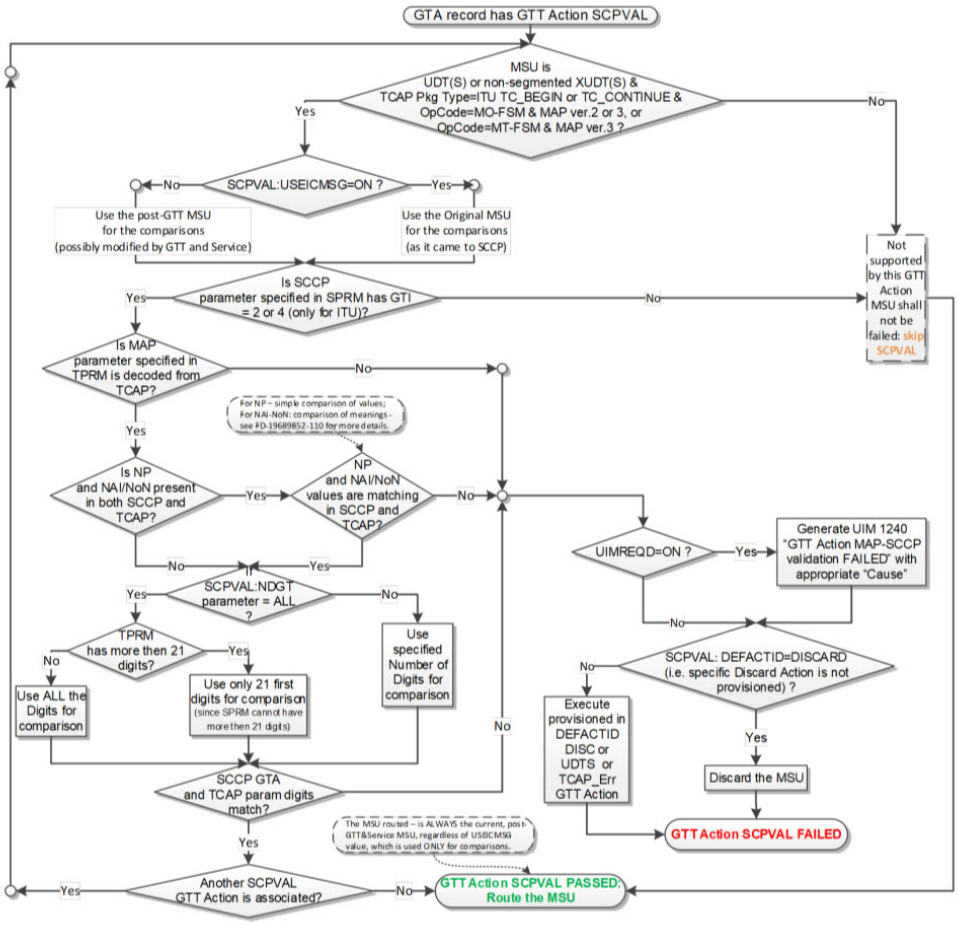
Parameter Name	Description	Value
SPRM	Define the SCCP parameter value. It is a mandatory parameter.	The value can be either of the following: • CGGTA • CDGTA
TPRM	Define the TCAP parameter value. It is a mandatory parameter.	The value can be either of the following: • SMRPOA • SMRPDA
NDGT	Specifies the number of digits that needs to be matched between SCCP parameter and MAP parameter. This is an optional parameter.	Value: • Any digit between 1-21 • All Default value: All

Parameter Name	Description	Value
USEICMSG	Specifies whether to retrieve the data for comparison from the original message or from the post-GTT message.	The value can be either of the following: **OFF**: Use original message as received by the SCCP. **ON**: Use post-GTT message that is, after possible EPAP/GTT translation/modification data has been applied.
UIMREQD	Specifies if an event has be generated in case of GTT action failure.	The value can be either of the following: • **ON**: Event to be generated • **OFF**: No event to be generated
DEFACTID	Defines the default action that is performed when SCPVAL GTT action fails.	String value

2.4.2.2.1 Workflow for SCPVAL Action

The following flowchart describes the implementation of MAP SCCP validation:

Figure 2-7 SCCP MAP Validation Flowchart



2.4.2.2.2 MMI Managed Objects for SCPVAL

MMI information associated with SCPVAL action is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for SCPVAL action.

Table 2-2 vSTP SCPVAL Managed Objects and Supported Operations

Managed Object Name	Supported Operations
gttactions	Insert, Update, Delete
gttactionsets	Insert, Update, Delete

gttactions - Insert, Update, Delete

Create a file with the following content:

```
{
 "act": "Scpval",
 "actid": "Act1",
 "defactid": "fallback",
 "ndgt": "2",
 "sprm": "Cdgta",
 "tprm": "Smrpda",
 "uimreqd": "true"
 "useicmsg": "true"
}
```

Execute the following command on an active SOAM to insert:

```
 /vstp/gttactions -v POST -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactions -v POST -r /tmp/GttAct1
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
```

Execute the following command on an active SOAM to update:

```
 /vstp/gttactions -v PUT -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactions -v PUT -r /tmp/GttAct1
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/gttactions/<Rule Name> -v DELETE
```

Example output:

```
 /vstp/gttactions/Act1 -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.0/vstp/
gttactions/Act1? for 'DELETE' operation
```

Execute the following command to display:

```
 /vstp/gttactions
```

Example output:

```
  /vstp/gttactions
{
 "data": [
{
        "act": "Scpval",
        "actid": "Act1",
        "defactid": "fallback",
        "ndgt": "2",
        "sprm": "Cdgta",
        "tprm": "Smrpda",
                                "uimreqd": true,
        "useicmsg": true
}
                        ],
                    "links": {},
                    "messages": [],
                    "status": true
}
```

gttactionsets - Insert, Update, Delete

Create a file with the following content:

```
{
    "actsn": "actset1",
    "actid1": "Act1“
}
```

Execute the following command on an active SOAM to insert:

```
 /vstp/gttactionsets -v POST -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactionsets -v POST -r /tmp/ActSet1
{
 "data": true,
```

```
 "links": {},
 "messages": [],
 "status": true
}
```

Execute the following command on an active SOAM to update:

```
 /vstp/gttactionsets -v PUT -r /<Absolute path>/<File Name>
```

Example output:

```
 /vstp/gttactionsets -v PUT -r /tmp/actset1
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/gttactionsets/<Set Name> -v DELETE
```

Example output:

```
 /vstp/gttactionsets/Set1 -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.0/vstp/
gttactionsets/Set1? for 'DELETE' operation
```

Execute the following command to display:

```
 /vstp/gttactionsets
```

Example output:

```
  /vstp/gttactionsets
{
 "data": [
{
    "actsn": "actset1",
    "actid1": "Act1“
}
],
"links": {},
    "messages": [],
```

```
    "status": true
}
```

2.4.2.2.3 SCPVAL Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to SCPVAL:

Alarm/ Event ID	Name
70278	GTT Action Failed

For more details related to Alarms and Events, refer to Alarms and KPIs Reference document.

Measurements

The following table lists the measurements specific to SCPVAL:

Measurement ID	Measurement Name
21776	VstpCdpaGttActScpvalTotal
21777	VstpCdpaGttActScpvalDiscard
21778	VstpCdpaGttActScpvalNotApplied
21779	VstpCgpaGttActScpvalTotal
21780	VstpCgpaGttActScpvalDiscard
21781	VstpCgpaGttActScpvalNotApplied

For more details related to measurements, refer to Measurement Reference document.

2.4.2.2.4 Dependencies

The SCPVAL action has no dependency on any other vSTP operation.

2.4.2.2.5 Troubleshooting

The following are the troubleshooting scenarios for SCPVAL action:

- If an incoming MSU successfully passes SCPVAL CdPA GTT action, then the `VstpCdpaGttActScpvalTotal` measurement will be pegged on a per Linkset basis.
- If validation was not applied by SCPVAL CdPA GTT action on an incoming message, VstpCdpaGttActScpvalNotApplied will be pegged on a per Linkset basis.
- If incoming MSU is discarded by SCPVAL CdPA GTT action, then VstpCdpaGttActScpvalDiscard measurement will be pegged on a per Linkset basis.

- If validation was not applied by SCPVAL CgPA GTT action on an incoming message, VstpCgpaGttActScpvalNotApplied will be pegged on a per Linkset basis .
- If an incoming MSU successfully passes SCPVAL CgPA GTT action , then VstpCgpaGttActScpvalTotal measurement will be pegged on a per Linkset basis.
- If incoming MSU is discarded by SCPVAL CgPA GTT action, then VstpCgpaGttActScpvalDiscard measurement will be pegged on a per Linkset basis.
- When anyone of the GTT Action (i.e. DUPLICATE, FORWARD, TCAP ERROR, SCPVAL) fails and UIMREQD is set to ON, then event 70278 GTT Action Failed will be generated. It contains error cause with SCCP and TCAP details, GTT Action set name and linkset ID.
- If any of the above statement fails as per given scenarios, then verify the configuration. In case the issue persistes, contact Oracle Support.

2.4.3 MTP Based GTT with Screening Action

vSTP supports the MTP based GTT with screening actions feature.

This feature provides the capability of performing SCCP services on MTP-routed messages. Therefore, allows the operator to perform GTT and GTT Actions on MTP Routed MSUs, similar to GTT handling for GT Routed MSUs.

> **Note:**
>
> This feature supports the screening based on MTP3 layer parameters only.

2.4.3.1 MTP Based GTT Feature Configuration

The MTP based GTT with Screening Action is performed if the service handling results in Fall through to GTT or if **GTT Required** option is **ON** for Service Relayed MSU.

The following system-wide options are used to configure this functionality:

- **MTP Routed GTT**

  The MTP Routed GTT (mtprgtt) option is used for MTP Routed GTT functionality as follows:

  – If option = **OFF**, then GTT shall not be performed on MTP Routed MSUs.

  – If option = **Use MTP Point codes**, then GTT shall be performed on MTP Routed MSU, SCCP Portion shall be updated based on translation entry but MSU shall be sent to Original DPC (and not to translated DPC).

  – If option = **Full GTT**, then GTT shall be performed on MTP Routed MSU, SCCP Portion as well as MTP Portion shall be updated based on translation results.

- **MTP Routed GTT fallback**
  The MTP Routed GTT fallback (mtprgttfallbk) option is used for error handling to be performed in case of GTT failure for MTP routed MSUs. It has the following values:

- If option = **GTT failure**, then MSU will be discarded with appropriate UIM. UDTS will be sent to originator and measurements shall be pegged as done for GT routed messages.
- If option = **Fall back to MTP routing**, then MSU (with translation/modification/ routing data from UDR-related service) shall be MTP routed.

The support for the following features is required for the functionality of MTP based GTT:

- SCCP Stop Action: provide a means for the operator to specify SCCP Stop Action in the MTP Screening Rules, to allow the MTP processing to fall through to GTT on non-discarded MSUs.
- XLAT = NONE: provide a means for the operator to specify GTT Translation Type = NONE.
- •

  GTT SET = DPC: A new GTT set, DPC (with set type dpc) shall be supported. The provisioning and behavior of the DPC Translations shall be same as OPC Translations. However, DPC GTT set cannot be used as secondary optional set (i.e. DPC GTT set cannot be assigned to OPCSN parameter in translation entry). The DPC GTT set type can be searched only when the GTT hierarchy is FLOBR specific.

2.4.3.1.1 MMI Managed Objects for MTP Based GTT

MMI information associated with MTP Based GTT Support is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for vSTP MTP Based GTT feature:

Table 2-3 vSTP MTP Based GTT Managed Objects and Supported Operations

Managed Object Name	Supported Operations
sccpoptions	Update
mtpscreeningrules	Insert, Update, Delete

sccpoptions - Display

The Signaling Connection Control Part (SCCP) Options are those configuration values that govern the overall SCCP functionality . There is a single instance of this resource, which contains each of the individual options that can be retrieved and set. Because there is no collection of instances, there is no collection GET action. No new SCCP Options resource can be created, so there is no POST action, and the single instance cannot be removed, so there is no DELETE action. The single instance GET is used to retrieve the options, and PUT is used to update one or more values within the set of options. A name for this single, non- deletable instance is neither required nor expected.

Example output for display:

```
{
       "class1seq": "Disabled",
        "dfltfallback": false,
        "dfltgttmode": "Cd",
        "mtprgtt": "Fullgtt",
        "mtprgttfallback": "Gttfail",
        "tgtt0": "None",
        "tgtt1": "None",
        "tgttudtkey": "Mtp",
        "tgttxudtkey": "Mtp"
}
```

mtpscreeningrules - Insert, Update, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
{
           "actionSccp": true,
            "area": "7",
            "nsfi": "Stop",
            "ruleName": "rule5",
            "scrRuleGroupName": "scr5",
            "scrRuleGroupType": "Opc",
            "signalingPointId": "3",
            "zone": "3"
}
```

2.4.3.1.2 MTP Based GTT Alarms and Measurements

Alarms and Events

No specific Alarms and Events are generated for MTP based GTT.

Measurements

The following table lists the measurements specific to the MTP based GTT feature:

Measurement ID	Measurement Name
21304	VstpRxMSUMtpRoutedSccp

For more details related to measurements, refer to Measurement Reference Guide.

2.4.3.2 Dependencies

The MTP based GTT support for vSTP has no dependency on any other vSTP operation.

2.4.3.3 Troubleshooting

In case of the error scenarios, the measurements specific to MTP based GTT feature are pegged. For information related to MTP based GTT measurements, see MTP Based GTT Alarms and Measurements.

2.5 Flexible GTT Load Sharing

Flexible GTT Load Sharing (FGTTLS) provides more routing diversity for GTT traffic. There are two parts to Flexible GTT Load Sharing: Flexible Intermediate GTT Load Sharing applied to GTT traffic requiring intermediate global title translation, and Flexible Final GTT Load Sharing applied to traffic requiring final global title translation.

2.5.1 Flexible Intermediate GTT Load Sharing

Flexible Intermediate GTT Load Sharing provides more flexible GTT load sharing arrangements for GTT traffic requiring intermediate global title translation (the routing indicator in the message is GT) than the load sharing arrangements provided by the Intermediate GTT Load Sharing feature. The Flexible GTT load sharing and Intermediate GTT load sharing features are enabled by default to perform Flexible Intermediate GTT Load Sharing.

Intermediate Load Sharing Feature Only

With the Intermediate GTT Load Sharing feature enabled and turned on and the load shares post-GTT destinations when intermediate GTT is being performed through the use of the MRN table. The destination point codes in the MRN table can appear in the MRN table only once. The MRN table contains groups of point codes with a maximum of 32 point codes in each group. This arrangement allows only one set of relationships to be defined between a given point code and any other point codes in the MRN group. All global title addresses in the GTT table that translate to a point code in the given MRN group will have the same set of load sharing rules applied.

For example, the following point codes and relative cost values are provisioned in the MRN table.

```
PC              RC
005-005-005     10
006-001-001     10
006-001-002     10
006-001-003     10
006-001-004     10
006-001-005     10
006-001-006     10
006-001-007     10
```

When the point code in the intermediate GTT is translated to 005-005-005, all traffic routed using the global title addresses in the global title translations containing this point code are load shared equally, no matter what the global title address is.

> **Note:**
>
> If you want to provision an IGT or GTT action without load sharing mode, then MRNSET is not specified.

2.5.2 Flexible Final GTT Load Sharing

Flexible Final GTT Load Sharing provides more routing diversity for GTT traffic requiring final global title translation (the routing indicator in the message is SSN) than the load sharing arrangements provided by the mated applications without the Flexible GTT Load Sharing feature enabled.

Final Load Sharing Feature Only

The destination point codes and subsystems in the MAP table can appear in the MAP table only once. The MAP table contains groups of point codes with a maximum of 32 point codes and subsystems in each group. This arrangement allows only one set of relationships to be defined between a given point code and subsystem and any other point codes and subsystems in the MAP group. All global title addresses in the GTT table that translate to a point code and subsystem in the given MAP group will have the same set of load sharing rules applied.

When the point code and subsystem in the final global title translation is translated to 005-005-005, subsystem 251, all traffic routed using the global title addresses in the final global title translations containing this point code and subsystem are load shared equally, no matter what the global title address is.

2.6 Weighted GTT Load Sharing

The default behavior for performing load sharing between nodes with the same relative cost is to perform the load sharing in a round-robin fashion. A limitation of this design is that all destinations have equal processing power and should receive an equal load. However, as new hardware is added to load-sharing groups, the load-sharing groups may have different processing capabilities. Customization of the load-sharing group would allow the traffic load to be distributed on the individual characteristics of each destination.

Another default behavior is to route traffic to a load-shared group if any member of that group with the relative cost value is available. Depending on the traffic, this can overwhelm and congest a node, even though other nodes at different relative cost values could have handled the traffic.

Both of these scenarios can be solved with the Weighted GTT Load Sharing feature, which allows unequal traffic loads to be provisioned in mated application (MAP) and mated relay node (MRN) load sharing groups.

The Weighted GTT Load Sharing feature is enabled by default. The MAP and MRN sets are used by MAP and MRN load sharing groups. Weighted GTT Load Sharing can be applied to load shared only or combined dominant/load shared MAP or MRN

groups, and cannot be applied to solitary mated applications, or dominant MAP or MRN groups.

This feature also allows provisioning control over load sharing groups so that if insufficient capacity within the load sharing group is available, the load sharing group is not used.

Weighted GTT Load Sharing provides two controls for GTT traffic distribution through either the MAP or MRN groups:

- Individual weighting for each entity in a relative cost (RC) group
- In-Service threshold for each RC group

An RC group is a group of entries in either a MAP group or an MRN group that have the same relative cost value. An entity is either a point code entry in the MRN table or a point code and subsystem number entry in the MAP table.

A MAP group or MRN group can also be referred to as an entity set.

Weighted GTT Load Sharing can be applied to only load shared or combined dominant/load shared MAP or MRN groups, and cannot be applied to solitary mated applications, or dominant MAP or MRN groups.

Individual Weighting

Individual weighting is a method for assigning a different load capacity to each member of an RC group. Each entity is assigned a weight from 1 to 99 and receives a percentage of the traffic equal to its weight relative to the RC group's total weight. To calculate the percentage of traffic that a particular entity receives within its RC group (assuming all nodes are active and available for traffic), use the following equation:

% of traffic for the entity = (weight value assigned to the entity/RC group weight) x 100%

> **Note:**
>
> With round-robin load-sharing, there is a concept of the preferred entity. The preferred entity is the outcome of GTT. It is the first entity used for load-sharing after initialization, and is the primary entity for Class 1 SCCP Sequenced traffic. When weights are applied, no entity has any preference over another based on GTT information. Distribution is based on the RC group chosen by GTT, not the specific entity.

Individual Weighting Example

Table 2-4 shows how weighting affects traffic delivery. Entity A has a weight of 40 and the total RC group weight is 110, entity A receives 36% of the traffic. Entity C is has a weight of 10 and receives only 9% of the traffic for this group. The total group weight is the sum of the individual weight values assigned to each entity in the group.

> **Note:**
>
> In order to maintain 100% for the RC group, some rounding may occur. This rounding error will always be ± 1%.

Table 2-4 RC Group Weight Example

Entity	RC	Weight	RC Group Weight	Percentage of Traffic
A	10	40	110	(40 / 110) * 100% = 36%
B	10	30		(30 / 110) * 100% = 27%
C	10	10		(10 / 110) * 100% = 9%
D	10	30		(30 / 110) * 100% = 28%

If all entities in an RC group have the same weight, the outbound traffic pattern provides equal distribution. For weighted load shared or weighted combined load shared MRN or MAP groups with In-Sequence Class 1 SCCP option on, In-Sequence Class 1 SCCP traffic is routed using the provisioned data as the initial method of routing and dynamic data (if the entity selected by provisioned data is prohibited) as the secondary method of routing. This allows all Class 1 traffic to be delivered to the same destination, and the traffic routing is affected unless the original destination changes status. If Transaction-Based GTT Load Sharing is not turned on, then the Weighted GTT Load Shared MSU Key is used. This provides a consistent MSU Key for the Class 1 SCCP

An MSU Key is a value calculated from parameters of an MSU that allows the MSU to be assigned to an entity within an RC group. An MSU Key always maps to the same entity until there is a status change to the MAP or MRN group.

In-Service Threshold

The in-service threshold defines the minimum percentage of weight that must be available for an RC group to be considered available. If the percentage of the available weight is less than the in-service threshold, then the entire RC group is considered unavailable for traffic. If the percentage of the available weight is equal to or greater than the in-service threshold, then the RC group is considered available, and traffic can be sent to any available entity in the RC group. The in-service threshold helps to prevent congestion when only a small portion of the RC group is available.

The in-service threshold has an initial value of 1%, and has a range of values from 1% to 100%. Current round-robin load sharing has an in-service threshold value of 1%, where if any entity in an RC group is available, it is always used.

The group weight that must be available to carry traffic (the required group weight) is determined by multiplying the total group weight (the sum of the individual weight values assigned to each entity in the group) by the in-service threshold value, expressed as a percentage. For example, if the RC group weight is 110, and the in-service threshold is 75%, the required group weight is 82.

An RC group can be in one of three states: Available, Prohibited, and Threshold-Prohibited. These states are determined by comparing the required RC group weight to the weight of the entities that are actually available for traffic, the entity available weight.

If the state of the entity in the RC group is Available, the entity available weight is the weight value assigned to the entity. If the state of the entity in the RC group is either

Congested or Prohibited, the entity available weight is 0. The sum of all entity available weights in the RC group is the RC group available weight. Table 2-5 shows how the states of the RC group are determined.

Table 2-5 RC Group In-Service Threshold States

RC Group State	Description
Available	The RC group available weight is greater than or equal to the Required RC group weight. Traffic can routed to the RC group in all circumstances.
Prohibited	All entities in the RC group are prohibited (the RC group Available Weight = 0). No traffic can be routed to this RC group.
Threshold-Prohibited	At least one entity in the RC group is not prohibited, but RC group available weight is less than the required RC group weight. Even if the RC group available weight is 0, if one entity is congested, then the state of the RC group is Threshold-Prohibited. Normally, no traffic is routed to this RC group. The Transaction-based GTT Load Sharingand the SCCP Class 1 Sequencing features may route traffic to this group if the primary node is congested. Instead of moving this transaction-based traffic to another node and then back quickly when the congestion abates, routing will continue to the primary node.

In-Service Threshold Example

In the example shown in Table 2-6, the RC group consisting of entities A, B, C, and D does not have sufficient available weight for the group (70 is less than 82), and therefore the RC group is considered Threshold-Prohibited. This RC group is unavailable for traffic.

The RC group consisting of entities E and F does have sufficient available weight for the group, and the RC group is considered Available.

The RC group consisting of entities G and H is Prohibited, since both entities G and H are Prohibited.

The RC group consisting of entities I and J is Threshold-Prohibited, since entity I is Congested. In order for the RC group status to be Prohibited, all entities in the RC group must be Prohibited. Non-Transaction-Based GTT Load Sharing traffic is not routed to the RC group.

If the Transaction-Based GTT Load Sharing feature is enabled and turned on, or SCCP Class 1 Sequencing is used, then traffic can be routed to entity I if that is the primary entity for the traffic (traffic would be routed if entity I were Available).

Table 2-6 In-Service Threshold Example

Entity	RC	Wgt.	RC Group Wgt.	In-Service Threshold	Req. RC Group Wgt.	Entity Status	Entity Avail. Wgt.	RC Group Avail. Wgt.	RC Group In-Service Threshold Status
A	10	40	110	75%	82	Available	40	70	Threshold - Prohibited
B	10	30				Prohibited	0		
C	10	10				Prohibited	0		
D	10	30				Available	30		
E	20	30	40	100%	40	Available	30	40	Available
F	20	10				Available	10		
G	30	20	70	50%	35	Prohibited	0	0	Prohibited
H	30	50				Prohibited	0		
I	40	25	50	50%	25	Congested	0	0	Threshold - Prohibited
J	40	25				Prohibited	0		

Load-Sharing Groups

Weighted GTT Load-Sharing can be applied to only load shared mated application or MRN groups, or combined dominant/load shared mated application or MRN groups.

A load shared MAP or MRN group is a MAP or MRN group containing entries whose RC (relative cost) values are equal.

When Weighted GTT Load Sharing is applied to load shared MAP or MRN groups, traffic is distributed among the entities according to:

- Entity Status – traffic is only routed to an entity if the entity is considered Available.
- Entity Available Weight – the entity receives a percentage of the traffic determined by its weight relative to the total available weight of the RC group.
- RC group status - refer to Table 2-5.
- Available RC group weight – The sum of all entity available weights in the RC group.

Table 2-7 shows an example of Weighted GTT Load Sharing applied to a load shared MAP or MRN group.

Table 2-7 Load Shared Group with Weighted GTT Load Sharing Example

Entity	RC	Weight	RC Group Weight	In-Service Threshold	Required RC Group Weight	Entity Status
A	10	40	110	50%	55	Available
B	10	30				Prohibited
C	10	10				Available
D	10	30				Available

Entity	Entity Available Weight	RC Group Available Weight	RC Group In-Service Threshold Status	MAP or MRN Group Status	Current Load %
A	40	80	Available	Available	50%
B	0				0
C	10				13%
D	30				37%

All entities in the load shared group are in the same RC group, so if the RC group is unavailable for traffic, all traffic is discarded.

A combined dominant/load shared MAP or MRN group is a MAP or MRN group containing a minimum of two entries whose RC (relative cost) values are equal and a minimum of one entry whose RC value is different.

When Weighted GTT Load Sharing is applied to combined dominant/load shared MAP or MRN groups, traffic is distributed among the entities according to:

- Entity Status – traffic is only routed to an entity if the entity is considered Available.
- Entity Available Weight – the entity receives a percentage of the traffic determined by its weight relative to the total available weight of the RC group.
- RC group status – refer to Table 2-5.
- Available RC group weight – The sum of all entity available weights in the RC group.
- MRN or MAP Group Status – the MRN or MAP group must be considered Available in order to route traffic.

Table 2-8 shows an example of a weighted combined load shared group.

Based on the results of global title translation, traffic is routed to one of the RC groups in the weighted combined load shared group. If that RC group is unavailable for traffic, the RC group with the next highest cost that is available for traffic is used to route the traffic. If a higher cost RC group is being used to route traffic, and a lower cost RC group becomes available, the lower cost RC group is then used to route the traffic.

The status of the combined dominant/load shared group is based on the status of the RC groups that make up the combined dominant/load shared group. If the status of any RC group is Available, then the status of the combined dominant/load shared group is Available. If no RC group is available for traffic, but the status of at least one of the RC groups is Threshold-Prohibited, then the status of the combined dominant/

load shared group is Threshold-Prohibited. If the status of all the RC groups is Prohibited, then the status of the combined dominant/load shared group is prohibited.

Table 2-8 Combined Dominant/Load Shared Group with Weighted GTT Load Sharing Example

Entity	RC	Weight	RC Group Weight	In-Service Threshold	Required RC Group Weight	Entity Status
A	10	40	110	75%	82	Available
B	10	30				Prohibited
C	10	10				Prohibited
D	10	30				Available
E	20	30	40	100%	40	Available
F	20	10				Available
G	30	10	10	1%	1	Available

Entity	Entity Available Weight	RC group Available Weight	RC group In-Service Threshold Status	MRN or MAP Group Status	Current Load %
A	40	70	Threshold - Prohibited	Available	0
B	0				0
C	0				0
D	30				0
E	30	40	Available		75%
F	10				25%
G	10	10	Available		100%

> **Note:**
>
> The Current Load % column shows the percentage of traffic each entity in the RC group handles.

MSU Routing under Congestion

For Transaction-Based GTT Load Sharing or SCCP Class 1 Sequenced traffic, the original destination of the traffic must be maintained under congestion. Diverting traffic during congestion can lead to invalid transaction states, and the originator is not informed of any problem. If a congested node is selected, then traffic is routed to that node. If the message is discarded, then a UDTS is generated so the originator is informed of a problem. If the node is prohibited, then the selection of an alternate node is acceptable.

For all other traffic, rerouting this traffic away from a congested node is acceptable, since no sequencing or state information needs to be maintained. This can be accomplished by considering a congested entity as Unavailable (thus, its available weight is 0). The congested node receives no traffic. The state of the RC group may transition from Available to Threshold-Prohibited.

2.7 Transaction-Based GTT Load Sharing

Transaction-Based GTT Load Sharing allows messages with the same transaction parameters (TCAP, SCCP, MTP, or ENHMTP parameters) to be routed to the same destination within an entity set.

> **Caution:**
>
> This feature is not enabled by default and once it is enabled, it cannot be disabled. To enable it, use MMI, which is described in the MMI API guide under the Vstp: Feature Admin States section.

An entity set is a group of entities that are used to determine the proper destination of a post-GTT message. This group of entities can be one of the following:

- A mated application (MAP) group
- A mated relay node (MRN) group
- A mated application set (MAPSET), if the Flexible GTTLoad Sharing feature is enabled
- A mated relay node set (MRNSET), if the Flexible GTT Load Sharing feature is enabled.

This feature applies to the following types of SCCP messages:

- UDT/UDTS class 0 messages
- UDT/UDTS class 1 messages
- XUDT/XUDTS class 0 messages
- XUDT/XUDTS class 1 messages.

UDT/UDTS and XUDT/XUDTS messages are load shared using a key derived from these elements in the message.

- MTP parameters - the first 3 bytes of the incoming OPC and 1 byte of the SLS.
- SCCP parameters - the last 4 bytes of the global title address field of the called party address.
- TCAP parameter - the TCAP Transaction ID in the messages.
- Enhanced MTP parameter - a combination of the SLS and the incoming OPC values.

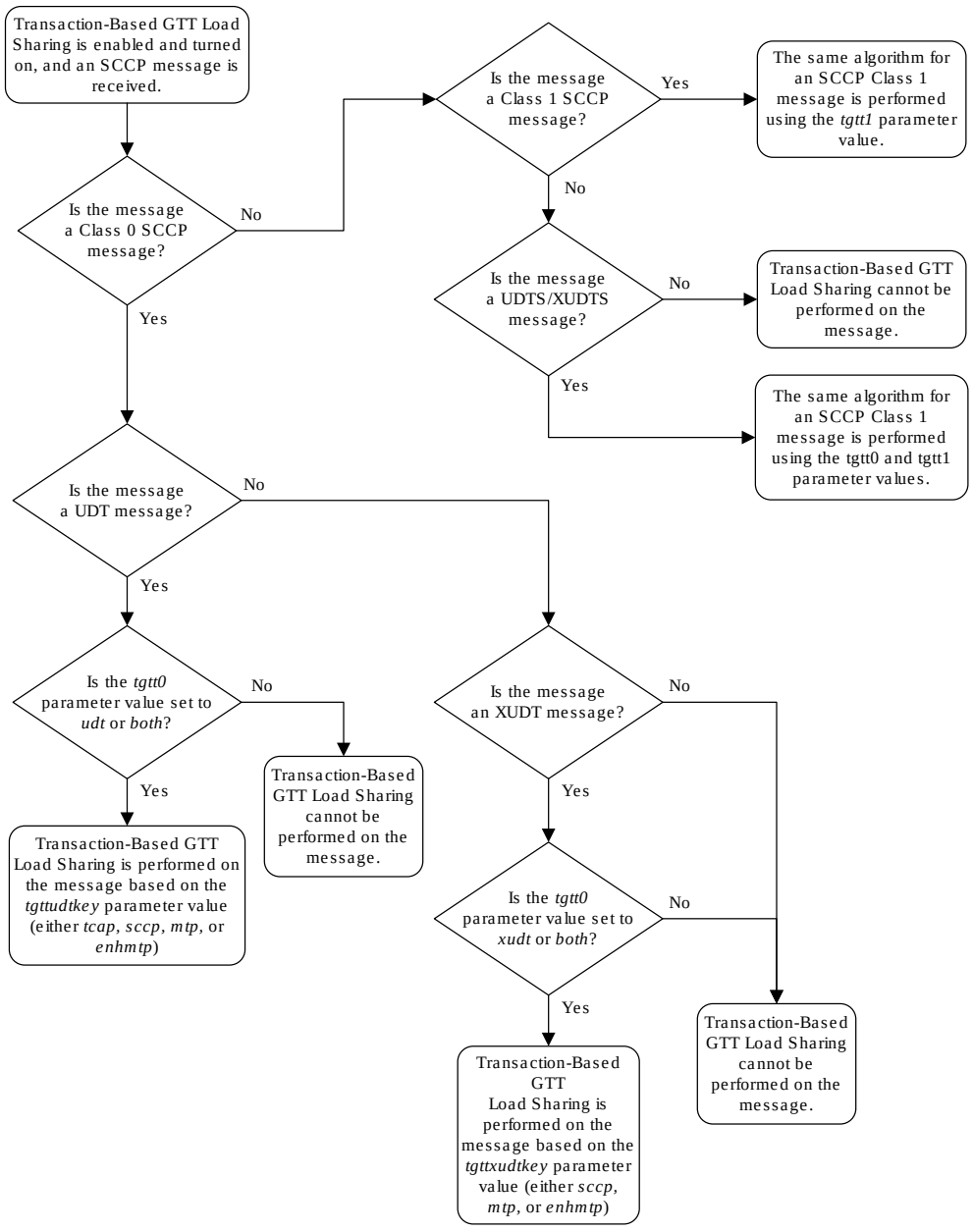
SCCP opts can be changed using MMI. Refer to MMI API documentation for updating the SCCP opts parameter. These parameters are:

- `tgtt0` – enable or disable Transaction-Based GTT Load Sharing for SCCP Class 0 UDT, UDTS, XUDT, or XUDTS messages.
- `tgtt1` – enable or disable Transaction-Based GTT Load Sharing for SCCP Class 1 UDT, UDTS, XUDT, or XUDTS messages.
- `tgttudtkey` – the Transaction Parameter for the incoming UDT or UDTS messages.

- `tgttxudtkey` – the Transaction Parameter for the incoming XUDT or XUDTS messages.

Figure 2-8 describes how the Transaction-Based GTT Load Sharing SCCP options are used.

Figure 2-8 Transaction-Based GTT Load Sharing SCCP Options



Only load shared and combined dominant/load shared entity sets are used to determine the routing for messages that are processed by the Transaction-Based GTT Load Sharing feature.

Using a load shared entity set, the entire entity set is a part of one RC group and the messages are load-shared based on the Transaction Parameter in the entities in the entity set. If none of the entities in the entity set are available for routing, then the message is discarded and a UDTS/XUDTS message is generated if Return on Error is set in the SCCP message. A UIM is generated indicating that the message has been discarded.

Using a combined dominant/load shared entity set, the RC group containing the point code, or point code and SSN, obtained as a result of the global title translation process is used to determine how the message is routed. If none of the entities in this RC group are available for routing, the next higher cost RC group is chosen. This is repeated until an entity in an entity set is available for routing. When an entity is found that is available for routing, the message is routed according to the criteria in that entity. If none of the entities in the entity set are available for routing, the message is discarded. A UDTS/XUDTS message is generated if “Return on Error” is set in the SCCP message. A UIM is generated indicating that the message has been discarded.

2.8 Stateful Application Feature

SS7 Firewall - Stateful Applications (SFAPP) allows vSTP to validate the messages coming in for a subscriber by validating them against the Visitor Location Register (VLR). The last seen details of the subscriber can be fetched from the Home Location Register (HLR). Once the HLR provides a validity of the new VLR, vSTP then allows the message into the network. If the message is not validated, it is handled as per configuration (either silent discard, fallback, or respond with error).

2.8.1 Supported MAP Operations

The following MAP Operations are supported by the Stateful Applications feature.

Table 2-9 Supported MAP Operations

MAP Operation	OpCode	Application Context (AC)	AC Code
sendParameters	9	infoRetrieval /v1	14
Registers	10	networkFunctionalSs	18
Erases	11	networkFunctionalSs	18
Activates	12	networkFunctionalSs	18
deactivates	13	networkFunctionalSs	18
interrogates	14	networkFunctionalSs	18
authenticationFailureReport	15	authenticationFailureReport /v3	39
registerPassword	17	networkFunctionalSs	18
processUnstructuredSS-Data	19	networkFunctionalSs /v1	18
mo-forwardSM	46	shortMsgMO-Relay	21
noteSubscriberPresent	48	mwdMngt/v1	24

Table 2-9 (Cont.) Supported MAP Operations

MAP Operation	OpCode	Application Context (AC)	AC Code
beginSubscriberActivity	54	networkFunctionalSs / V1	18
restoreData	57	networkLocUp/v2	1
processUnstructuredSS-Request	59	networkUnstructuredSs v2	19
readyForSM	66	mwdMngt /v2/v3	24
purgeMS	67	istAlerting /v2/v3	4
purgeMS	67	msPurging /v3	27
ss-Invocation-Notification	72	ss-InvocationNotification	36
statusReport	74	reporting	7
istAlert	87	istAlerting /v3	4
NoteMM-Event	89	mm-EventReporting	42
updateLocation	2	networkLocUp	1
updateGprsLocation	23	gprsLocationUpdate/v3	32
sendAuthenticationInfo	56	infoRetrieval /v2/v3	14

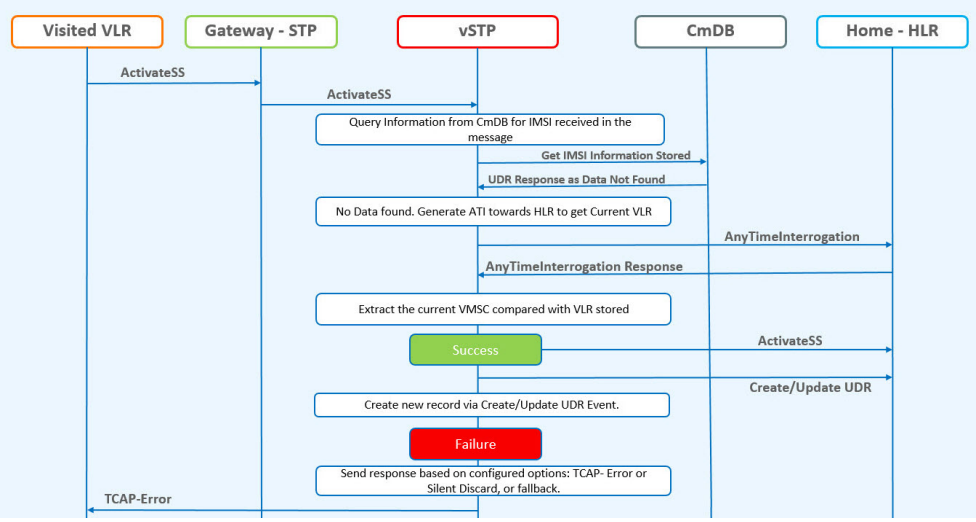
2.8.2 VLR Validation

The VLR Validation uses the information stored in the HLR about the current VLR to validate the VLR from which the message is received.

The vSTP Call flow for VLR Validation first lookup the Common DB that is UDR for IMSI. If the record is available, then the ATI is not sent to HLR and the UDR information is used further. But, in case the record is not available in UDR, then ATI is sent to HLR. Both the scenarios of vSTP call flow for VLR Validation are described below:

- **vSTP Call Flow - When no record is found in Common DB**
  The following figure shows the vSTP call flow when IMSI record is not available in Common DB:

Figure 2-9 VLR Validation - vSTP Call Flow when No IMSI Record Found in UDR



1. The incoming message will be decoded.
   a. An Error will be generated in case of decode failure.
2. The message information will be stored in the local database.
3. The request to get the IMSI information is generated towards UDR.
4. If the IMSI record is not found in UDR, the Any Time Interrogation (ATI) request will be generated towards the HLR.
   a. The ATI Request will be coded so that Acknowledgment is received on the same MP, as the DB is local.
5. For a successful response from the HLR:
   a. The ATI Response will be decoded to get the current VLR address.
   b. The current VLR address will be compared with the CgPA stored in the local database for the subscriber.
   c. On a successful Match, forward the message stored in the local DB to HLR. The UDR is updated with the new IMSI record by sending Update or Create Event to UDR corresponding to IMSI of query message.
   d. In case of failure,
      i. Send the configured response.
      ii. Increment the measurement for failed messages.

The ATI sent to HLR must be formatted as follows:

1. MTP OPC=vSTP SID, MTP DPC = HLR PC
2. SCCP CGPA (RI = SSN, PC = Local Signaling Point SID, SSN = <SSFAPP SSN>, SCCP CDPA (received message CDPA)
3. TCAP BEGIN with valid MAP dialogue portion (as per MAP specification)
4. TCAP DTID = unique OTID generated for each ATI (The DTID will not be reused within 4.5 seconds)

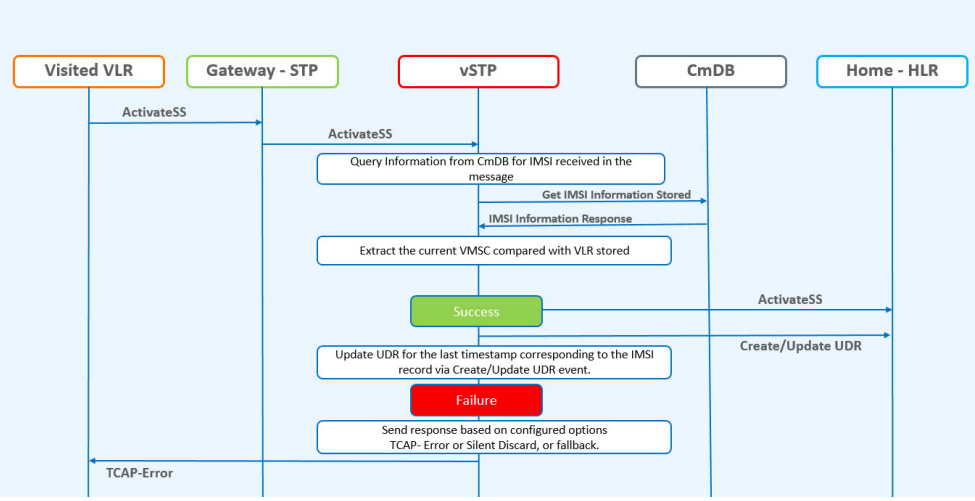
5. ATI details: IMSI = IMSI/MSISDN received in received message, and other mandatory parameters

The Local Signaling Point will validate the ATI_ACK received from the HLR. A valid ATI_ACK message is defined as:

1. It is a well formatted ANSI or ITU SCCP UDT, non-segmented XUDT message, with a valid TCAP END message, with valid dialogue portion, and single component in the component portion as return result with operation code = ATI_ACK
2. Value of DTID received in TCAP END matches with one of the ongoing transactions
3. Component type is a return result and contains ATI_ACK.
4. VMSC digits are received in ATI_ACK

- **vSTP Call Flow - When IMSI record is found in Common DB**
The following figure shows the vSTP call flow when the IMSI record is available in Common DB:

Figure 2-10 VLR Validation - vSTP Call Flow when IMSI Record is Found in UDR



1. The incoming message will be decoded.
   a. An Error will be generated in case of decode failure.
2. The message information will be stored in the local database.
3. The request to get the IMSI information is generated towards UDR.
4. The current VLR address from UDR response will be compared with the CgPA stored in the local database for the subscriber.
5. On a successful Match,
   a. Forward the Message stored in the local DB to HLR.
   b. The UDR is updated with the latest timestamp for this IMSI record by sending Update event .
6. In case of failure,

a. Send the configured response.

b. Increment the measurement for failed messages.

2.8.3 Velocity Check

The Velocity Check use case uses the information stored in HLR about the current VLR and the age of location parameter to identify if the new VLR is reachable from the current VLR stored in HLR.

This use case is dependent on the validity of the information stored in the VLR and the T3212 timer (periodic update location timer). This timer governs the rate at which the mobile subscriber autonomously updates their location. In case the time distance between two networks is less than the value of T3212 timer configured for the network, this use case test would provide false positives since the location age information would not have been properly updated in the VLR.
The assumption for successful execution of this use case are:

- The First location update can be identified using the IMSI only in the address.
- The Age of Location provided by HLR is accurate.
- The quantum of information (Age of Location) will not be less than the time to get travel.

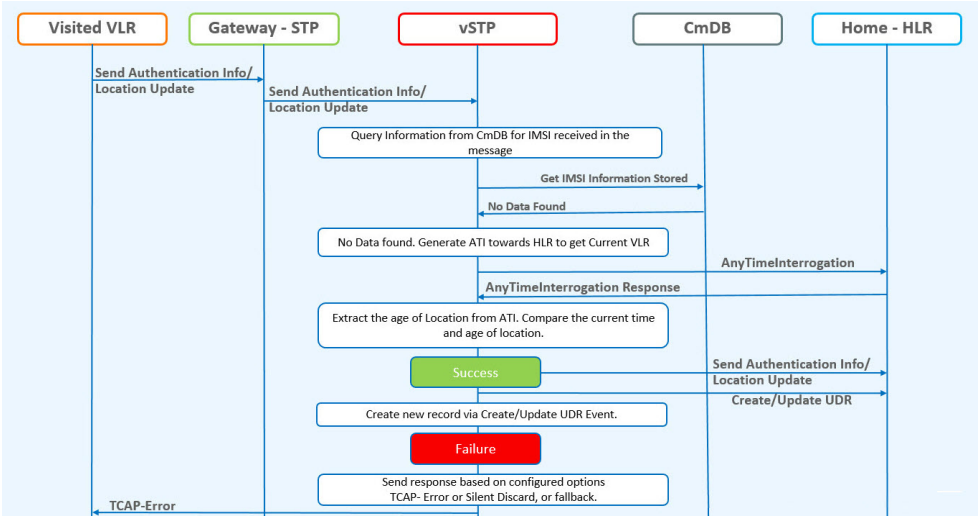
The vSTP Call flow for Velocity Check, can be completed in a reasonable amount of time for Location Update to succeed.

The vSTP Call flow for Velocity Check, first lookup the Common DB that is UDR, for IMSI. If the record is available in UDR, then the ATI is not sent to HLR and the UDR information is used further. But, in case the record is not available in UDR, then ATI is sent to HLR.
In both the scenarios, the UDR is updated in case of successful validation. If record is not found in UDR and validation is successful through ATI, then a new record is created in UDR with that IMSI. In case the IMSI record is available in UDR and validation is successful, then the last updated time of the record is updated in UDR.

Both the scenarios of vSTP call flow for VLR Validation are described below:

- **vSTP Call Flow for Velocity Check - When no IMSI record is found in Common DB**
  The following figure shows the vSTP call flow when there is no record available in Common DB:

Figure 2-11 Velocity Check - vSTP Call Flow when IMSI Record is not Found in UDR



1. A local database on vSTP will be configured to identify the network locations (using country codes for VLR addresses) and the shortest amount of time it may take to travel between them.
2. The incoming message will be decoded:
   a. An Error will be generated in case of decode failure.
   b. A Measurement will be pegged for the decode failure with OpCode and CgPA.
3. The message information will be stored in the local database.
4. The request to get the IMSI information is generated towards UDR.
5. If the IMSI record is not found in UDR, the ATI request will be generated toward the HLR identified in the CdPA of the incoming message. The ATI request will be coded so that it is received on the same MP, as DB is local.
6. In case the HLR sends a failure in the ATI response:
   a. A measurement will be pegged to identify HLR error corresponding message from CgPA (VLR).
7. For a success response, extract the Age of Location from the ATI Response message and the VMSC address in the HLR.
8. A record is created in UDR for the IMSI after successful validation.
9. In case the VLR from which the SAI/LU was received matches the VLR in the ATI response, do nothing.
10. In case the VLR addresses do not match:
    a. Calculate the time difference between the current time and the Age of Location.
    b. Verify the Age of Location is less than the travel time configured in the local database.

c. Calculate the distance between two country codes using Havrshine Formula. Longitude/Latitude values are retrieved from database for corresponding entries.

d. In case the time value is not within limits:

i. The validation gets failed.

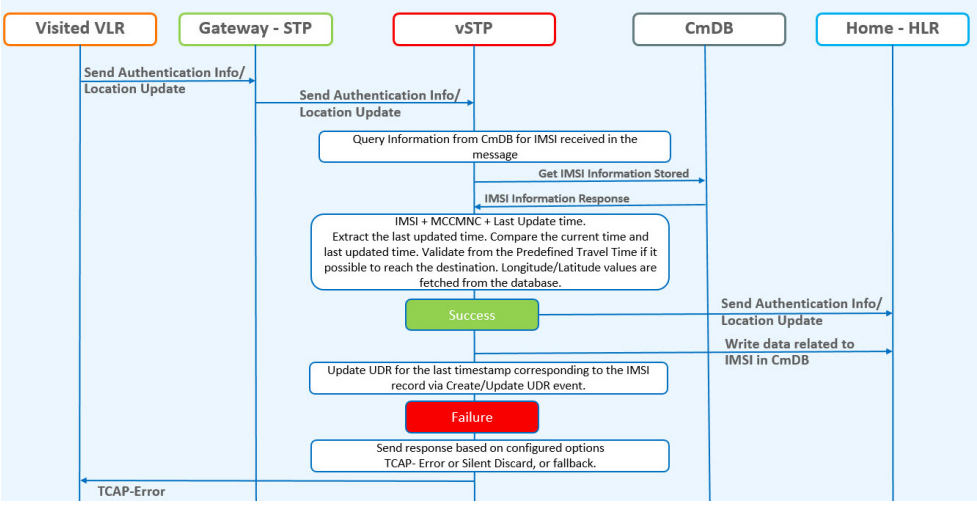
ii. A measurement will be pegged.

iii. Response will be generated based on the configured option.

11. If validation is successful, forward message to HLR and update the UDR with relevant data with VLR number, last updated Network, last update time.

- **vSTP Call Flow - When IMSI record is found in Common DB**
The following figure shows the vSTP call flow when the IMSI record is available in Common DB:

Figure 2-12 Velocity Check - vSTP Call Flow when IMSI Record Found in UDR



1. A local database on vSTP will be configured to identify the network locations (using country codes for VLR addresses) and the shortest amount of time it may take to travel between them.
2. The incoming message will be decoded:
   a. An Error will be generated in case of decode failure.
   b. A Measurement will be pegged for the decode failure with OpCode and CgPA.
3. The message information will be stored in the local database.
4. In case VLR address do not match:
   a. Lookup into SfappCCMCCMap table and for corresponding country codes and retrieve the MCC.
   b. The exception or neighboring list table is checked for with old MCC, if it is available in neighboring list then do nothing. Else, the following step will be performed.

5. The exception or neighboring list table is checked for with old MCC, if it is available in neighboring list then the process ends. Else, the following step will be performed.
6. The distance between 2 country codes is calculated using Havrshine Formula. Use Longitude/Latitude values from database.
7. The Time (= Distance / Velocity) shall be calculated and used to authenticate the subscriber location.
8. Validate the last time distance check based on last location with the VLR address received in the incoming message.
9. In case the VLR addresses do not match:
    a. Calculate the distance between 2 country codes using Havrshine Formula using longitude and latitude values (from SfappLongLat MO).
    b. Calculate the time using distance calculated from above point and travel_velocity value from vSTPSccpOptions MO.
    c. Verify that Time calculated in point b is less than the (current time -last update time from UDR).
10. If validation is successful forward message to HLR and update the UDR with relevant data with VLR number, last updated Network, last update time.
11. In case the validation failed,
    a. A measurement will be pegged.
    b. Response will be generated based on the configured option.

Note:

- The T3212 timer is responsible for periodic location update for subscribers. If the timer is set to a value greater than the shortest travel time value between two network locations, then the location validation in the use case fails.
- Results of the use cases depends on the pre-configured values of SfappCCMCCMAP, SfappCountryLongLat, SfappCountryCodes, and SfappNeighboringCountries entries.

2.8.3.1 Velocity Check Flow Charts

The following flow charts provide an overview of the Velocity Check feature for Stateful Applications:

Figure 2-13 SFAPP Process Message

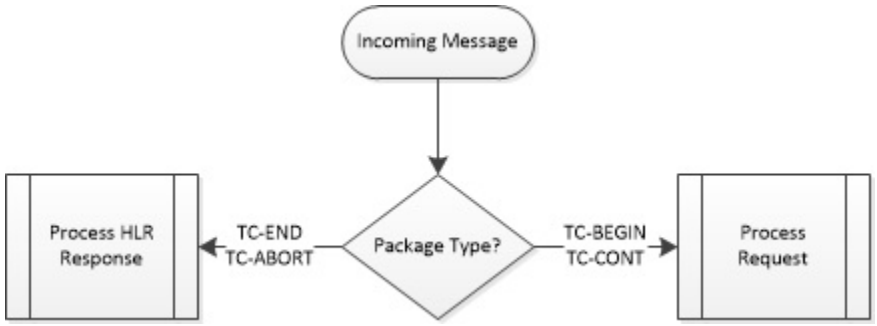


Figure 2-14 Perform VLR Validation

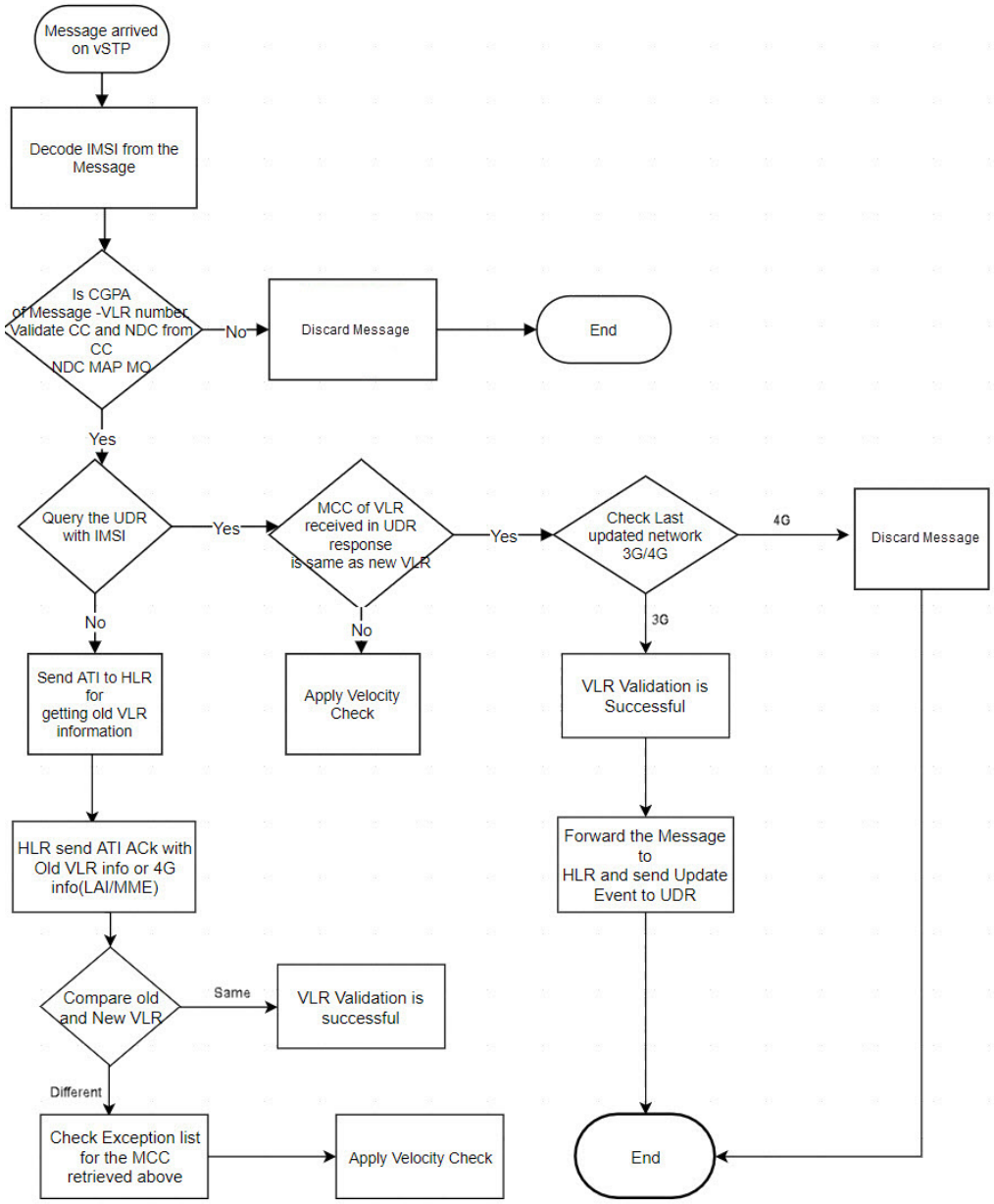
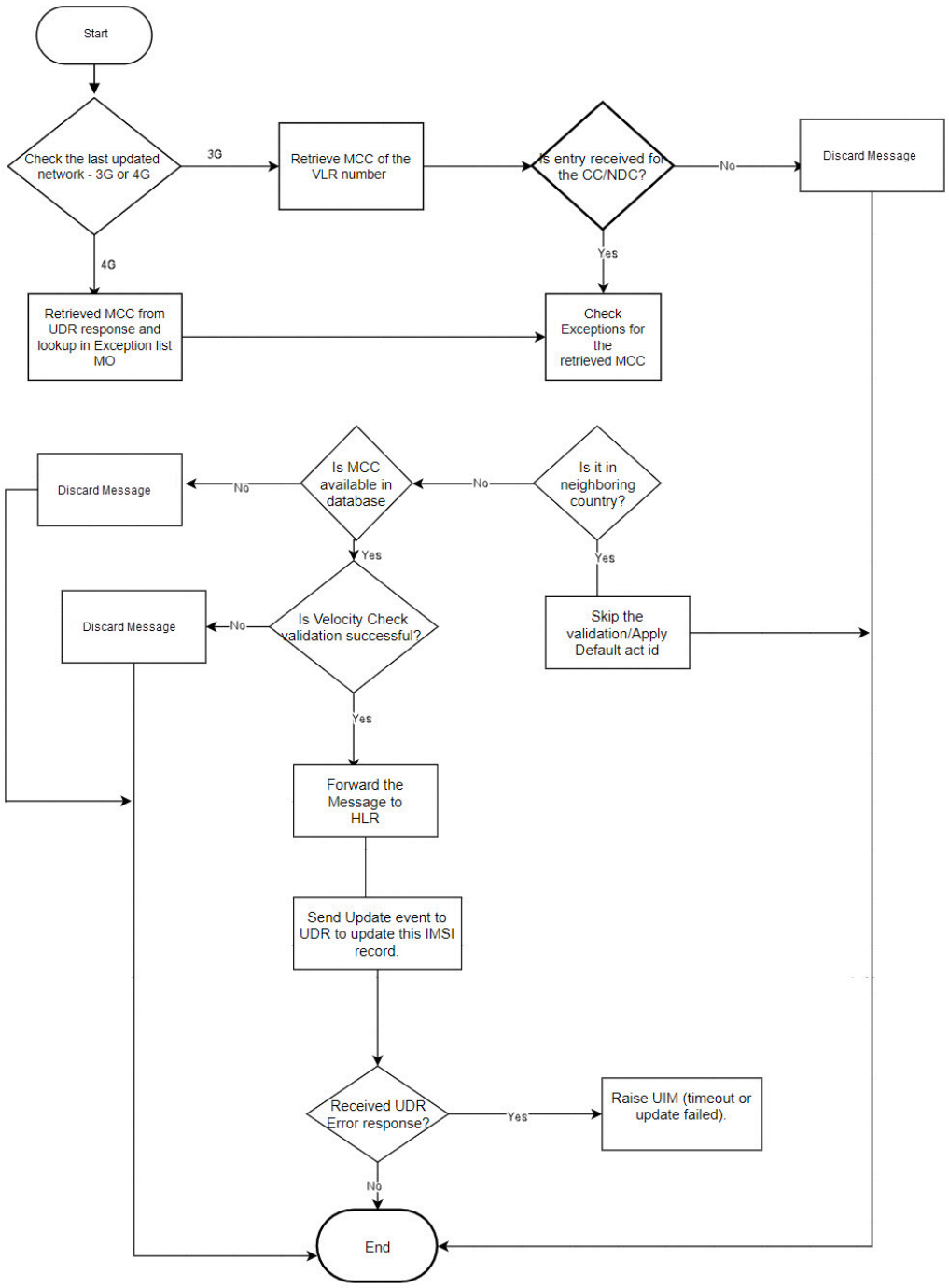


Figure 2-15 Perform Velocity Check



2.8.4 Stateful Security Dynamic Learning

The Stateful Security Dynamic Learning feature enables vSTP to create and use a whitelist that is created as part of learning from the validation attempts defined in VLR Validation. This feature is independent of the category of messages but it provides protection against all the messages coming from VLRs that fail the validation and are

not part of the created whitelists. A grey list and black list is also created for the VLRs that fail the validation.

Learning is controlled by these modes using a mode parameter in the SFAPPOPTS table:

- **Learn Mode**: This mode allows to learn about new VLRs and no validations are performed. The newly learnt VLRs are considered as whitelisted.

  > **Note:**
  >
  > The user can configure the amount of time for which the vSTP operates in Learn mode. The time is configured in SFAPPOPTS table.
  > Hence, the switch from Learn to Test mode can happen either by configuring the timer, or manual switch.

- **Test Mode**: This mode validates all the learned VLRs. In case the VLR is not validated, the learnt VLRs remains greylisted and and measurements and alarms are generated.
- **Active Mode** : This mode allows validations based on the learned white lists in the system. New VLRs are also learned in this mode.

  The status of dynamically learnt VLRs are changed to whitelist or blacklist as per their status.
- **OFF Mode**: When none of the above modes is active, it is considered as OFF mode. In this mode, if VLR entry is in whitelist, then no validation is performed for that VLR.
  By default, the OFF mode remains enabled. That means the SFAPP dynamic learning functinality is disabled.

> **Note:**
>
> - In any mode, if VLR is in whitlist table, then it is considered as whitelisted, and the message is forwarded to HLR.
> - If user has changed the mode from Learn/Test/Active mode to OFF mode, then the user has to wait for at least 10 mins before switching the mode again to Active/Learn/Test mode.

2.8.4.1 Call Flow in Learn Mode

This mode does not validate any VLRs and consider all the VLRs interacting with the network as valid. All the New VLRs that are used during this modes shall be added to the dynamic tables.

The Learn mode and be changed to Test mode in the following ways:

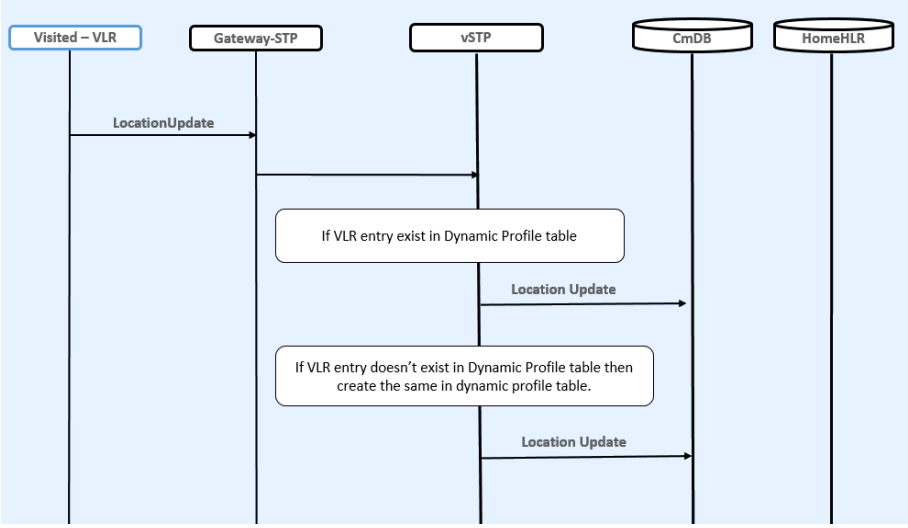
- Automatically, upon expiry of the configured learn mode time limit, if configured. You can configure the time in number of hours for which the vSTP operates in this mode in SFAPPOPTS table. The recommended time period for Learn mode is 6 to 12 hours.

- By manual switching of mode

VLR Validation in Learning Mode

The following figure shows the vSTP call flow for VLR validation in learning mode:

Figure 2-16 VLR Validation in Learning Mode

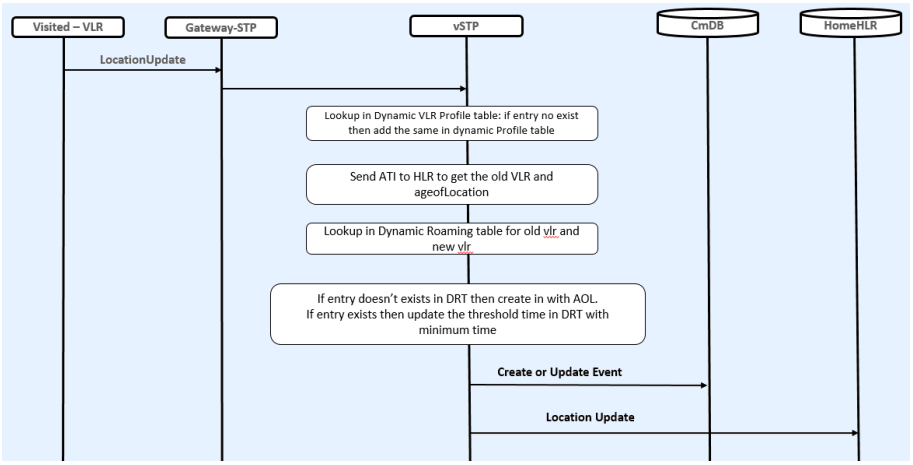


1. The incoming message will be decoded.
   An Error will be generated in case of decode failure.
2. The message information will be stored in the local database.
3. Lookup in VLR Whitelist table (static Profile).
   - If entry is found for new VLR, then the validation is skipped.
   - If entry is not found in static Whitelist VLR table, then the lookup is performed in Dynamic Profile Table (DPT).
4. - If the entry is not available in DPT, then create it with filter as graylisted, and forward the message to HLR.
   - If entry is avilable in DPT and it is GL, then forward the message to HLR.
5. Also, Send the Create or Update event to UDR for IMSI record.

Velocity Check in Learning Mode

The following figure shows the vSTP call flow for Velocity check in learning mode:

Figure 2-17 Velocity Check in Learning Mode



1. The incoming message will be decoded:
   a. An Error will be generated in case of decode failure.
   b. A Measurement will be pegged for the decode failure with OpCode and CgPA.
2. The message information will be stored in the local database.
3. If New VLR entry is not there is Dyn VLR Profile table then create it.
4. The ATI request will be generated toward the HLR identified in the CdPA of the incoming message.
5. In case the HLR sends a failure in the ATI response, a measurement will be pegged to identify HLR error corresponding message from CgPA (VLR).
6. For a success response, extract the Age of Location from the ATI Response message and the VMSC address in the HLR.
7. In case the New VLR from which the SAI/LU was received matches the old VLR in the ATI response, no action is required.
8. In case the VLR addresses does not match and old VLR is not available in Dynamic Profile table, then create the entry.
9. Lookup in Dynamic Roaming table (DRT):
   - If entry is not available, then create the DRT entry with threshold value as AgeofLocation value received in ATI ack.
   - If DRT is already available for the same combination of old VLR and new VLR, and the value of age of location is different than that in the dynamic VLR roaming entry, age of location value in roaming entry is updated to a minimum of the age of location in dynamic VLR roaming entry and the age of location received in ATI ACK. Also Increment the entry_usage_threshold.
10. Send the update location to HLR and also send CreateorUpdate event to UDR.

If user has configured the switch-mode timer then after expiry of that timer (in hrs), mode will switch to test mode.

2.8.4.2 Call Flow in Test Mode

This mode validates all the learned VLRs at all times. In case the VLR is not validated, it is added to greylist and measurements and alarms are generated. These measurements and alarms allows the operator to validate the whitelists and the overall solution, before they choose to go to the Active mode.

The mode can be changed to ACTIVE mode:

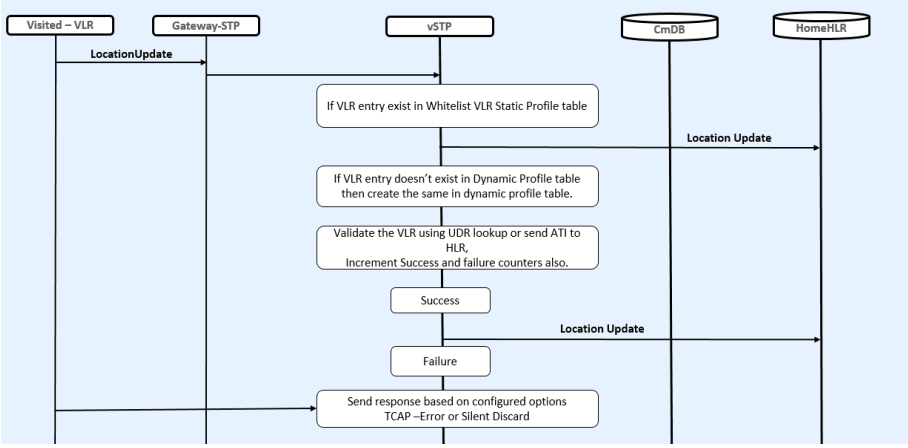
- Automatically, upon expiry of the test mode time limit, if configured
- By manual switching of mode

All the messages coming from the VLRs are allowed to the home network. This mode allows the operator to test the VLRs creation in learning mode.

VLR Validation in Test Mode

The following figure shows the vSTP call flow for VLR validation in test mode:

Figure 2-18 VLR Validation in Test Mode



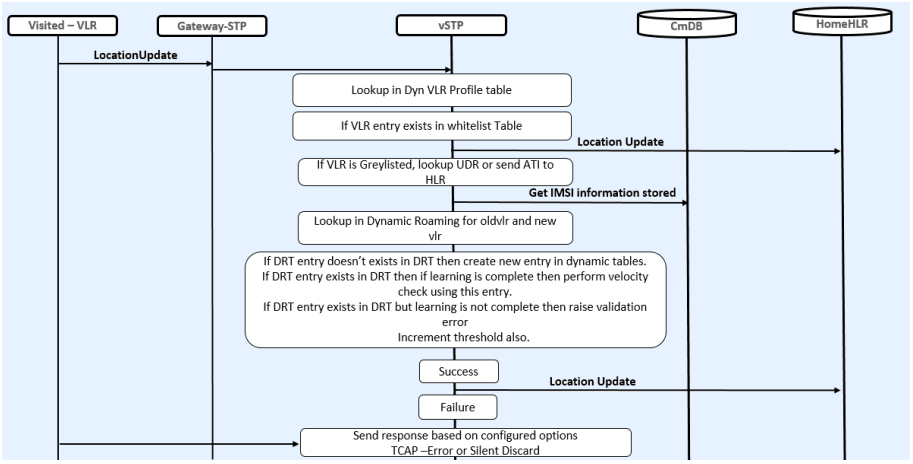
1. The incoming message is decoded. An error is generated in case of decode failure.
2. The message information gets stored in the local database.
3. Lookup in VLR Whitelist table (Profile).
   If entry is available for new VLR, then skip the validation. Otherwise, continue below steps.
4. Lookup in DPT:
   - If entry is not available for New VLR, then create the Entry in DPT.
   - If entry in DPT exists, then VLR validation is performed with lookup in UDR for that IMSI.
5. If record is not found in UDR then send ATI to HLR.
6. Update success & failure counts based on validation results.
7. If validation is success then send location update to HLR and send CreateorUpdate event to the UDR for latest timestamp.

8. If validation is failed then send response based on configured option:
   Fail Action Id is FALLBACK (do not discard messages even if the validation fails in test mode for dynamic VLRs)
9. The Greylisted dynamic VLRs remain unchanged. They are not moved to Whitelisted or Blacklisted VLRs. However, the event notification for status change (GL->BL, GL->WL, and so on) is raised, based on the threshold values.

Velocity Check in Test Mode

The following figure shows the vSTP call flow for Velocity check in test mode:

Figure 2-19 Velocity Check in Test Mode



1. 1. The incoming message is decoded.
   a. An Error will be generated in case of decode failure.
   b. A Measurement is pegged for the decode failure with OpCode and CgPA.
2. The message information is stored in the local database.
3. If no new VLR entry is available in Dyn VLR Profile table, then create the VLR entry.
4. Perform validation by sending ReadEvent to UDR for that IMSI record.
   - If the record is available in UDR, then extract the lastUpdatedTimestamp and VLR from UDR response.
   - If the record is not available in UDR, then ATI request is generated towards the HLR identified in the CdPA of the incoming message.
     For a success response from HLR, extract the Age of Location from the ATI Response message and the VMSC address in the HLR.
5. In case the new VLR from which the SAI/LU was received, matches the old VLR in the UDR/ATI response, no action is performed.
6. In case the VLR addresses do not match:
   - If old VLR is not available in DPT, then create the entry.
   - If old VLR status is Blacklisted, then entry is not created in DPT. The velocity check results in Validation Failure.

2.8.4.3 Call Flow in Active Mode

This mode enables the following actions:

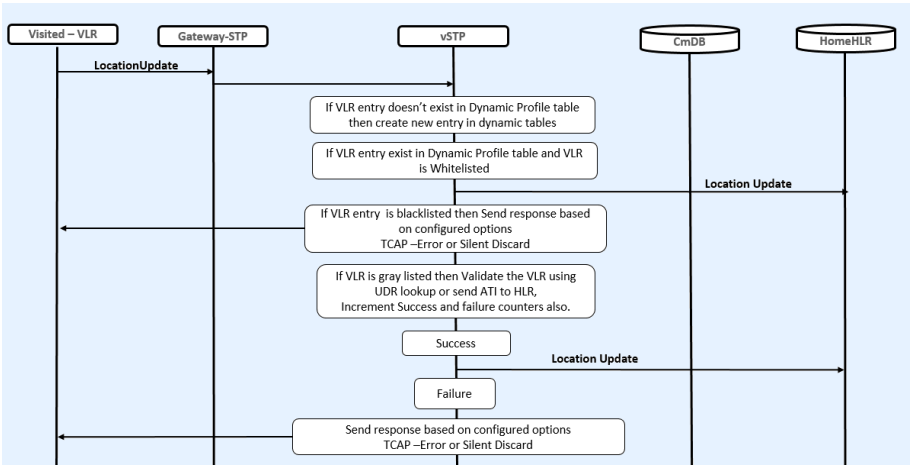
- Learning of new VLRs. The status of existing VLRs get changed as per success or failure counts.
- Handling the dynamic VLRs based on their status. The following table describes the dynamic VLRs with status and respective results:

Status	Result
Whitelist	Validation Success. VLR validation is not performed
Blacklist	Validation Failure
Graylist	VLR validation is not performed **Note**: – Success and Failure validation count is incremented based on validation result. – The GrayListed dynamic VLRs status can change to Whitelisted or Blacklisted
Successful Validation Count	When the net **successful validation count** reaches threshold, then VLR status is changed to Whitelisted. **Note**: **success count - failure count** >= **success threshold**
Failure Validation Count	When the net **failure validation count** reaches threshold, then VLR status is changed to Blacklisted. **Note**: **failure count - success count** > = **failure threshold**

VLR Validation in Active Mode

The following figure shows the vSTP call flow for VLR validation in active mode:

Figure 2-20 VLR Validation in Active Mode

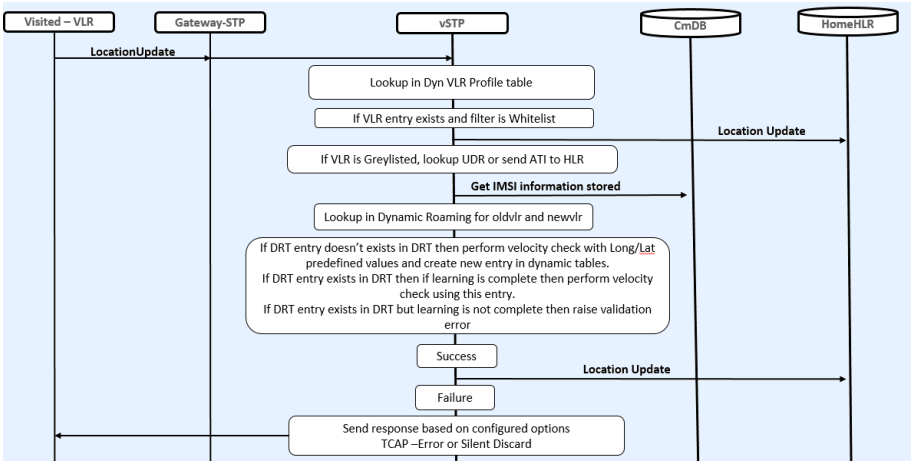


1. If the VLR is available in DPT or Whitelist Profile Table (WPT) as whitelist, then the validation is successful and LocUpdate is sent to HLR.
2. In case the VLR is available in DPT as blacklist, then the message is rejected.
3. If DPT entry is GL, then VLR validation is performed.
4. If entry does not exists, then create new entry in DPT (as learn mode is also enabled in active mode).
5. If entry is GL or entry doesn't exists in DPT, then perform validation such as lookup in UDR.
   - If IMSI record is found in UDR, then extract VLR from UDR response.
   - If record is not found in UDR then, send ATI to HLR and extract VLR from ATI ACK.
6. If old and new VLRs are same, then validation is success, otherwise the validation is failed.
7. Move VLR to BL/WL based on the threshold value, validation result, and raised event.
8. On successful validation, send CreateorUpdate event to UDR.

Velocity Check in Active Mode

The following figure shows the vSTP call flow for Velocity check in active mode:

Figure 2-21 Velocity Check in Active Mode



1. If old and new VLRs are not same, then perform velocity check.
2. If the status of the old VLR Blacklisted, then entry is not created in DPT. The velocity check results in Validation Failure.
3. Perform lookup in DRT for old and new VLR combination. If entry exists and learning is complete (velocity_threshold exceeds), then perform velocity check using the entry.
4. If no DRT entry is available, then create entry using long/lat table time and perform velocity check using that DRT entry. Update UDR if validation is successful. Also update VLR success or failure count, based upon the validation result.

5. If entry is available but learning is not complete, then take time from LONG/LAT table and reset the time also with LonG/Lat table Time and Perform velocity check and VLRs count based upon the result.
6. Update UDR if validation is successful.

2.8.5 SFAPP Configurations

This section provides procedures to configure the connection required for SFAPP to access the database.

SFAPP is configured using the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.8.5.1 MMI Managed Objects for SFAPP

MMI information associated with SFAPP is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

Table 2-10 lists the managed objects and operations supported for vSTP SFAPP feature.

Table 2-10 vSTP SFAPP Managed Objects and Supported Operations

Managed Object Name	Supported Operations
SfappNeighboringCountries	Insert, Delete
VstpMateStp	Insert, Update, Delete
SfappCountryCodes	No operations supported
SfappCountrylongLati	No operations supported
SfappCCMCCMap	Insert, Delete
VstpSccpApplications	Insert, Update, Delete
VstpSccpOptions	Update

SfappNeighboringCountries - Insert, Delete

Execute the MMI Client command from an active SOAM.

```
 /vstp/SfappNeighboringCountries/
{
    "data": [
        {
            "mcc": 289,
            "name": "Abkhazia",
            "neighMcc": 250,
            "neighName": "Russia",
            "uniqueIdentifier": "289-250"
        },
…
        {
            "mcc": 648,
            "name": "Zimbabwe",
```

```
            "neighMcc": 655,
            "neighName": "South Africa",
            "uniqueIdentifier": "648-655"
        },
        {
            "mcc": 648,
            "name": "Zimbabwe",
            "neighMcc": 645,
            "neighName": "Zambia",
            "uniqueIdentifier": "648-645"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM for Delete operation:

```
 /commonsecurity/neighboringcountries/<uniqueIdentifier> -v DELETE
```

Example output:

```
No output returned by URI: https://localhost/mmi/dsr/v3.1/
commonsecurity/neighboringcountries/648-645? for 'DELETE' operation
```

VstpMateStp - Insert, Update, Delete

Example:

Execute this command on an active SOAM to display entries.

```
 /vstp/matestps/
{
   "data": [
       {
           "domain": "Itun",
           "pointCode": "13"
       }
   ],
   "links": {},
   "messages": [],
   "status": true
}
```

Create a file as follows for insert:

```
$cat matestp.json
```

```
{
    "domain": "Itun",
    "pointCode": "13"
}
```

Execute this command on an active SOAM to insert:

```
 /vstp/matestps/ -v POST -r <Absolute Path>/<filename>
```

Example output:

```
 /vstp/matestps/ -v POST -r matestp.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/matestps/<pointCode> -v DELETE
```

Example output:

```
 /vstp/matestps/12 -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.1/vstp/
matestps/12? for 'DELETE' operation
```

SfappCCMCCMap - Insert, Delete

Execute the MMI Client command from an active SOAM.

```
 /commonsecurity/mappings/
{
    "data": [
        {
            "cc": 1,
            "mcc": 310,
            "ndc": 1,
            "uniqueIdentifier": "1-1"
        },
…
       {
            "cc": 998,
            "mcc": 434,
            "uniqueIdentifier": "998-0"
        }
    ],
    "links": {},
    "messages": [],
```

```
    "status": true
}
```

Execute the following command to display:

```
 /commonsecurity/mappings/<uniqueIdentifier>
```

Example output:

```
  /commonsecurity/mappings/"998-0"{
    "data": {
        "cc": 998,
        "mcc": 434,
        "uniqueIdentifier": "998-0"
    },
    "links": {
        "delete": {
            "action": "DELETE",
            "description": "Delete this item.",
            "href": "/mmi/dsr/v3.1/commonsecurity/mappings/998-0",
            "type": "status"
        },
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/commonsecurity/mappings/998-0",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
[root@fixsetup-soa1 ~]# cat mapping.json
        {
            "cc": 998,
            "mcc": 434
        }
```

Create a file as follows for insert:

```
cat mapping.json
        {
            "cc": 998,
            "mcc": 434
        }
```

Execute the following command to insert:

```
 /commonsecurity/mappings/ -v POST -r <Absolute Path>/<filename>
```

Example output:

```
 /commonsecurity/mappings/ -v POST -r mapping.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /commonsecurity/mappings/<uniqueIdentifier> -v DELETE
```

Example output:

```
 /commonsecurity/mappings/"998-0" -v DELETENo output returned by URI:
https://localhost/mmi/dsr/v3.1/vstp/gttactions/actid2006? for 'DELETE'
operation
```

VstpSccpApplications - Insert, Update, Delete

Execute the MMI Client command from an active SOAM.

```
 /vstp/sccpapplications/
{
    "data": [
        {
            "appType": "Sfapp",
            "ssn": 67
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

Execute the following command to display:

```
 /vstp/sccpapplications/<appType>


 /vstp/sccpapplications/"Sfapp"
{
    "data": {
        "appType": "Sfapp",
        "ssn": 67
    },
    "links": {
        "delete": {
            "action": "DELETE",
            "description": "Delete this item.",
            "href": "/mmi/dsr/v3.1/vstp/sccpapplications/Sfapp",
```

```
            "type": "status"
        },
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/vstp/sccpapplications/Sfapp",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
```

Example output:

```
     "data": {
        "cc": 998,
        "mcc": 434,
        "uniqueIdentifier": "998-0"
    },
    "links": {
        "delete": {
            "action": "DELETE",
            "description": "Delete this item.",
            "href": "/mmi/dsr/v3.1/commonsecurity/mappings/998-0",
            "type": "status"
        },
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/commonsecurity/mappings/998-0",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
[root@fixsetup-soa1 ~]#
Insert
[root@fixsetup-soa1 ~]# cat mapping.json
        {
            "cc": 998,
            "mcc": 434
        }
```

Create a file as follows for insert:

```
 $cat sccpapplication.json
{
    "appType": "Sfapp",
    "ssn": 68
```

```
}
```

Execute the following command to insert:

```
 /vstp/sccpapplications/ -v POST -r <Absolute Path>/<filename>
```

Example:

```
 /vstp/sccpapplications/ -v POST -r sccpapplication.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

To update the file:

```
$cat  sccpapplication.json
{
    "appType": "Sfapp",
    "ssn": 69
}
```

Execute this command on an active SOAM to update:

```
 /vstp/sccpapplications/ -v PUT -r <Absolute Path>/<filename>
```

Example output:

```
 /vstp/sccpapplications/ -v PUT -r sccpapplication.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/sccpapplications/<appType> -v DELETE
```

Example output:

```
 /vstp/sccpapplications/"Sfapp" -v DELETE
No output returned by URI: https://localhost/mmi/dsr/v3.1/vstp/
sccpapplications/Sfapp? for 'DELETE' operation
```

VstpSCCPOptions- Update

Execute the MMI Client command from an active SOAM.

```
 /vstp/sccpoptions/
{
    "data": {
        "class1seq": "Disabled",
        "dfltfallback": false,
        "dfltgttmode": "Cd",
        "mtprgtt": "Off",
        "mtprgttfallback": "Mtproute",
        "tgtt0": "None",
        "tgtt1": "None",
        "tgttudtkey": "Mtp",
        "tgttxudtkey": "Mtp",
        "travelVelocity": 700
    },
    "links": {
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/vstp/sccpoptions/",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
```

> **Note:**
>
> The **travelVelocity** is an existing MO and a new parameter "travel_velocity" has been added as part of SFAPP feature.

Create a file as follows for update:

```
 $cat  sccpoption.json
{
    "class1seq":"Disabled",
    "dfltfallback": false,
    "dfltgttmode": "Fcd",
    "itun16ScmgEnabled":false,
    "tgtt0": "None",
    "tgtt1": "None",
```

```
    "tgttudtkey": "Mtp",
    "tgttxudtkey": "Mtp",
    "mtprgtt": "Usemtppc",
    "mtprgttfallback" "Gttfail",
    "travelVelocity": 650
}
```

Execute the following command to update:

```
 /vstp/sccpoptions/ -v PUT -r <Absolute Path>/<filename>
```

Example output:

```
 /vstp/sccpoptions/ -v PUT -r sccpoption.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Example output:

```
 /vstp/sccpoptions/
{
    "data": {
        "class1seq": "Disabled",
        "dfltfallback": false,
        "dfltgttmode": "Fcd",
        "mtprgtt": "Usemtppc",
        "mtprgttfallback": "Gttfail",
        "tgtt0": "None",
        "tgtt1": "None",
        "tgttudtkey": "Mtp",
        "tgttxudtkey": "Mtp",
        "travelVelocity": 650
    },
    "links": {
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/vstp/sccpoptions/",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
```

SfappCountryCodes

There is no MMI support available for SfappCountryCodes, but a user can retrieve the data by executing get command on an active SOAM.

SfappCountrylongLati

There is no MMI support available for SfappCountrylongLati, but a user can retrieve the data using get command on an active SOAM.

2.8.5.2 MMI Managed Objects for SFAPP

The following table lists the managed objects and operations supported for SFAPP Dynamic Learning feature.

Table 2-11 SFAPP Dynamic Learning Managed Objects and Supported Operations

Managed Object Name	Supported Operations
SfappOptions	Display, Update
whitelistvlrprofile	Insert, Update, Delete
vlrprofiles	Display
vlrromings	Display

SfappOptions - Display, Update

Execute the MMI Client command from an active SOAM to display:

```
/vstp/sfappoptions
```

Example Output:

```
{
    "data": [
        {
            "agingTimer": "None",
            "failureThreshold": "4",
            "learnTimer": "5",
            "sfappMode": "Test",
            "successThreshold": "5",
            "velocityThreshold": "40"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

Create a file as follows for insert:

```
cat <filename.json>
{
```

```
   "failureThreshold": "5"
}
```

Execute this command on an active SOAM for Update operation:

```
 /vstp/sfappoptions -v PUT -r /tmp/<filename.json>
```

Example output:

```
{
    "data": [
        {
            "agingTimer": "None",
            "failureThreshold": "5",
            "learnTimer": "5",
            "sfappMode": "Test",
            "successThreshold": "5",
            "velocityThreshold": "40"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

Whitelist Vlr Profiles - Insert, Update, Delete

Example:

Execute this command on an active SOAM to display entries.

```
 /vstp/whitelistvlrprofiles/

"data": [
       {
            "filter": "WhiteList",
            "vlr": 1
       }
```

Create a file as follows for insert:

```
Cat <filename>
        {
            "filter": "WhiteList",
            "vlr": 1
        }
```

Execute this command on an active SOAM to insert:

```
/vstp/whitelistvlrprofiles –v POST –r /tmp/<filename>
```

Example output:

```
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Execute this command on an active SOAM to delete:

```
 /vstp/whitelistvlrprofiles/16 -v DELETE
```

Example output:

```
 /vstp/whitelistvlrprofiles/12 -v DELETE
```

VLR Profiles - Display

Execute the MMI Client command from an active SOAM.

```
 /vstp/vlrprofiles
{
    "data": [
        {
            "failureCount": 0,
            "filter": "GrayList",
            "lastUsedTime": "1969-12-31T19:00:00-05:00",
            "successCount": 0,
            "vlr": "4114001133"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

VLR Roaming - Display

Execute the MMI Client command from an active SOAM.

```
/vstp/vlrroamings
{
    "data": [
        {
            "entryUsageCount": 2,
            "lastUsedTime": "1969-12-31T19:00:00-05:00",
            "newVlr": 65746892,
```

```
            "oldVlr": 65746892,
            "time": 4085,
            "uniqueIdentifier": "65746892-65746892"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

2.8.5.3 SFAPP Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to the SFAPP support for vSTP:

Alarm/ Event ID	Name
70293	SFAPP Validation Error
70294	SFAPP Validation Matching State not found
70295	SFAPP Validation Encoding Error
70296	SFAPP Validation Response Timeout Error.
70297	SFAPP Validation Velocity Chk Failed.
70298	SFAPP Validation Failed **Note**: The parameter `ageOfLoc` and `Threshold` with zero can be ignored if not relevant for scenarios where this UIM is observed.
70299	SFAPP Invalid CC/NDC received
70300	Updation failed in UDR
70301	VSTP SFAPP Stack Event Queue Utilization
SFAPP Dynamic Learning	
70429	VstpDynVlrStatusChanged
70430	VstpDynVeloThreshCrossed
70431	VstpDynVLRProfAging
70432	VstpDynVLRRoamAging
70433	VstpVlrDynLearningOFF
70434	VstpVlrDynLearningLearntimer

For more details related to Alarms and Events, refer to Alarms and KPIs Reference document.

Measurements

The following table lists the measurements specific to the SFAPP support for vSTP:

Measurement ID	Measurement Name
21702	VstpSfappMsgSuccess
21703	VstpSfappMsgFailed
21704	VstpSfappMsgError1

Measurement ID	Measurement Name
21705	VstpSfappMsgError2
21706	VstpRxSfappMsg
21707	VstpRxSfappMsgDiscard
21708	VstpSfappInternalError
21709	VstpSfappCADecodeFail
21710	VstpSfappCATimeOut
21711	VstpSfappCAAvgProcessTime
21712	VstpSfappCAMaxProcessTime
21713	VstpSfappSubsNotFound
21714	VstpSfappCATx
21715	VstpSfappCATxFail
21716	VstpSfappPduFull
21717	VstpSfappCAProcesTime
21718	VstpSFAPPStackQueuePeak
21719	VstpSFAPPStackQueueAvg
21720	VstpSFAPPStackQueueFull
21782	VstpTxSfappMsg
21783	VstpTxSfappMsgPeak
21784	VstpTxSfappMsgAvg
SFAPP Dynamic Learning	
21937	VstpDynNewVLR
21938	VstpDynNewRoamEntry
21939	VstpDynVLRBL
21940	VstpDynVLRWL
21941	VstpDynVLRGL
21942	VstpDynVelCrossed
21943	VstpDynVLRProfAging
21944	VstpDynVLRRoamAging

For more details related to measurements, refer to Measurement Reference document.

2.8.5.4 UDR Configuration for SFAPP

Configuring UDR fot SFAPP involves adding vSTP MP(s) to UDR and then configuring UDR on the ComAgent server.

As a prerequisites for UDR configuration, it is assumed that the user is aware of UDR and ComAgent functionality. Also, UDR must be installed and the UDR topology must be configured.

Perform the following steps:

1. Add details about the vSTP MP on the ComAgent Remote Servers screen as a client by navigating to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and clicking **Insert** on an active OCUDR NOAMP.
2. Select the OCUDR server group from the *Available Local Server Groups* that needs to communicate with vSTP MP.

3. From the active OCUDR GUI, navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** and verify connection are `InService`.
4. From the active OCUDR GUI, navigate to **Communication Agent**, and then **Maintenance**, and then **Routed Services Status** and verify the *STPDbSvc* status is `Normal`.
5. From an active DSR NOAM, navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and click **Insert**.
6. Add the UDR NO IP in the ComAgent Remote Server screen as a Server.
7. Select the STP MP server group from the *Local SG* that needs to communicate with UDR.
8. Also add the Standby and DR NOs to the Local SG.
9. Navigate to **Communication Agent**, and then **Configuration**, and then **Connection Groups**, select *STPSvcGroup* and click **Edit**.
10. Add all available UDR NO servers.
11. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status**, select the server name, and check the connection status.

UDR Configuration: SOAP Provisioning Request for IMSI
Here's an example of provisioning SFAPP data with the Type as RN and GRN in an individual IMSI.

```
<?xml version="1.0" encoding="UTF-8"?>
<subscriber>
<field name="IMSI">6912347700</field>
<field name="VPLMN">816308</field>
<field name="MCC">611</field>
<field name="MMER">epc.mnc905.mcc679.org</field>
<field name="MMEH">s6amme-epc.mnc905.org</field>
<field name="HSSR">hss@3gppnetwork.org</field>
<field name="HSSH">hss-epc.mnc905.mcc679.3gppnetwork.org</field>
<field name="lastUN">3G</field>
<field name="VLR">12340000</field>
</subscriber>
```

> **Note:**
>
> An UPDATE request from vSTP is assigned to an Active UDR only. However, a READ request from vSTP can be assigned to both Active or Standby UDR. To check the status of the UDR, navigate to **Communication AgentMaintenanceHA Services Status**. Check value for the **Active SRs** field for the UDR. If the value is **1**, the UDR is in active status. Therefore, an UPDATE request will be sent to this UDR.

2.8.6 Dependencies

The SFAPP support for vSTP has no dependency on any other vSTP operation.

2.8.7 Troubleshooting

The vSTP SFAPP sends default response in case of the following scenarios:

- **SFAPP thread CPU utilization exceeds congestion level**
  Check if the SFAPP thread CPU utilization exceeded Congestion Level 2. This check is performed at the beginning of the message processing cycle and if set, vSTP immediately responds with default response.

  The equipment status value set against eirDefRespInErr option of EirOptions table is sent right away.
- **SFAPP operational state**
  Check if the SFAPP operational state is **Unavailable**. vSTP performs this check before sending the message to UDR and if the state **Unavailable**, the default response is sent and the query is not sent to UDR. The VstpSfappCATimeOut meal is pegged in this scenario.

The following points must be considered while configuring SFAPP over vSTP:

- The J1 and ATM interfaces are not supported.
- Single vSTP MP VM can support only one 4-Port ADAX HDC3 Card.
- An ADAX HDC3 card cannot be accessed from Multiple VSTP MP VMs .
- The ADAX HDC3 driver components and RPMs needs to be installed separately.
- The DSR patch is required to be applied on vSTP MP VM that is connected to ADAX HDC3 card.
- In SFAPP dynamic learning, when no new VLRs get reflected in the replicated tables (VstpSfappVlrProfile/ VstpSfappVlrRoaming), then ensure that the vSTP OAM process is up and running on SOAM and its not under reboot.

2.9 M3UA Client Support

The MTP3-User Adaptation (M3UA) Client support allows vSTP to trigger the M3UA connection initiation. For information related to M3UA Protocol, refer to RFC 4666.

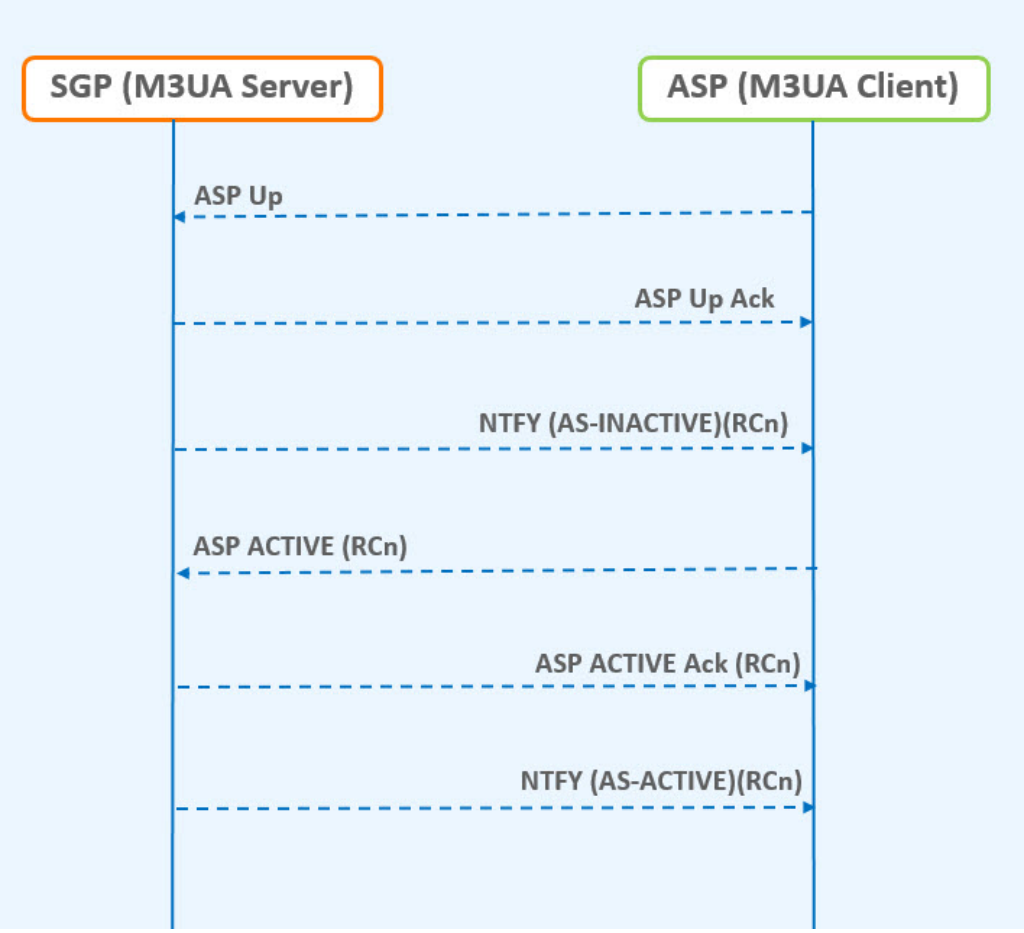
The M3UA client support over vSTP enables a user to achieve the following functionalities:

- Initiation of SCTP connection to send INIT message to the server.
- Initiation of ASP state maintenance messages such as, ASP-UP, ASP-Active etc.
- Receiving and processing of SS7 Signaling Network Management messages such as, DAVA, DUNA, DUPU, DRST, DAUD and SCON.
- Receiving and processing of M3UA notify messages (NTFY).
- M3UA peer receiving the DATA message sends an MTP-TRANSFER indication primitive to the upper layer.
- On receiving an MTP-TRANSFER request primitive from an upper layer at an ASP the M3UA layer sends a corresponding DATA message to its M3UA peer.
- The M3UA message distribution function determines the Application Server (AS) by comparing the information in the MTP-TRANSFER request primitive with a provisioned Routing Key.

Message Flow

The following figure shows the message flow for M3UA client server functionality, where, SGP acts as the M3UA server and ASP is the M3UA client:

Figure 2-22 Message Flow for ASP - M3UA Client



2.9.1 M3UA Client Support Feature Configuration

This section provides procedures to configure the connection required for M3UA client support.

M3UA client support is configured using the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.9.1.1 MMI Managed Objects for M3UA Client Support

MMI information associated with M3UA Client Support is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for vSTP M3UA Client Support feature:

Table 2-12 vSTP M3UA Client Support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
connections	Insert, Update, Delete
linksets	Insert, Update, Delete

connections - Insert, Update, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$cat conn.json
{
    "configurationLevel": "0",
    "name": "conn1",
                "connectionMode": "Client",
    "connCfgSetName": "Default",
                "connectionType": "M3UA",
    "localHostName": "lhost1",
                "remoteHostName": "rhost1"
}
```

linksets - Insert, Update, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
cat ls_sample.json
{
                    "localSignalingPointName": "lsp111",
                "numberSignalingLinkProhibitedThreshold": "1",
                "routingContext": 8, "asNotification": "true",
                "remoteSignalingPointName": "psps111",
                "numberSignalingLinkAllowedThreshold": "1",
                "gttmode": "Fcd", "configurationLevel": "0",
                "name": "ls1", "ituTransferRestricted": "false",
                "linkTransactionsPerSecond": "5000",
                "enableBroadcastException": "true",
                "cgGtmod": false, "type": "M3ua“
}
```

The POST operation using REST Call will configure the connection in the client mode.

2.9.1.2 MNP Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to the M3UA Client Support feature:

Alarm/ Event ID	Name
19231	Received Invalid M3UA Message
19235	Received M3UA Error
19256	M3UA Stack Event Queue Utilization

For more details related to alarms and events, refer to Alarms and KPI Guidelines.

Measurements

The following table lists the measurements specific to the M3UA Client Support feature:

Measurement ID	Measurement Name
21271	VstpTxM3uaDataMsg
21001	VstpRxM3uaDataMsg
21002	VstpTxM3uaDataOctets
21003	VstpRxM3uaDataOctets
21098	vSTPTxAsnOctets
21099	vSTPRxAsnOctets
21031	VstpTxASPUp
21032	VstpTxASPDown
21033	VstpTxHeartbeat
21034	VstpTxASPActive
21035	VstpTxASPInactive
21036	VstpRxDUNA
21037	VstpRxDAVA
21038	VstpRxDUPU
21039	VstpRxDRST
21040	VstpTxDAUD
21041	VstpRxASPUpAck
21042	VstpRxASPDownAck
21043	VstpRxASPActiveAck
21044	VstpRxASPInactiveAck
21045	VstpRxM3uaNotify

For more details related to measurements, refer to Measurement Reference Guide.

2.9.2 Troubleshooting

In case of the error scenarios, the measurements specific to M3UA client support feature are pegged. For information related to M3UA measurements, see M3UA Client Support Alarms and Measurements.

2.9.3 Dependencies

The M3UA Client support for vSTP has no dependency on any other vSTP operation.

2.10 Time Division Multiplexing

vSTP supports the Time Division Multiplexing (TDM) feature. This feature provides access to E1/T1 links based ADAX HDC3 PCIe TDM Card using PCIe Pass-through.

2.10.1 Feature Overview

The TDM support functionality includes the following components

- **TDM Hardware:** The hardware involves Adax HDC3 PCIe card with physical TDM connectivity supporting Virtual IO. This card contains built-in processor to process the MTP2 layer on hardware itself.

  Adax HDC3 PCIe card supports direct access using PCIe Pass-through. Therefore, a single Adax 4-port or 8-Port HDC3 PCIe card can be accessed only from a single VM at a time.
- **MTP Network Interworking Function (NIF):** An additional MTP NIF layer is added to existing vSTP MP so that the MTP3 Layer can communicate with the MTP2 layer running on the TDM PCIe Card.

  The M3RL layer in vSTP MP VM communicates with the MTP2 layer running on the Adax HDC3 card via the MTP2 Adapter layer.
- **MTP2 Adapter:** The MTP2 Adapter NIF layer on vSTP MP communicates with MTP2 layer using Virtual-IO calls. It uses the libraries and APIs provided by Adax to communicate with Adax HDC3 Card.
- **Host machine:** The Host machine allows PCI Pass-through access to the vSTP MP virtual machines.

2.10.2 Supported TDM Links

The TDM link implementation supports the following modes:

- E1 Low Speed Link (LSL) - 64 kbps and 56 kbps
- T1 Low Speed Link (LSL) - 64 kbps and 56 kbps
- E1 High Speed Link (HSL) - 2.048 mbps, 12-bit sequence numbers
- T1 High Speed Link (HSL) - 1.536 mbps , 12-bit sequence numbers

> **Note:**
>
> The Adax HDC3 card supports either E1 or T1 mode at a time. The mode must be defined during driver configuration.

2.10.3 vSTP TDM Support Components

3-Tier vSTP setup installed on the virtualization environment running on underlying Host Servers.

Adax HDC3 PCIe Card installed on Host Sever(s).

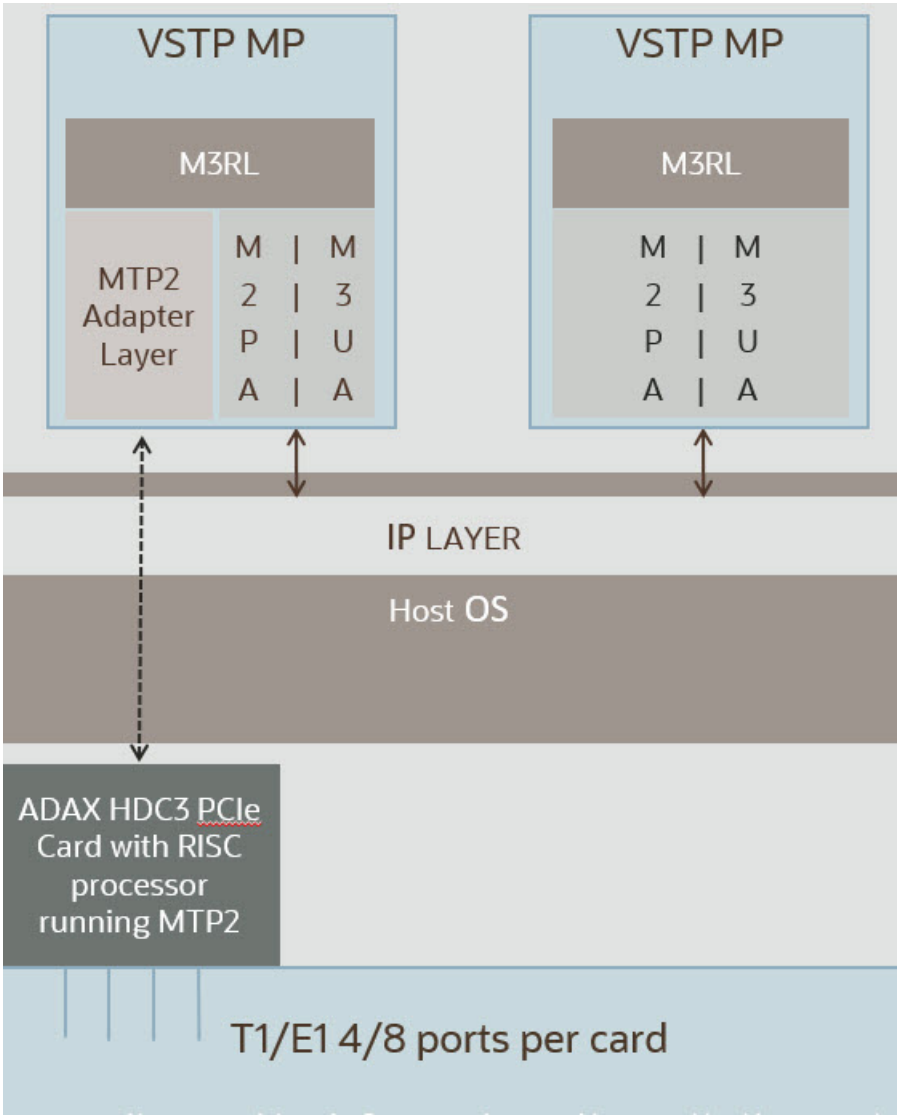
VSTP MP(s) supporting TDM are co-located with TDM card(s) on same host.

MTP2 Adapter layer on VSTP MP communicates with MTP2 Layer running on the Adax HDC3 Card.

M3RL Layer and MTP2 Adapter layer exchange data and link primitives.

The following figure describes the component level diagram for the vSTP TDM setup:

Figure 2-23 vSTP TDM Support Components



2.10.4 TDM Protocol Layers

The vSTP TDM support comprises of the following protocol layers:

- MTP2 Adapter Layer (NIF) - Ingress & Egress
- M3RL Layer
- TDM Interface Mapping

The following sections describe these protocols.

2.10.4.1 TDM Interface Mapping

TDM interface is a logical name given to a specific timeslot within a trunk on a TDM PCIe card. The VSTP MP Host Name, Port and time-slot uniquely identifies a TDM

Interface. The TDM Link Type (E1/T1) and Speed is specified for each TDM link interface.

Following are possible TDM configuration options:

Mode	Type	Time-slot	Speed	Encoding	Framing	CRC4	Timing
E1	LSL	1 to 31	64 or 56 Kbps	Hdb3, Ami	NA	On,Off	Scs , Mcs , Ics
E1	HSL	NA	2.048 Mbps	Hdb3, Ami	NA	On,Off	Scs , Mcs , Ics
T1	LSL	1 to 24	64 or 56 Kbps	B8zs, Ami	Sf, Esf	NA	Scs , Mcs , Ics
T1	HSL	NA	1.536 Mbps	B8zs, Ami	Sf, Esf	NA	Scs , Mcs , Ics

2.10.4.2 M3RL Layer

The M3RL Layer performs all the functionalities specified in ITU-Q.703 & ITU-Q.704. For the Linksets with MTP2 Adapter type, the M3RL layer sends link indications & SS7 traffic to the MTP2 Adapter Layer. M3RL Layer processes the Link Status indications received from the MTP2 Adapter layer.

Upon change of link availability status, the M3RL layer performs following:

- Changeover or changeback procedures.
- Traffic buffering while the Linkset is On-Hold.
- Traffic rerouting upon completion of change back or changeover procedure.
- Congestion management for the links.

2.10.4.3 MTP2 Adapter Layer (NIF)- Ingress and Egress

The MTP2 Adapter Layer runs as an independent thread. It acts as a mediation layer between the M3RL Layer running on vSTP application and the MTP2 layer running on TDM PCIe Card.

The MTP2 Adapter layer has following functions:

- Sending MTP3 data & indications from M3RL Layer to MTP2 layer on TDM PCIe Card.
- Reading MTP3 data from MTP2 layer on TDM PCIe card & sending to M3RL layer.
- Polling the MTP2 Layer on TDM PCIe Card for Link Status update indications & passing on these indications to the M3RL layer.
- Fetching the FSN & BSN numbers from TDM PCIe Card during Link changeover.
- Perform buffer retrieval from MTP2 link buffer on TDM PCIe Card & sending the retrieved buffers to M3RL layer.
- Buffer any unsent messages to MTP2 Layer.

2.10.5 TDM Functionalities

This section describes different functions performed by the TDM support feature in vSTP:

2.10.5.1 Remote Inhibition/Uninhibition of Link

The Remote Inhibit functionality inhibits or uninhibits the Link from far end. This feature is mainly used for maintenance purpose.

The traffic is not routed through an inhibit link. When inhibit message (LIN) is received on vSTP, the link becomes unavailable on MTP3 layer. There is no link state change on MTP2 layer. vSTP sends LIA as acknowledgment for LIN message, confirming that the link is inhibit.

When uninhibit message (LUN) is received on vSTP, the link becomes available on MTP 3 layer. vSTP sends LUA as acknowledgment of LUN message to confirm that the link is uninhibit and the traffic can be routed through that same link.

2.10.5.2 Timer Set

Timer Set is collection is time out values for SS7 timers. Time latency for linksets can be different. Hence different timer sets are required.

vSTP supports timer sets for following layers:

- M2PA
- M3UA
- MTP3
- MTP2

This feature allows a user to configure SS7 timer sets for each layer for specific linkset.

Refer to MMI configuration options for inserting, updating and deleting the timer set.

2.10.5.3 MTP2 Link Congestion

MTP2 Link congestion is derived from the utilization of link transmissionbuffers maintained at MTP2 adaption layer and unacknowledged messages buffered at Adax MTP2 connection queue.

Comcol sysmetric framework is used to track the usage and calculating thresholds. The threshold values for congestion levels are defined in the following table:

Table 2-13 Congestion Threshold Values

Congestion Level	Threshold Level	Onset Threshold	Clear Threshold
3	Critical	95	90
2	Major	85	80
1	Minor	60	50

Based on the congestion level of Links, congestion level of Linkset is derived as per the following formula:

Congestion Level of Linkset = Max (Congestion level of all Links in the linkset)

Based on congestion Level of linkset, congestion level of RSPs with route having the same linkset are derived.

MTP2 Link Congestion Detection

For MTP2 Link Congestion detection, the congestion threshold values are used as per Congestion Threshold Values.

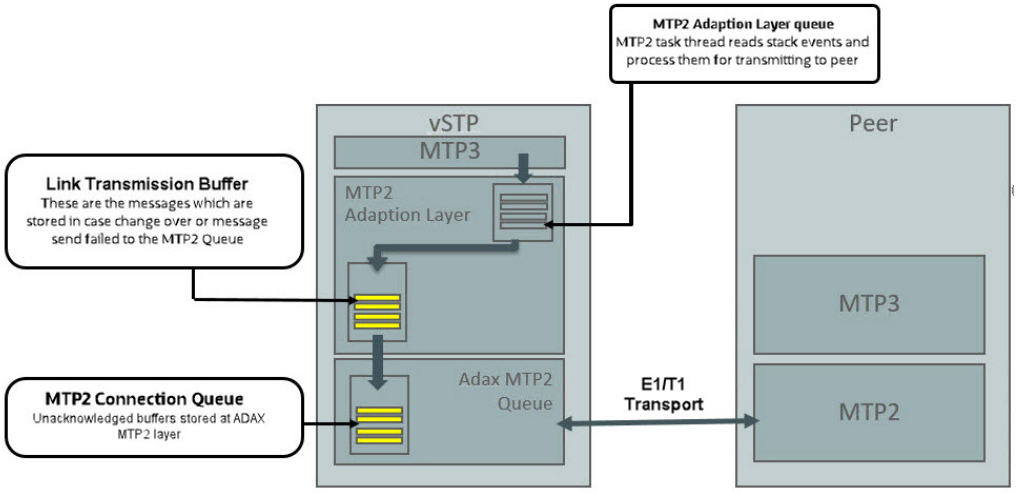
(Link TPS * 2) base is used for the base calculation of the congestion detection.

If sum of Link transmission buffer and MTP2 connection buffer queue utilization percentage is above configured threshold level, then the link is considered as congested.

Example:

Te following figure describes the MTP2 link congestion detection:

Figure 2-24 MTP2 Link Congestion Detection



2.10.5.4 Remote Processor Outage Handling

Remote processor outage (RPO) is a procedure where the processor outage status of the remote signaling point is communicated to the local signaling point.

Handling of RPO

In case of RPO, the following procedure is followed:

1. A notification message is initiated by the RSP to MTP2 layer.
2. After receiving the notification, the MTP2 layer stops sending data messages to remote point and sets the Link state to out of service. It send RPO indication to MTP3 layer.
3. MTP3 layer receives the RPO notification and it starts the change over procedure. If MTP2 received PO recovered message, it send the indication to MTP3 Layer. Once RPO recovered message received at MTP3 Layer , it marks the link as available and initiate the change back procedure.
4. When link comes in-service state, MTP2 starts data message transfer to remote end.

2.10.6 TDM Support Feature Configuration

This section provides procedures to configure the TDM support.

TDM support is configured using the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.10.6.1 MMI Managed Objects for TDM Support

MMI information associated with TDM Support is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for vSTP TDM Support feature:

Table 2-14 vSTP TDM Support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
interfacemappings	Insert, Update, Delete
mtp2board	Display
linksets	Insert, Update, Delete
links	Insert, Delete
mtp3timersetconfigs	Insert, Update, Delete
mtp2timersetconfigs	Insert, Update, Delete

interfacemappings - Insert, Update, Delete

This MO configures the interface channel for an MTP2 Link. This channel is specified while configuring the MTP2 link.

Sample JSON to configure MTP2 interface channel named *channel1*:

```
{
"channelName": "channel1",
"hostName": "rAdax-so1mp2",
"linkType": "T1",
"port": 1,
"speed": "Lsl_56k",
"timeSlot": 1
}
```

To display, execute the MMI Client command from an active SOAM:

```
/vstp/interfacemappings/channel1
```

Example Output:

```
{
"channelName": "channel1",
"hostName": "rAdax-so1mp2",
"linkType": "T1",
"port": 1,
"speed": "Lsl_56k",
"timeSlot": 1
}
```

mtp2board - Display

This REST MO displays the TDM PCIe card configuration on the VSTP MP. Sample output for MTP2 Board Display :

```
{
    "boardType": "HDC3",
    "elt1Port": "4",
    "ethPort": "0",
    "machVer": "4",
    "mrl": "3",
    "pormVer": "15",
    "serialNum": "2558",
    "sourceNode": "rAdax-so1mp1"
}
```

linksets - Insert, Update, Delete

This MO configures the Linkset for a given Adjacent Point Code.

Example JSON to configure Linkset with MTP2 Adapter:

```
{
"enableBroadcastException": false,
"linkTransactionsPerSecond": 100,
"localSignalingPointName": "LSP1",
"name": "Linkset1",
"remoteSignalingPointName": "RSP1",
"type": "Mtp2"
}
```

To display, execute the MMI Client command from an active SOAM:

> **Note:**
>
> Provide name of the link in <LinkName>.

```
/vstp/linksets/<LinkName>
```

Example Output:

```
{
"cgGtmod": false,
"configurationLevel": "135",
"enableBroadcastException": false,
"gttmode": "Fcd",
"ituTransferRestricted": false,
"linkTransactionsPerSecond": 100,
"localSignalingPointName": "LSP1“,
"mtpScrEventLog": true,
"mtpScrSetName": "Set3",
"mtpScrTestMode": false,
"name": "Linkset1",
"remoteSignalingPointName": "RSP1",
"type": "Mtp2"
}
```

links - Insert, Update, Delete

This MO configures link with the given channel.

Sample JSON to configure MTP2 link with MTP2 channel configuration *channel1*

```
{
    "channelName": "channel1",
    "linksetName": " Linkset1 ",
    "name": “Ls1Lnk13",
    "signalingLinkCode": 1
}
```

To display, execute the MMI Client command from an active SOAM:

```
/vstp/links/<LinkName>
```

Example Output:

```
{
    "channelName": " channel1 ",
    "configurationLevel": "24",
    "linksetName": " Linkset1 ",
    "name": " Ls1Lnk13 ",
    "signalingLinkCode": 1
}
```

mtp3timersetconfigs - Insert, Update, Delete

Create a file with the following content:

```
{
   "name": "config1",
```

```
    "sltT1Timer": 8000,
    "sltT2Timer": 35000,
    "sltT17Timer": 2000,
    "t10Timer": 25000,
    "t11Timer": 3000,
    "t12Timer": 800,
    "t13Timer": 800,
    "t15Timer": 600,
    "t16Timer": 800,
    "t17Timer": 800,
    "t18Timer": 3000,
    "t1Timer": 800,
    "t2Timer": 800,
    "t23Timer": 180000,
    "t3Timer": 800,
    "t4Timer": 600,
    "t5Timer": 600,
    "t6Timer": 800,
    "t8Timer": 800
}
```

Execute following command on Active SOAM to insert :

```
/vstp/mtp3TimersetConfig -v POST -r /<Absolute path>/<File Name>
```

Example Output:

```
{
  "data": true,
     "links": {},
     "messages": [],
     "status": true
  }
```

Execute following command on Active SOAM to update :

```
/vstp/mtp3TimersetConfig -v PUT -r /<Absolute path>/<File Name>
```

Example Output:

```
{
     "data": true,
     "links": {},
     "messages": [],
     "status": true
      }
```

Execute following command on Active SOAM to delete:

```
/vstp/mtp3TimersetConfig/<set name> -v DELETE
```

Example Output:

```
No output returned by URI: https://localhost/mmi/dsr/v4.0/vstp/
mtp3TimersetConfig/Mtp3Config1? for 'DELETE' operation
```

To display, execute following command on Active SOAM:

```
/ vstp/mtp3TimersetConfig
```

Example Output:

```
{
 "data": [
{
    "name": "config1",
    "sltT1Timer": 8000,
    "sltT2Timer": 35000,
    "sltT17Timer": 2000,
    "t10Timer": 25000,
    "t11Timer": 3000,
    "t12Timer": 800,
    "t13Timer": 800,
    "t15Timer": 600,
    "t16Timer": 800,
    "t17Timer": 800,
    "t18Timer": 3000,
    "t1Timer": 800,
    "t2Timer": 800,
    "t23Timer": 180000,
    "t3Timer": 800,
    "t4Timer": 600,
    "t5Timer": 600,
    "t6Timer": 800,
    "t8Timer": 800
}
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

mtp2timersetconfigs - Insert, Update, Delete

Create a file with the following content:

```
{
            "name": "Set1",
            "t1Timer": 5000,
            "t2Timer": 5000,
```

```
            "t3Timer": 1000,
            "t4EmergencyTimer": 200,
            "t4NormalTimer": 840,
            "t5Timer": 40,
            "t6Timer": 1000,
            "t7Timer": 200
}
```

Execute following command on Active SOAM to insert :

```
/vstp/mtp2timersetconfigs -v POST -r /<Absolute path>/<File Name>
```

Example Output:

```
{
     "data": true,
     "links": {},
     "messages": [],
     "status": true
      }
```

Execute following command on Active SOAM to update :

```
/vstp/vstp/mtp2timersetconfigs -v PUT -r /<Absolute path>/<File Name>
```

Example Output:

```
{
     "data": true,
     "links": {},
     "messages": [],
     "status": true
      }
```

Execute following command on Active SOAM to delete:

```
/vstp/mtp2timersetconfigs/<set name> -v DELETE
```

Example Output:

```
No output returned by URI: https://localhost/mmi/dsr/v4.0/vstp/
mtp2timersetconfigs/config1? for 'DELETE' operation
```

To display, execute following command on Active SOAM:

```
/vstp/mtp2timersetconfigs
```

Example Output:


```
  {
 "data": [
{
    "name": "Set1",
    "t1Timer": 5000,
    "t2Timer": 5000,
    "t3Timer": 1000,
    "t4EmergencyTimer": 200,
    "t4NormalTimer": 840,
    "t5Timer": 40,
    "t6Timer": 1000,
    "t7Timer": 200
}
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


2.10.6.2 TDM Support Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to the TDM support for vSTP:

Alarm/ Event ID	Name
70001	Link Down
70005	Link Unavailable
70009	Link Congested
70102	MTP3 Ingress Link MSU TPS Crossed
70103	MTP3 Egress Link MSU TPS Crossed
70104	MTP3 Ingress Link Management TPS Crossed
70084	VSTP MTP2 Transmission and Retransmission Buffer Utilization
70220	MTP2 Link admin state change
70221	Failed to send message to TDM driver
70222	Failed to receive message from TDM driver
70223	MTP2 link operational state changed
70224	MTP2 link failed
70225	MTP2 Ingress message discarded
70226	MTP2 Egress message discarded
70227	Received Remote Out Of Service on MTP2 link

For more details related to Alarms and Events, refer to Alarms and KPIs Reference document.

Measurements

The following table lists the measurements specific to the TDM support for vSTP:

Measurement ID	Measurement Name
21800	VstpMtp2LnkOutageDuration
21804	VstpMtp2LnkAvailableDuration
21805	VstpMtp2RxLnkMSUOctets
21806	VstpMtp2RxLnkMSUOctetsForGTT
21807	VstpMtp2TxLnkMSUOctets
21808	VstpMtp2Priority0MsuDiscarded
21809	VstpMtp2Priority1MsuDiscarded
21810	VstpMtp2Priority2MsuDiscarded
21811	VstpMtp2Priority3MsuDiscarded
21813	VstpMtp2RxLnkMSUForGTT
21816	VstpMtp2LnkMaintUsage
21821	VstpMtp2LnkCO
21823	VstpMtp2OOSDuration
21824	VstpMtp2LnkRPODuration
21826	VstpMtp2LnkCumlInhibitDuration
21827	VstpMtp2LnkRemoteInhibitDuration
21828	VstpMtp2RxLnkMSUError
21835	VstpMtp2LnkTotalOutage
21836	VstpMtp2LnkTotalRPOCount
21839	VstpMtp2RxLnkMSUInError
21840	VstpMtp2LnkTotalActiveDuration
21841	VstpMtp2LnkTotalUnAvailableDuration

For more details related to measurements, refer to Measurement Reference document.

2.10.7 Troubleshooting

The following are the troubleshooting scenarios for TDM support:

- **The E1/T1 links do not align properly**
  Do the following to troubleshoot:
  - Verify that the cable is not faulty.
  - Verify the cable connections.
  - Verify that the Adax HDC3 card configuration (in QCXfile) is as per the Interface Mapping configuration.
  - Ensure that the Adax HDC3 card timing source configuration is correct. In case of SUERM errors, modify the timing source.
- **Frequent toggling of the E1/T1 Links**
  Do the following to troubleshoot:
  - Verify that the point codes associated with the linkset are correct.
  - Verify that the link alignment and SLTM timers are correct.

- **Adax HDC3 Card is not detected on a vSTP MP VM**
  Do the following to troubleshoot:
  - Check that the vSTP MP VM and the Adax HDC3 card are co-located on same host machine.
  - Check the Adax HDC3 RPMs.
    The following RPMs are required on vSTP MP VM for configuring Adax HDC3 Card:
  - Adax-LiS-2.21.8-1-RedHat-6.10-x86-64bit.rpm
  - Adax-hdc-1.79-1-RedHat-6.10-x86-64bit-LiS2.21.8-MAJ234.rpm
  - Adax-qcx-1.25-1-Linux-x86-64bit.rpm

Points to Consider

The following points must be considered while configuring TDM:

- The J1 and ATM interfaces are not supported.
- Single vSTP MP VM can support only one 4-Port Adax HDC3 Card.
- An Adax HDC3 card cannot be accessed from Multiple VSTP MP VMs .
- The Adax HDC3 driver components and RPMs needs to be installed separately.
- The DSR patch is required to be applied on vSTP MP VM that is connected to Adax HDC3 card.

2.10.8 Dependencies

The TDM support for vSTP has no dependency on any other vSTP operation.

2.11 Scalability

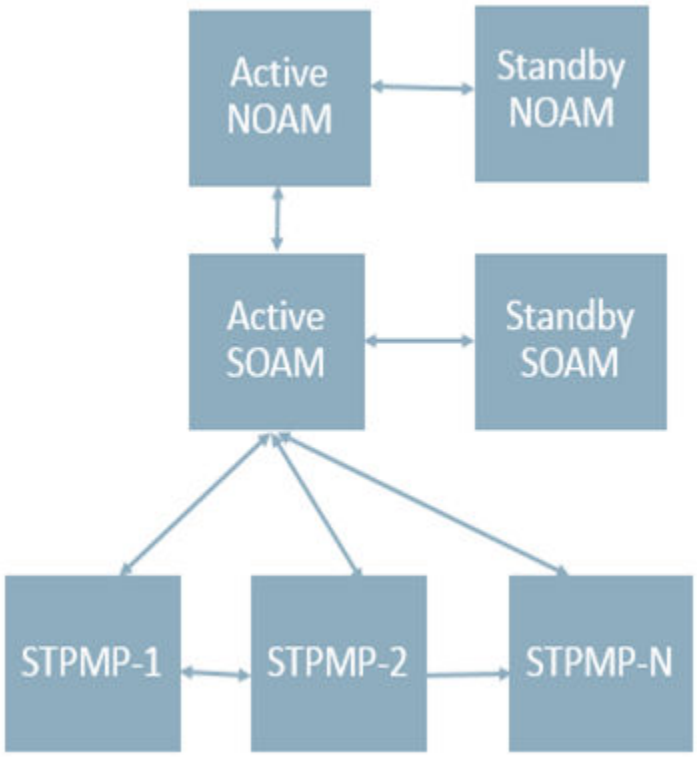
vSTP supports 10K MPS SS7 traffic capacity at the system level. This allows vSTP to support redundancy and diversity at the signaling interfaces. That is, more than one active STP-MP server can support signaling interfaces pointing toward the same remote signaling point.

Topology

vSTP supports two topologies.

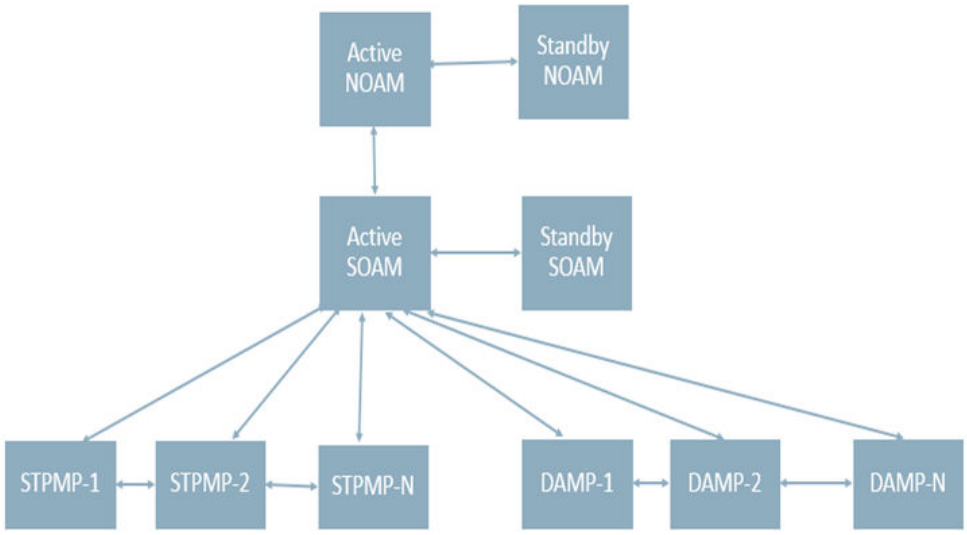
- **Only STP-MP servers in a site**

Figure 2-25 Only STP-MP Site



- **STP-MP and DA-MP servers in a site**

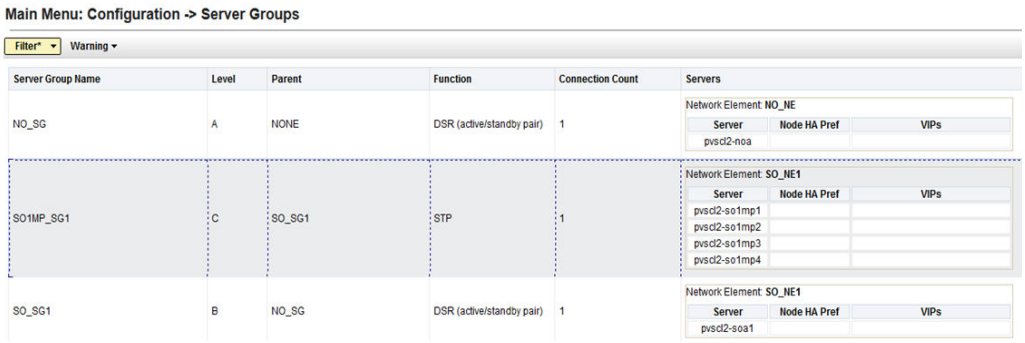
Figure 2-26 STP-MP and DA-MP in a Site



Server Group Configuration

The following table shows multiple STP servers in one server group.

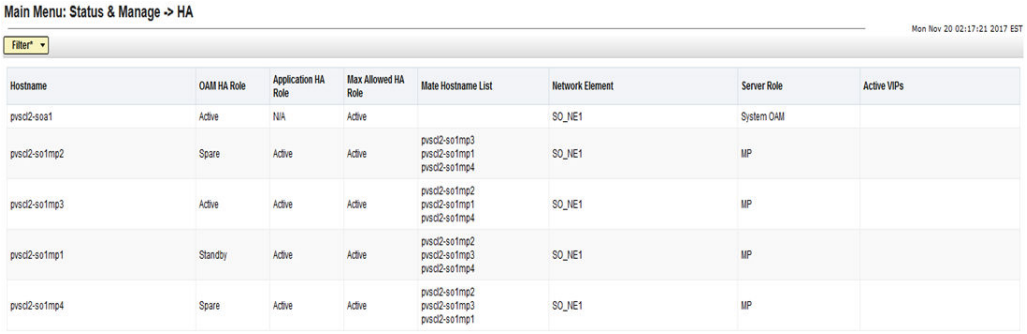
Figure 2-27 Multiple STP Servers in a Server Group



HA Status

The HA role needs to be active for all STP servers as shown in the following table:

Figure 2-28 HA Role for STP Servers



2.12 In-Sequence Delivery of Class 1 UDT Messages

The In-Sequence Delivery of Class 1 UDT Messages provides for the sequencing for both UDT and XUDT Class 1 MSUs. All UDT/XUDT Class 1 messages are routed out in the same order that they were received. To enable the sequencing of UDT/XUDT Class 1 messages, the `class1seq` parameter value of the SCCP options using MMI is set to `on`.

When the `class1seq` parameter value is `off`, load sharing of the UDT/XUDT Class 1 messages is performed using the load sharing configuration in the MAP and MRN tables. The delivery of the UDT/XUDT Class 1 messages in sequence is not guaranteed.

If the messages are not in the correct sequence when they arrive, they are not delivered to the next node in the correct sequence. Message re-sequencing is the responsibility of the originating and destination nodes.

GT-routed Class 0 UDT/XUDT messages are not sequenced.

2.13 SLS Rotation

The Signaling Link Selection(SLS) Rotation feature facilitates a proper distribution of SLS values to provide a good distribution of traffic and load sharing across links and linksets.

In many cases, MSCs, switches and other originating nodes do not send an adequate distribution of SLS values, which results in a poor distribution of traffic across links.

For example, in case of ITU ISUP messages, SLS is obtained from the lower 4 bits of CIC field representing the circuit that is being used. CIC selection can be determined based on an odd or even method where SSP uses either all the odd CICs or all the even CICs to help prevent glaring. This causes Least Significant Bit (LSB) of the SLS to be fixed (0 or 1), which means SSP sends either odd or even SLS. As a result, the transit nodes (STPs) do not achieve a good distribution of traffic across links.

For combined linkset in ANSI and ITU MTP protocols, the LSB of the SLS is used to load share between linksets of a combined linkset and the remaining SLS bits are used to distribute traffic across different links within a linkset. Since, STP receives improper distribution of SLS values (LSB either 0 or 1) the STPs cannot perform proper load sharing across linksets and links of a linkset.

Similarly for single linkset, STPs cannot perform proper load sharing across all links of a linkset, because of receiving improper distribution of SLS values (LSB either 0 or 1).

To overcome this problem, the SLS Rotation feature provides the following SLS Rotation options to users:

- Outgoing Bit Rotation
- Use of Other CIC Bit
- Incoming Bit Rotation
- Random SLS

2.13.1 Outgoing Bit Rotation

If the **Outgoing Bit Rotation** option is configured, the vSTP rotates the 4 bits of SLS according to the outgoing linkset. Thus, changing the LSB of the SLS.

This option can be used as a solution to the problem of vSTP selecting same linkset of a combined linkset. Bit rotation can be used on a per linkset basis to ensure that vSTP does not use static LSB (always 0 or always 1) in the received SLS for linkset selection. It is applicable to all ITU messages.

The **Outgoing Bit Rotation** option enables a user to select the SLS field bit (from 1-4) that must be used as LSB for the linkset selection, while defining a linkset. This rotation during linkset selection affects the 4 bits of SLS selection in the following manner:

- If bit position 4 is selected (`slsrsb` =**4**) for the outgoing linkset, then bit locations 4 3 2 1 are rotated to positions 3 2 1 4.

  For example, SLS = 0110 becomes Rotated SLS = 1100
- If bit position 3 is selected (`slsrsb` =**3**) for the outgoing linkset, then bit locations 4 3 2 1 are rotated to positions 2 1 4 3.

For example, SLS = 0110 becomes Rotated SLS = 1001

- If bit position 2 is selected (`slsrsb` =**2**) for the outgoing linkset, then bit locations 4 3 2 1 are rotated to positions 1 4 3 2.

  For example, SLS = SLS = 0110 becomes Rotated SLS = 0011

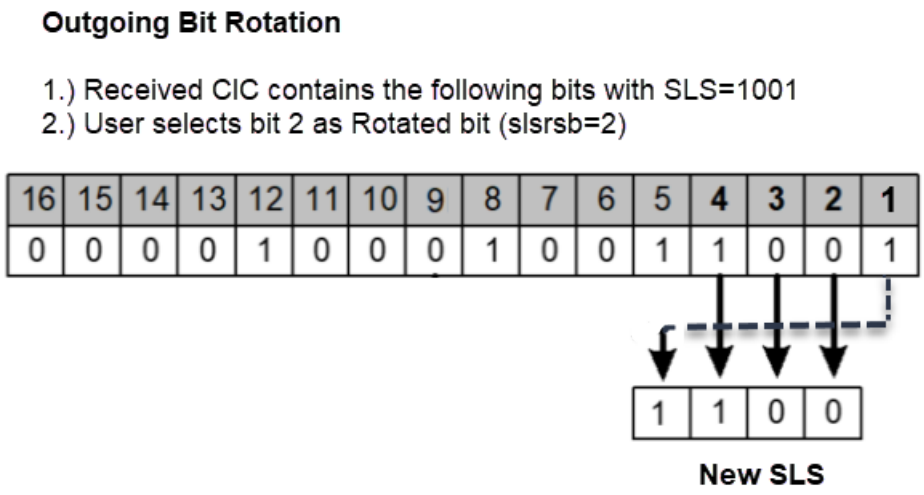
- If bit position 1 is selected (`slsrsb` =**1**) for the outgoing linkset, then no rotation is performed since bit 1 is the existing LSB. Bit **1** is the default value.

  For example, SLS = 0110 remains 0110 only.

Outgoing Bit Rotation Example:

The following figure shows an example of **Outgoing Bit Rotation**:

Figure 2-29 Example: SLS Outgoing Bit Rotation



Note:

- After the SLS is rotated then the existing algorithm for selecting a linkset and signaling link is performed and the message is sent out on the selected link. Note that the SLS is modified only for the link selection algorithm and is not modified in the outgoing message.
- For ITU ISUP messages, SLS is obtained from the lower 4 bits of the CIC field representing the circuit being used. Use of Outgoing bit rotation alone does not guarantee an even distribution of ITU-ISUP messages across all links within a linkset. The vSTP uses all 4 bits of the SLS to determine the actual link to route messages. Since the static bit is simply rotated within the SLS, all possible values of the SLS field will still not be realized. A second option, "Use of Other CIC Bit", must be applied to guarantee even distribution across all links within the linkset.

2.13.2 Use of Other CIC Bit

If the **Use of Other CIC Bit** option is selected, then vSTP derives SLS as per the following rule:

- The bits at positions 2 to 4 of the CIC serve as three lower bits of SLS.
- The Most Significant Bit (MSB) of SLS can be any bit from the bits at position 5 to 16 of the CIC.

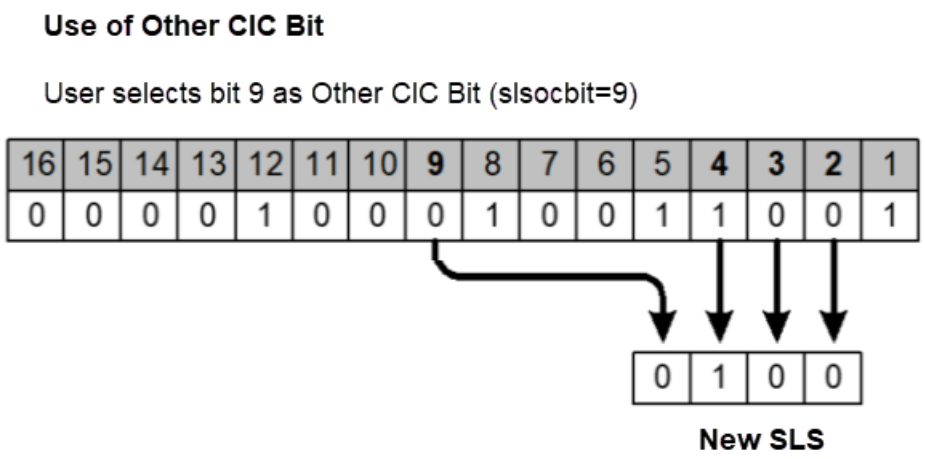
This option can be used as a solution to the problem of vSTP not sharing load between all links within a linkset. It is applicable to ITU ISUP messages.

The **Use of Other CIC Bit** option applies to all ITU ISUP MSUs based on the combination of `slsocbEnabled` and `slsocbit` parameters. User needs to set the value of the `slsocbEnabled` parameter in m3rloptions MO to **true** and configure `slsocbit` in Linkset MO to specify the bit (bits at position 5 through 16 of CIC) to be used as the other CIC bit . The specified bit acts as the MSB of the new SLS and bits at position 2 through 4 of the received CIC become the LSBs of the new SLS. Once the SLS is generated, the existing algorithm for selecting a linkset and signaling link is performed and message is sent out on the selected link.

Use of Other CIC Bit Example:

The following figure shows an example of **Use of Other CIC Bit**

Figure 2-30 Example: SLS Use of Other CIC Bit



2.13.3 Incoming Bit Rotation

If the **Incoming Bit Rotation** option is selected, then vSTP rotates the 4 bits of ITU SLS and 5 or 8 bits of ANSI SLS according to the incoming linkset. Thus, changing the LSB of the SLS.

This option provides additional capability to fairly distribute traffic across links and linksets, however it still does not guarantee an even distribution of messages for all set of input SLS values. It is applicable to all ITU and ANSI messages.

- **ITU Messages**
  For ITU messages, the SLS value is only 4 bits and all 4 bits are considered for rotation. The **Incoming Bit Rotation** is applied on ITU MSUs based on the combination of `islsrsb` and `islsbrEnabled` parameters. User needs to set the value of the `islsbrEnabled` parameter in m3rloptions MO to **true** and configure `islsrsb` in Linkset MO to specify the bit to be used as LSB. This rotation affects the 4 bits of SLS selection in the following manner:
  - If bit position 4 is selected (`islsrsb` =**4**) for the incoming linkset, then bit locations 4 3 2 1 are rotated to positions 3 2 1 4.

    For example, SLS = 1101 becomes Rotated SLS = 1011
  - If bit position 3 is selected (`islsrsb` =**3**) for the incoming linkset, then bit locations 4 3 2 1 are rotated to positions 2 1 4 3.

    For example, SLS = 1110 becomes Rotated SLS = 1011
  - If bit position 2 is selected (`islsrsb` =**2**) for the incoming linkset, then bit locations 4 3 2 1 are rotated to positions 1 4 3 2.

    For example, SLS = 0110 becomes Rotated SLS = 0011
  - If bit position 1 is selected (`islsrsb` =**1**) for the incoming linkset, then no rotation is performed since bit 1 is the existing LSB. Bit **1** is the default value.

    For example, SLS = 0110 remains 0110 only.
- **ANSI Messages**
  The Incoming Bit Rotation is applied on ANSI messages as per the combination of the following parameters.

Table 2-15 Parameters used for Incoming Bit Rotation of ANSI

Parameter Name	Description
`islsbrEnabled`	User needs to set the value of the `islsbrEnabled` parameter in m3rloptions MO to **true**.
`asls8`	Specifies if the adjacent node is sending MSUs with 5 or 8 bits SLS. This parameter value is configured in Linkset MO.
`rsls8`	The inclusion of 5 or 8 bits of SLS in the rotation depends on the value of the `rsls8` parameter in Linkset MO. – If the value is **true**: 8 bits SLS is considered for rotation – If the value is **false**: the least significant 5 bits of SLS are considered for rotation
`slscnv` and `slsci`	The combination of both these parameters with `asls8` decides if 5 to 8 bits SLS conversion option is applied on incoming 5 bits SLS or not. `slscnv` is configured in m3rloptions MO and `slsci` is configured in Linkset MO.
`islsrb`	Configure `islsrsb` in Linkset MO to specify the bit to be used as LSB.

The combination of values provided to these parameters on incoming linkset decides the SLS bits (5 or 8) to be considered for rotation. The following table describes the combination of parameter values with respective rotation rule:

> **Note:**
>
> In below table, the values of **CNV** represents combination of the following parameters:
> **CNV = YES** : (SLSCNV=On) or (SLSCNV= PerLs and SLSCI on the outgoing linkset =true)
>
> **CNV=NO** : (SLSCNV=Off) or (SLSCNV= PerLs and SLSCI on the outgoing linkset =false)

Table 2-16 Rules applied for Incoming Bit Rotation of ANSI

Rule	asls8	rsls8	islsbr	CNV	Incoming SLS Bits Rotation (islsbr)
1	false	false	1-5	NO	The least significant 5 bits of SLS will be considered for rotation.
2	false	false	1-5	YES	The least significant 5 bits of SLS will be considered for rotation.
3	false	true	1-8	NO	No ISLSBR will be performed. **Note:** Enable 5-bit to 8-bit ANSI SLS conversion on outgoing linkset to perform ISLSBR
4	false	true	1-8	YES	The 8-bit SLS value obtained after 5-8 bit conversion is considered for rotation.

Table 2-16 (Cont.) Rules applied for Incoming Bit Rotation of ANSI

Rule	asls8	rsls8	islsbr	CNV	Incoming SLS Bits Rotation (islsbr)
5	true	false	1-5	Has No Impact	The least significant 5 bits of SLS will be considered for rotation.
6	true	true	1-8	Has No Impact	The 8-bits SLS will be considered for rotation.

Incoming Bit Rotation Example:

The following table shows an example of **Incoming Bit Rotation** for ANSI messages:

Incoming ANSI SLS	RSLS8 on incoming linkset	Chosen LSB	Rotated SLS	Applied Rule from **Rules applied for Incoming Bit Rotation of ANSI**
11000110	false	2	11000011	5
01011110	true	7	01111001	6
10010	false	4	**101**01010 **Note:** The highlighted bits indicates the 3 new SLS bits introduced by 5-bit ANSI to 8-bit ANSI SLS conversion.	2
10010	true	8	**01**10010**1** **Note:** The highlighted bits indicates the 3 new SLS bits introduced by 5-bit ANSI to 8-bit ANSI SLS conversion.	4
01101	false	4	10101	1
01101	true	7	No Rotation	3

2.13.4 Random SLS

If the **Random SLS** option is selected, then vSTP randomly generates SLS values. This randomly generated SLS value is then used to select an outgoing linkset and a link in order to achieve load balancing.

This option is applicable to all the ITU SCCP (Class 0 and Class 1), ANSI SCCP Class 0, and ANSI ISUP messages.

For this option, the system-wide `randsls` parameter provides the flexibility to provision Random SLS value as Off, Class0, All (Class0 & Class1), or PerLs . The Per-Linkset `randsls` parameter can provide the additional flexibility to apply Random SLS generation on per linkset basis. User shall be able to provision specific linksets with Random SLS value as Off, Class0, or All (Class0 & Class1).

For ANSI MSUs, `randsls` is applied based on the configuration for ingress linkset . For ITU MSUs, it is applied based on the configuration for egress linkset .

- **ITU Messages**
  For ITU, this option is available system-wide as well as on per linkset basis. The following table describes the rules applied on incoming MSU when **Random SLS** option is selected for ITU:

  Table 2-17 Rules applied for Random SLS for ITU

System-wide randsls (in m3rloptions)	randsls on outgoing linkset	Random SLS
Off	Has No Impact	Random SLS is not applied on any ITU message.
All	Has No Impact	Random SLS is applied on all ITU SCCP messages.
Class0	Has No Impact	Random SLS is applied on all ITU SCCP CLASS0 messages.
PerLs	Off	Random SLS is not applied on any ITU message going through this linkset .
PerLs	All	Random SLS is applied on all ITU SCCP messages going through this linkset .
PerLs	Class0	Random SLS is applied on all ITU SCCP CLASS0 messages going through this linkset .

- **ANSI Messages**
  For ANSI, this option is available on per linkset basis only. The following table describes the rules applied on incoming MSU when **Random SLS** option is selected for ANSI:

  Table 2-18 Rules applied for Random SLS for ANSI

System-wide randsls (in m3rloptions)	randsls on outgoing linkset	Random SLS
Off	Has No Impact	Random SLS is not applied on any ANSI message.
All	Has No Impact	Random SLS is not applied on any ANSI message.
Class0	Has No Impact	Random SLS is not applied on any ANSI message.

Table 2-18 (Cont.) Rules applied for Random SLS for ANSI

System-wide randsls (in m3rloptions)	randsls on outgoing linkset	Random SLS
PerLs	Off	Random SLS is not applied on any ANSI message going through this linkset .
PerLs	All	Random SLS is applied on ANSI SCCP Class0 and ISUP messages going through this linkset .
PerLs	Class0	Random SLS is applied on all ANSI SCCP CLASS0 messages going through this linkset .

> **Note:**
>
> The SLS modified using the above options is used for internal linkset and link selection only. The actual SLS field of the message does not get modified. Therefore, the SLS value received by vSTP remains the SLS value sent out by the vSTP.

2.13.5 Combining SLS Rotation Options

In order to provide an even distribution of ITU and ANSI messages sent by M3RL, vSTP allows to combine the **Random SLS**, **Use of Other CIC Bit**, **Incoming Bit Rotation**, and **Outgoing Bit Rotation** options in the following manner:

ITU Messages

If a user activates the above options for a given linkset, then the ITU SLS field is processed in the following order:

1. If the `randsls` parameter value is set as ON, then 8-bit random SLS is generated.

   > **Note:**
   >
   > Random SLS of ITU is based on either the global option or outgoing linkset parameter. For more details on Random SLS, see SLS Rotation.

2. If the global `slscnv` or `slsci` parameters for outgoing linkset are ON, then the 4-bits ITU SLS is converted to 8-bits SLS using 4-to-8 Bit SLS Conversion option.
3. If it is an ITU-ISUP message, then the least-significant 4-bits of the modified SLS are modified using the **Other CIC Bit** option.
4. The least-significant 4-bits of the modified SLS are modified using **Incoming Bit Rotation** or **Outgoing Bit Rotation**.
5. The modified SLS is used by the existing linkset and link selection algorithms to select a linkset and link.

6. The Message is sent out to the selected link containing the original and unmodified SLS field.

For ANSI Messages

If a user activates these options for a given linkset, then the ANSI SLS field is processed in the following order:

1. If the `randsls` parameter value is set as ON, then 8-bit random SLS is generated.

> **Note:**
>
> Random SLS of ANSI is based on the incoming linkset parameter with the value of global option set as is PerLs. For more details on Random SLS, see SLS Rotation.

2. If RANDSLS is applied and the system-wide `slsreplace` parameter value is true, then the randomly generated SLS is replaced in the MSU and Step 5 is executed.
3. If the global `slscnv` or `slsci` parameters for outgoing linkset are ON, then the 5-bits ANSI SLS is converted to 8-bits SLS using 5-to-8 Bit SLS Conversion option.
4. If **Random SLS** is not applied, then the converted SLS is modified using the **Incoming Bit Rotation** option.
5. The modified SLS is used by the existing linkset and link selection algorithms to select a linkset and link.
6. The SLS is modified using standard 5th bit rotation, replaced in the MSU and sent out to selected link.

2.13.6 SLS Conversion

The Signaling Link Selection(SLS) conversion feature allows vSTP to convert the SLS bits of ITU and ANSI messages. The SLS conversion is applicable to all the MTP-Routed and GT-Routed MSUs.

vSTP supports the following SLS conversions:

- ANSI 5-bit to ANSI 8-bit SLS Conversion
- ITU to ANSI SLS Conversion
- ANSI to ITU SLS Conversion

2.13.6.1 ANSI 5-bit to ANSI 8-bit SLS Conversion

The ANSI 5-bit to ANSI 8-bit SLS Conversion enables a user to perform 5-bit ANSI conversion to 8-bit ANSI. If this conversion option is configured, then the SLS is converted from 5-bit to 8-bit ANSI. The conversion is performed during routing, between linkset and link selection. SLS rotation follows the link selection.

The messages, which satisfy the following conditions can only be converted from 5-bit to 8-bit SLS:

- The incoming and outgoing linksets are SS7 ANSI.
- The incoming linkset has ASLS8=NO .

- The value of the `slsci` parameter is YES and the `slscnv` parameter is PERLs or ON for the outgoing linkset.
- The 3 most significant bits of the SLS are **000**.

If the above conditions are fulfilled, then only the new SLS value is calculated as per the following figure:

Figure 2-31 ANSI 5-bit to ANSI 8-bit SLS Conversion

Calculation of ANSI 5-bit to ANSI 8-Conversion

$SLS_{new} = (((B + rand [P_{low8bits}] + rand [P_{high8bits}]) \bmod 8)) << 5 + SLS_{old}$

Where,

SLS_{new} = 8-bit new SLS value obtained after pre-pending the 3 new bits to the existing SLS value

SLS_{old} = 5-bit ANSI SLS value

B = 3 least significant bits of OPC

$P_{low8bits}$ = lower 8 bits of incoming link

$P_{high8bits}$ = higher 8 bits of incoming link

rand[] = static table filled with random numbers (values do not change after startup)

2.13.6.2 ITU to ANSI SLS Conversion

The ITU to ANSI SLS Conversion enables a user to perform 4-bit ITU to 5-bit ANSI conversion. If this conversion option is configured, then the SLS is converted from 4-bit ITU to 5-bit ANSI.

If ITU 4-bit SLS is *ABCD* then the ANSI 5-bit SLS is calculated as *D (~D) ABC*.

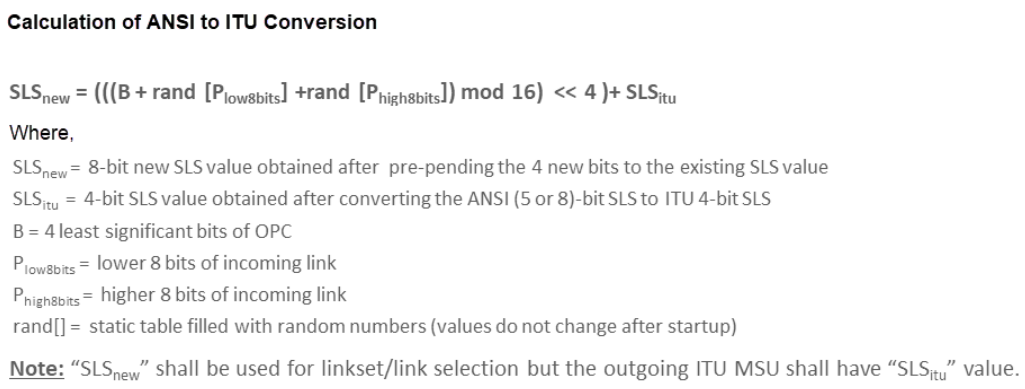
This conversion can further be followed by **ANSI 5-bit to ANSI 8-bit SLS Conversion** in order to achieve more randomization for linkset or link selection during the network conversion.

2.13.6.3 ANSI to ITU SLS Conversion

The ANSI to ITU SLS Conversion enables a user to perform 5-bit or 8-bit ANSI to 4-bit ITU conversion.

For this conversion, the 5 or 8 bit ANSI SLS value is converted to 4-bit ITU SLS value by doing MOD 16. This conversion can further be followed by 4-bit ITU to 8-bit ITU SLS conversion in order to achieve more randomization for linkset or link selection during the network conversion as shown in the following figure:

Figure 2-32 ANSI to ITU SLS Conversion



2.13.6.4 Interaction between SLS Conversion Algorithms

This section describes the interaction of SLS conversion algorithms during network conversion:

- **ITU to ANSI Conversion**
  The following table describes the interaction between different SLS conversion algorithms and the associated outgoing SLSs for ITU to ANSI Conversions:

Table 2-19 Interaction between SLS Conversion Algorithms - (ITU to ANSI Conversion)

randsls	5-bit to 8-bit conversion	islsbr	slsreplace	Bits for Linkset / Link Selection	Outgoing SLS
No	No	No	Has no impact	5 bits obtained after 4-bit ITU to 5-bit ANSI Conversion	5 bits obtained after 4-bit ITU to 5-bit ANSI Conversion
No	No	Yes	Has no impact	Rotated 5 bits	5 bits obtained after 4-bit ITU to 5-bit ANSI Conversion
No	Yes	No	Has no impact	Converted 8 bits	Converted 8 bits
No	Yes	Yes	Has no impact	Converted and rotated 8 bits	Converted 8 bits

Table 2-19 (Cont.) Interaction between SLS Conversion Algorithms - (ITU to ANSI Conversion)

randsls	5-bit to 8-bit conversion	islsbr	slsreplace	Bits for Linkset / Link Selection	Outgoing SLS
Yes	No	No	No	Random 8 bits	5 bits obtained after 4-bit ITU to 5-bit ANSI Conversion
Yes	No	No	Yes	Random 8 bits	Random 8 bits
Yes	No	Yes	Has no impact	NA	NA
Yes	Yes	No	No	Converted 8 bits	Converted 8 bits
Yes	Yes	No	Yes	NA	NA
Yes	Yes	Yes	Has no impact	NA	NA

As per the above table, the following are the key points during ITU to ANSI conversion:

- The `randsls` and `islsbr` parameters are mutually exclusive.
- The `randsls` and **5-bit to 8-bit SLS conversion** are mutually exclusive when `slsreplace` flag is ON.
- The `slsbr` parameter is not applicable for ITU to ANSI network conversions because in case of these conversions, messages are already converted to ANSI by the time `slsbr` is applied. Also, `slsbr` is applicable only for ITU MSUs.
- During ITU to ANSI network conversion, the ingress linkset is ITU, hence the value of `asls8` will always be No. Therefore, if `randsls` is applied after ITU to ANSI network conversion, the outgoing SLS will be of 5 or 8 bits, depending on the values of the m3rloptions,`slsreplace` and LINKSET(EGRESS), `slsci` /m3rloptions, or `slscnv` parameters.

- **ANSI to ITU Conversion**

The following table describes the interaction between different SLS conversion algorithms and the associated outgoing SLSs for ANSI to ITU Conversions:

Table 2-20 Interaction between SLS Conversion Algorithms - (ANSI to ITU Conversion)

randsls	4-bit to 8-bit conversion	islsbr/slsbr	Bits for Linkset /Link Selection	Outgoing SLS
No	No	No	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion
No	No	Yes	Rotated 4 bits	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion
No	Yes	No	Converted 8 bits	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion
No	Yes	Yes	Converted and rotated 8 bits	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion
Yes	No	No	Random 8 bits	4 bits obtained after 5-bit to 4-bit or 8-bit to 4bit ANSI-ITU SLS Conversion
Yes	No	Yes	NA	NA
Yes	Yes	No	NA	NA
Yes	Yes	Yes	NA	NA

As per the above table, the following are the key points during ANSI to ITU conversion:

- The `randsls` and `islsbr/slsbr` parameters are mutually exclusive.
- The `randsls` and **4-bit to 8-bit SLS conversion** are mutually exclusive.

2.13.7 SLS Rotation Feature Configuration

This section provides procedures to configure the SLS Rotation feature.

SLS Rotation requires the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.13.7.1 MMI Managed Objects for SLS Rotation

MMI information associated with SLS Rotation functionality is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for vSTP SLS Rotation feature:

Table 2-21 vSTP SLS Rotation Managed Objects and Supported Operations

Managed Object Name	Supported Operations
m3rloptions	Update
linksets	Insert, Update, Delete

m3rloptions - Display, Update

Execute the following command on Active SOAM to display table data:

```
/vstp/m3rloptions
```

Sample Output:

```
{
"cnvAInat": 1,
"cnvCgda": true,
"cnvCgdi": true,
"cnvCgdn": false,
"cnvCgdn24": false,
"cnvClgItu": "Off",
"gtCnvDflt": true,
"islsbrEnabled": false,
"lsOnHoldTimer": 60,
"randsls": "Off",
"slsRotation": true,
"slscnv": "Off",
"slsocbEnabled": false,
"slsreplace": false,
"sltT1Timer": 12000,
"sltT2Timer": 30000,
"sparePCSupportEnabled": true,
"t10Timer": 30000,
"t11Timer": 30000,
"t15Timer": 3000,
"t16Timer": 1400,
"t17Timer": 2000,
"t18Timer": 10000,
"t1Timer": 800,
"t2Timer": 1400,
"t3Timer": 800,
"t4Timer": 800,
"t5Timer": 800,
"t6Timer": 800,
"t8Timer": 800
)
```

To update:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
{
        "randsls": "Off",
        "slsRotation": true,
        "slscnv": "Off",
        "slsocbEnabled": false,
        "slsreplace": false
 }
```

Execute the following command on Active SOAM to update the data:

```
        /vstp/m3rloptions –v PUT –r /<Absolute Path>/<File Name>.json
```

linksets - Insert, Update, Delete

Execute the following command on Active SOAM to display table data:

```
/vstp/linksets
```

Sample Output:

```
{
"asNotification": true,
"asls8": false,
"cgGtmod": false,
"configurationLevel": "1428",
"enableBroadcastException": false,
"gttmode": "Sysdflt",
"islsrsb": 1,
"ituTransferRestricted": false,
"l2TimerSetName": “AnsiDefault",
"l3TimerSetName": "Default",
"linkTransactionsPerSecond": 100,
"localSignalingPointName": "LSPI15",
"numberSignalingLinkAllowedThreshold": 0,
"numberSignalingLinkProhibitedThreshold": 0,
"randsls": "Off",
"remoteSignalingPointName": "RSP16",
"name": "LS7114",
"rsls8": false,
"slsci": false,
"slsrsb": 1,
"type": "M2pa“
}
```

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
{
    "islsrsb": 1,
    "randsls": "Off",
    "rsls8": false,
    "slsci": false,
    "slsrsb": 1,
    "linkTransactionsPerSecond": 1200,
    "localSignalingPointName": "LSPI15",
    "name": "LS7114",
    "remoteSignalingPointName": "RSP16",
    "type": "M2pa"     }
```

Execute this command on an active SOAM to insert:

```
/vstp/linksets –v POST –r /<absolute path>/<file name>
```

This MO configure the Linkset for a given Adjacent Point Code.

Execute this command on an active SOAM to update:

```
/vstp/linksets –v PUT –r /<absolute path>/<file name>
```

Execute this command on an active SOAM to delete:

```
/vstp/linksets/<Linkset Name> –v DELETE
```

2.13.7.2 Configuring SLS Rotation Through vSTP GUI

The SLS Rotation functionality can be configured from Active System OAM (SOAM). Select **VSTP > Configuration** page.

The following parameters must be configured in the **Link Set** option:

- Incoming SLS Rotated Signaling Bit
- Random SLS
- Rotate SLS by 5 or 8 bits
- SLS Conversion Indicator
- Rotated SLS Bit
- Other CIC Bit

For more details related to these parameters, see Link Sets.

The following parameters must be configured in **M3rlOptions**:

- Incoming SLS Bit Rotation
- Linkset On Hold timer

- Randsls
- Signaling Link Supervision Timer
- Signaling Link Interval Time
- SlsRotation
- Slscnv
- SlsReplace

For more details related to these parameters, see M3rl Options.

2.13.7.3 SLS Rotation Alarms and Measurements

There are no alarms, events, or measurements specific to the SLS Rotation functionality.

The **vSTP Link Performance** and **vSTP Link Usage** measurements are pegged during message routing of egress messages. For more details related to these measurements, refer to Measurement Reference document.

2.13.8 Troubleshooting

The troubleshooting scenarios for SLS Rotation:

- If no SLS Rotation algorithm is applied.
  - Ensure that correct parameters are set on ingress and egress Linkset connected to vSTP MP as per SLS Rotation Algorithm.
  - Ensure that appropriate m3rloptions MO parameters are set.
  - SLS Rotation algorithms are specific to domain and type of message such as, SCCP or ISUP. Therefore, the configurations must be done accordingly. For example, Algorithm Use of Other CIC bit is applicable only for ITU ISUP messages.
- If ANSI SLS in Egress Message is not correct as per the SLS Rotation Algorithm applied:
  - Consider that for ANSI domain, the standard 5th Bit Rotation is always applicable and it is modified in Egress Message.
- If SLS Rotation on Domain Conversion is not working properly:
  - Few parameters can be set on Linksets, therefore while performing domain conversion, ensure that you specify the correct parameter values to get desired output.
  - For ANSI, check value of parameter ASLS8 in incoming linkset.
  - Consider that the interaction between different algorithms of SLS Rotation during domain conversion has certain exceptions.
  - For more details, see Interaction of SLS Conversion algorithms during network conversion.
- If certain SLS Algorithm does not get applied.
  - When multiple algorithms are applied to a particular domain message type, the SLS Rotation algorithms are applied as per points mentioned in slide 31 and 32. Combining SLS Rotation Options.

- Modifying SLS Rotation related parameter values can render one of SLS Rotation Algorithm as inapplicable. Revert the modified parameter values to return to the previous manner of load sharing.
- Contact My Oracle Support (MOS) if the problem persists.

2.13.9 Dependencies

The SLS Rotation feature for vSTP has no dependency on any other vSTP operation.

The following points must be considered for SLS Rotation functionality:

- Usage of 5th bit as LSB for incoming bit rotation must be avoided if all the nodes are GR compliant. This is due to the fact that ANSI mandated outgoing 5 bit rotation causes the 5th bit to not have a uniform distribution of 0's and 1's.
- If 5 to 8 Bit Conversion is applied on incoming 5 bit SLS, then 3 new SLS bits (calculated based on the OPC) are prefixed to the 5-bit SLS. If all 8 SLS bits are considered for applying ISLSBR, the 3 new SLS bits become sticky bits and cause uneven distribution. In this scenario, ISLSRSB value 6-8 cause even more uneven distribution.
- If 5 bits SLS is received on incoming linkset, 5 to 8 bit conversion is OFF on outgoing linkset, and 8 bits SLS are considered for applying ISLSBR, then no rotation happens. The 5 to 8 Bit Conversion option must be turned ON to perform ISLSBR.
- When two linksets are used as a combined linkset, they should have the same settings for all SLS algorithms (For example, Other CIC Bit, Rotated SLS Bit), otherwise there can be a random behavior. This is not enforced in vSTP , and there is no warning mechanism for incorrectly provisioned linksets and routes.
- Different RANDSLS configurations on two linksets , which happen to be a part of combined linkset for the routes defined for a destination node may result in undesired SLS distribution. vSTP does not prompt or reject the linkset provisioning command if the provisioning is done contrary to the above.
- For different segments of the same MSU, randsls generates different SLS and different link selection. For other SLS algorithms, it is assumed that the Incoming linkId or SLS is same for different segments of the same MSU, hence the outgoing linkId or linkset id will be same for different segments of the same MSU.

2.14 Segmented XUDT Support

The Segmented XUDT feature allows vSTP to perform the following operations:

- Reassembly of incoming XUDT Class 1 SCCP segmented messages
- Segmentation of the outgoing XUDT Class 1 SCCP reassembled messages

This functionality ensures that all segments of the SCCP Class 1 XUDT messages are routed to same destination, irrespective of the service used for translation.

vSTP performs reassembly on the incoming segmented XUDT messages. After the reassembly, the required services or translation is performed on the reassembled message.

The segmentation is performed on the outgoing XUDT reassembled message to generate segments and perform routing.

For more details, see

2.14.1 Reassembly

Reassembly is process of assembling segments that belongs to same message at destination SCCP. The segments associated to same message are uniquely identified by the reassembly key.

A reassembly key includes the following fields:

- MTP Routing Label (OPC, DPC, SLS)
- Calling Party Address
- Segmentation Local Reference (Unique number generated by originator SCCP and included in `Segmentation` parameter.

When the first segment of an MSU sequence is received, a reassembly timer `TReassembly` is started.

The destination SCCP ensures the following:

- The segments are reassembled in correct segmentation order and if out of order segments are received, then reassembly must stop and reassembly error procedure is applied.
- Reassembly process completes in a definite amount of time governed by timer `Treassembly`. In case of failure in completing within the time, the reassembly stops and reassembly error procedure is applied.

2.14.1.1 Error Handling during Reassembly

The reassembly errors must be handled as follows:

- When a reassembly procedure fails and `alwMsgDuringRsmblyErr` in the sccpoptions MO is **True**, then all the received segmented MSUs of the message are passed for further processing.
- When a reassembly procedure fails and `alwMsgDuringRsmblyErr` in the sccpoptions MO is **False**:
  - If `return on Error` option is set in the XUDT Message received, then only one XUDT with data = first segment data received and the XUDTS is sent to the originator.
  - If `return on Error` option is not set in the XUDT Message received, then the message is discarded.

2.14.2 Segmentation

The segmentation functionality is the process of segmenting the reassembled message into segments. Segmentation is performed only on the reassembled messages, provided the length of the reassembled message is greater than `Configured Segmented MSU length` The value of this parameter can be configured using the parameter`segmentedMSULength` defined in the sccpoptions MO.

Maximum number of segments supported is 16. While segmenting, if the number of required segments is greater than 16, then XUDTS is generated. However,

if the `return on error` option is set in the reassembled message, the reassembled message gets discarded. The segmentation failure event is generated and measurement is pegged.

2.14.3 Segmented XUDT Feature Configuration

This section provides procedures to configure the Segmented XUDT feature.

Segmented XUDT requires the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.14.3.1 MMI Managed Objects for Segmented XUDT Support

MMI information associated with Segmented XUDT feature is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* gets opened, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for Segmented XUDT feature:

Table 2-22 Segmented XUDT Managed Objects and Supported Operations

Managed Object Name	Supported Operations
sccpoptions	IUpdate, Delete

sccpoptions - Display, Update

Execute the following command on Active SOAM to display table data:

```
/vstp/sccpoptions
```

Sample Output:

```
{
    "data": {
        "alwMsgDuringRsmblyErr": true,
        "class1seq": "Disabled",
        "dfltfallback": false,
        "dfltgttmode": "Cd",
        "isSegXUDTfeatureEnable": true,
        "mtprgtt": "Off",
        "mtprgttfallback": "Mtproute",
        "reassemblyTimerDurationAnsi": 5000,
        "reassemblyTimerDurationItu": 10000,
        "segmentedMSULength": 200,
        "tgtt0": "None",
        "tgtt1": "None",
        "tgttudtkey": "Mtp",
        "tgttxudtkey": "Mtp",
        "travelVelocity": 700
    },
```

```
    "links": {
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v3.1/vstp/sccpoptions/",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
```

To update:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
{
        "alwMsgDuringRsmblyErr": false,
        "isSegXUDTfeatureEnable": false,
        "segmentedMSULength": 250
}
```

Execute the following command on Active SOAM to update the data:

```
/vstp/sccpoptions -v PUT –r /<Absolute path>/<File Name>
```

Sample Output:

```
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

2.14.3.2 Configuring XUDT Segmentation Through vSTP GUI

The XUDT Segmentation functionality can be configured from Active System OAM (SOAM). Select **VSTP > Configuration** page.

The following parameters must be configured in the **SCCP Options** option:

- XUDT Segmentation feature
- Reassembly timer duration for ANSI
- Reassembly timer duration for ITU
- Allow Msg During Rsmbly Err
- Length of Segmented MSU

For more details related to these parameters, see SCCP Options.

2.14.3.3 XUDT Segmentation Alarms and Measurements

Alarms and Events

The following table lists the Alarms and Events specific to the XUDT Segmentation support for vSTP:

Alarm/ Event ID	Name
70331	SCCP XUDT Reassembly Failure
70332	SCCP XUDT Segmentation Failure

For more details related to Alarms and Events, refer to Alarms and KPIs Reference document.

Measurements

The following table lists the measurements specific to the XUDT Segmentation support for vSTP:

Measurement ID	Measurement Name
21902	VstpRxSccpReassProcFail
21903	VstpRxSccpXUDTSgmnts
21904	VstpRxSccpSgmntsDisc
21905	VstpRxSccpSgmntsReassFail
21906	VstpTxSccpSegProcSucc
21907	VstpTxSccpSegProcFail
21908	VstpTxSccpLargeMsgs
21909	VstpRxSccpReassSegSucc
21901	VstpRxSccpReassProcSucc

For more details related to measurements, refer to Measurement Reference document.

2.14.4 Troubleshooting

The troubleshooting steps for vSTP XUDT Segmentation feature are as follows:

- If a Segmented Class 1 XUDT message is received for reassembly, then the measurement **VstpRxSccpXUDTSgmnts** is pegged to count the Number of ingress segmented XUDT messages received from network.
- If the reassembly procedure is successful, then the measurement **VstpRxSccpReassProcSucc** is pegged to count the Number of times reassembly procedure completed successfully.
- If the reassembly procedure is successful, then the measurement **VstpRxSccpReassSegSucc** is pegged to count the Number of Segmented XUDT Messages reassembled successfully.
- If the reassembly procedure fails, then the measurement **VstpRxSccpReassProcFail** is pegged to count the number of times reassembly procedure failed.

- If the reassembly procedure fails, then the measurement **VstpRxSccpSgmntsReassFail** is pegged to count the Number of segmented XUDT messages that encountered Reassembly failure due to any errors.
- If the reassembly procedure fails, then the measurement **VstpRxSccpSgmntsDisc** is pegged to count the Number of segmented XUDT messages Discarded, this measurement is pegged if **alwMsgDuringRsmblyErr** in the sccpoptions MO is **False**.
- If a reassembled message is received for segmentation then the measurement **VstpTxSccpLargeMsg**s is pegged to count the number of reassembled large messages received for segmentation.
- If the segmentation procedure is successful, then the measurement **VstpTxSccpSegProcSucc** is pegged to count the number of times segmentation procedure completed successfully.
- If the segmentation procedure fails, then the measurement **VstpTxSccpSegProcFail** is pegged to count the number of times segmentation procedure failed.
- If reassembly procedure fails, then check the event **SCCP XUDT Reassembly Failure** is raised in the vSTP GUI with the following reasons:
  - **out of sequence segments received**
  - **reassembly Timer Expired**
  - **Internal Error**

  If the reassembly failure occurs due to reassembly Timer Expiry, then user may need to adjust the value of the parameter **reassemblyTimerDurationAnsi** or **reassemblyTimerDurationItu** defined in sccpoptions MO.
- If segmentation procedure fails, then check the event SCCP XUDT Segmentation Failure raised in the vSTP GUI. The event is raised with the reason **number of required segments is greater than the maximum number of segments**. In case of this error, adjust the value of **segmentedMSULength** parameter in sccpoptions MO.

Contact My Oracle Support in case the problem persists.

2.14.5 Dependencies

The XUDT Segmentation feature has no dependency on any other vSTP operation.

The following points must be considered for XUDT Segmentation functionality:

- Segments of the same message received on different vSTP MPs (as result of CO or CB or any other scenario) are not completely supported. The reassembly error procedure will be initiated for such messages.
- Reassembly is performed for only segmented XUDT Class 1 messages. Segmentation functionality will be performed only on the reassembled messages(performed by vSTP).
- XUDT Reassembly functionality is not supported for Route on SSN messages.

2.15 Duplicate Point Code Support

The Duplicate Point Code support functionality allows vSTP to route traffic for two or more countries that may have overlapping point code values.

The users divide their ITU-National or Spare destinations into groups. These groups are based on the country. When the user enters an ITU National or Spare point code, they must also enter the group code to associate point code with groups. A group code is unique two letter code to identify a group.

2.15.1 ITU Point Code Support Functionality

When an ITU-N message arrives at vSTP, an internal point code based on the 14 bit PC is created in the message. Also, the group code gets assigned to the incoming linkset. The following points must be considered while configuring the Duplicate Point Code functionality:

- If the user does not assign any group code while adding ITU-N nodes (Local Signalling Point or Remote Signalling Points), then by default the **aa** group code is assigned.
- For every group that is used, either a True PC or secondary point code must be provided using the Local Signalling Point command.
- When a message is received from M3UA, then the group code is determined by the network appearance present in the message.

2.15.1.1 Operations for MTP3 and SCCP Management Messages

When vSTP receives a network management message concerning an ITU-National or Spare destination, the routeset to apply the message is determined based on the concerned point code and the group code of the message.

When vSTP generates MTP and SCCP management messages that concern an ITU-National or Spare destination, then only the messages with the same group code are sent to point codes.

When M3UA receives a management message (DAVA, DUNA), then the group code is determined by the **NA** present in the message.

2.15.1.2 Interaction

ITU-International linksets do not have a group code. ITU-National or Spare MSUs received on ITU-International linksets are assigned a group code of **aa**.

Gateway Screening has no impact of group codes support. However, the user can effectively screen on group codes by assigning a different screenset to linksets that have different group codes.

Each ITU-N destination and group code can have it’s own ITU-I or ANSI alias PC. Each ITU-I or ANSI node can be assigned one ITU-N destination. For conversion from ITU-I or ANSI to ITU-N to succeed, the ITU-N alias of the sending node must have the same group code as the destination group code. So each ITU-I or ANSI node can only send and receive messages from one ITU-N group.

2.15.2 ITU Duplicate Point Code Support Configuration

This section provides procedures to configure the ITU Duplicate Point Code Support feature.

ITU Duplicate Point Code Support requires the vSTP managed objects. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.15.2.1 MMI Managed Objects for Duplicate Point Code

MMI information associated with Duplicate Point Code feature is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* gets opened, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for Duplicate Point Code feature:

Table 2-23 Duplicate Point Code Managed Objects and Supported Operations

Managed Object Name	Supported Operations
localsignalingpoints	Insert
remotesignalingpoints	Inser, Update, Delete
networkappearances	Insert

localsignalingpoints - Display, Update

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat lsp.json
{ "ss7DomainType": "Itun",
"configurationLevel": "0",
"pcType": "Spc",
"mtpPointCode": "2057",
"name": "lsp1111","groupCode":"bb“
}
```

Execute the following command on Active SOAM to update the data:

```
/vstp/localsignalingpoints -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:

```
{
"data": [
{
"configurationLevel": "384",
"groupCode": “bb",
```

```
"mtpPointCode": "2057",
"name": "lsp111",
"pcType": "Tpc",
"ss7DomainType": "Itun"
},
],
"links": {},
"messages": [],
"status": true
}
```

> **Note:**
>
> In case no value is provided for the `group id` parameter, then default value **aa** is assigned.

remotesignalingpoints - Insert, Update, Delete

Execute the following command on Active SOAM to display table data:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat rsp.json
{"configurationLevel": "0",
"name": "psps111",
"ss7DomainType": "Itun",
"mtpPointCode": "4114",
"enableBroadcastException": true,
"groupCode": "pp"
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/remotesignalingpoints -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:

```
{
"data": [
{
"configurationLevel": "385",
"enableBroadcastException": true,
"groupCode": “pp",
"mtpPointCode": "4114",
"name": "psps111",
"nprst": "Off",
"rcause": "None",
"splitiam": "None",
"ss7DomainType": "Itun"
}
],
```

```
"links": {},
"messages": [],
"status": true
}
```

> **Note:**
>
> In case no value is provided for the `group id` parameter, then default value **aa** is assigned.

networkappearances - Insert

Execute the following command on Active SOAM to display table data:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat na.json
{
"name": "Na2",
"na": 10,
"naType": "Itun",
"groupCode": "ab"
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/ networkappearances -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:

```
/vstp/networkappearances
{
"data": [
{
"groupCode": "aa",
"na": 10,
"naType": "Itun",
"name": "Na2"
}
],
"links": {},
"messages": [],
"status": true
}
```

2.15.2.2 Configuring Duplicate Point Code Support Through vSTP GUI

The Duplicate Point Code functionality can be configured from Active System OAM (SOAM). Select **VSTP > Configuration** page.

The **Group Code** parameter must be configured in the **Local Signalling Points** and **Remote Signalling Points** options.

For more details related to these parameters, see Local Signaling Points and Remote Signaling Point.

2.15.2.3 Alarms and Measurements

There are no alarms, events, or measurements specific to the Duplicate Point Code functionality. However, the existing vSTP alarms and measurements are pegged during the Duplicate Point Code operations.

2.15.3 Troubleshooting

There are no alarms or measurements specific to Duplicate Point Code support functionality. However, different vSTP alarms and measurements are pegged in case of general error scenarios.

2.15.4 Dependencies

The Duplicate Point Code support feature has no dependency on any other vSTP operation.

Considerations

The following points must be considered while configuring Duplicate Point Code functionality:

- The Duplicate Point Code support is applicable only for ITU-National/ITU-Spare Destinations.
- The ITU-National traffic from a group must be destined for a PC within the same group.
- No duplicate point codes are allowed within a group.
- It is not possible to change the group code for a destination. To move a destination from one group to another, user must provision a new destination that uses the new group code and delete the old destination.
- If conversion between ITU-N and ITU-I or ANSI is used, then only one ITU-N group can send traffic to a specific ANSI or ITU-I node.

2.16 Support for CAT2 SS7 Security

The CAT2 SS7 Security functionality allows vSTP to detect anomalies on inbound Category 2 packets through bulk upload of customer IR.21 documents.

> **Note:**
>
> The IR.21 document contains operator wise network information such as, MCC-MNC, Node GT (HLR/VLR/MSC), and CC-NDC.

2.16.1 Feature Overview

vSTP provides the IR.21 Utility to read and record the information present in GSMA IR.21 document.

The SCPVAL GTT Action addresses the SS7 CAT2 security checks. This GTT action ensures that the MSU details such as, CGPA and IMSI belongs to same operator after validating it with the newly generated table.

The CAT2 SS7 functionality is described as follows:

The IR.21 xml file is parsed through IR.21 utility. The information required for message validation is extracted from the file. The data is stored in vSTP tables.

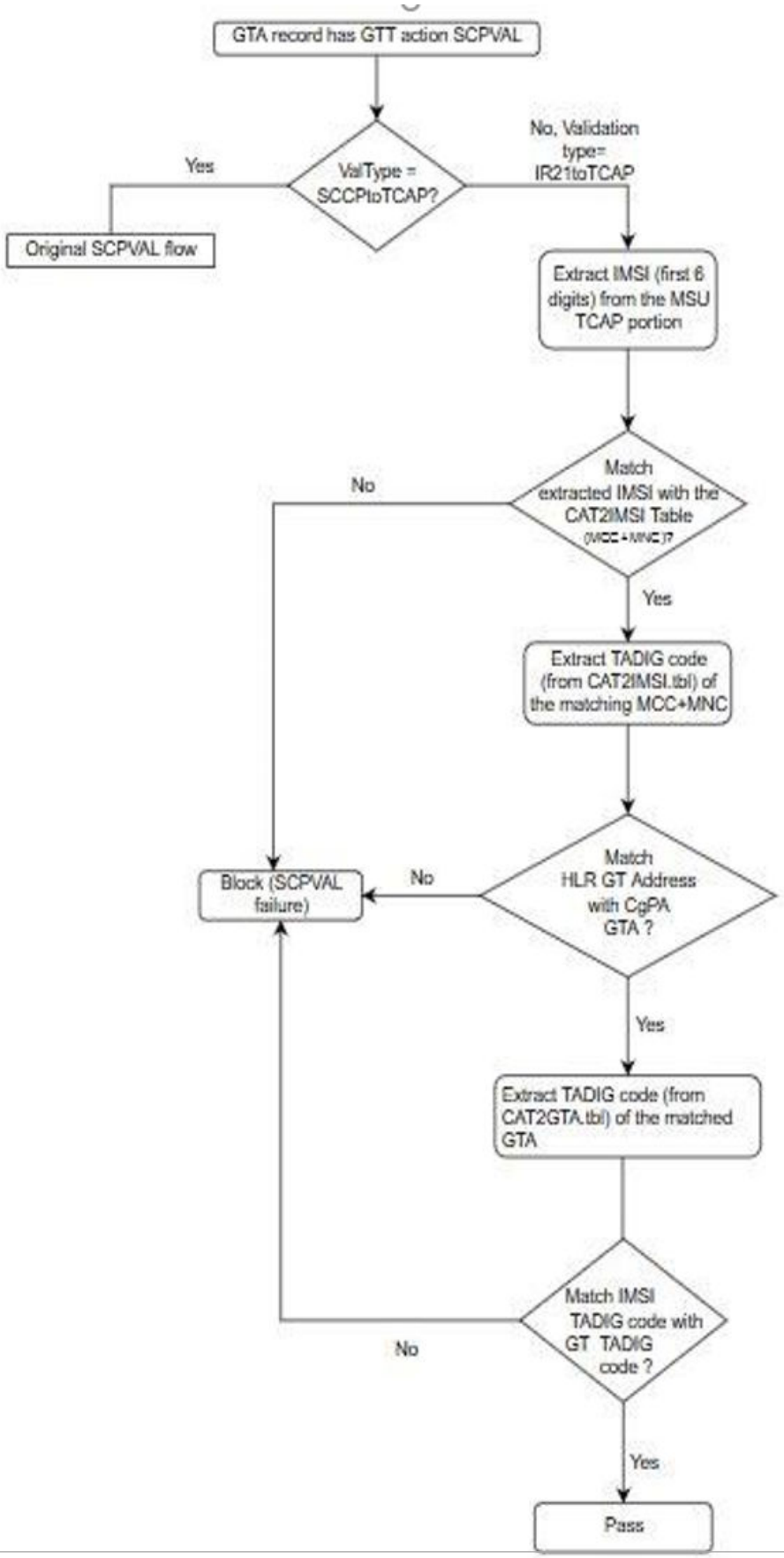
> **Note:**
>
> The information can also be populated using MMIs. However, it is not the preferred method.

The GTT is configured to enforce CAT 2 validation on the received MSUs.
The validation is performed based on the data available in IR21RoutingInfo and IR21NetworkElement tables.

CAT2 SS7 Security Workflow

The following flow chart provides an overview of the CAT2 SS7 Security functionality:

Figure 2-33 CAT2 SS7 Security Workflow



The CAT2 SS7 Security functionality is described as follows:

- **Conversion of IR21 xml file**
  - vSTP provides the IR21 Utility on SOAM. The IR21 Utility accepts operator IR21 input file in XML format and generate error message in case of no or other than IR21 XML files.
  - The output is generated in the form of two CSV files named `IR21NetworkElement.csv` and `IR21RoutingInfo.csv`.
  - The enteries in the CSV files have length based validation for all fields. For example, sender TADIG code and TADIG code must be of 5 digits, IMSI must be of 6 digits, Node Type must be of 1 digit, GT Address range must be of 15 digits.
  - The `IR21NetworkElement` table stores value 0 for HLR and 1 for MGT. Therefore, no validation is performed on this value.

> **Note:**
>
> The IR21 utility supports parsing of 1000 IR.21.xml input files in alphabetical order in an instance. For more details on IR21 Utility, see GUI Configurations for CAT2 SS7 Security Support.

- **Bulk upload after conversion**
  The generated CSV files are imported using the **Import** option under **Diameter Common** on SOAM.

  The following data is extracted from IR21 file and stored on vSTP:
  - Sender TADIG code (RAEX IR.21 Information) : It is retrieved from the RAEX IR21 FileHeader tag and used to identify the operator. It consist of two fields, with a total length of five characters consisting of three-character country code and a two character operator or company idenfier. Sender TADIG code is stored against each entry.
  - Routing Information Data (Section ID 4) : It is a mandatory section in IR21 document of the operator. The vSTP `IR21RoutingInfo` table stores the MCC-MNC (E.212) along with TADIG code from this section. The vSTP `IR21NetworkElement` stores the CC-NC (from E.214) along with TADIG code from this section.
  - Network Element Information Data (Section ID 13) – It is an optional section in IR21 document of the operator. The vSTP `IR21NetworkElement` table stores the HLR Node type GT address or Address range along with the TADIG code from this section.
- **Validation**
  The SCPVAL GTT action validates that the MSU details: CgPA and IMSI belongs to same operator. The validation is performed using the data available in `IR21RoutingInfo` and `IR21NetworkElement` tables.

  The following OPCODES are applicable for CgPA and IMSI validation:
  - provideRoamingNumber (4)
  - provideSubscriberInfo (70)
  - provideSubscriberLocation (83)

- cancelLocation (3)
- insertSubscriberData (7)
- deleteSubscriberData (8)
- getPassword (18)
- reset (37)
- activateTraceMode (50)
- unstructuredSS-Request (60)
- unstructuredSS-Notify (61)
- informServiceCentre (63)
- alertServiceCentre (64)
- setReportingState (73)
- remoteUserFree (75)
- istCommand (88)

The IMSI has upto 15 digits value. The value is composed of three parts:

- **Mobile Country Code (MCC)**: Consists of 3 digits
- **Mobile Network Code (MNC)**: Consists of 2 or 3 digits
- **Mobile Subscriber Identification Number (MSIN)**: 9 or 10 digits

The MCC and MNC parameters (first 5-6 digits) determine the Operator ID. Hence, these values are used during CAT2 validation.

At first, the match is performed with 6 digit, and if the match is not found, then it is performed with 5 digits. In case, the match is not found, the validation gets failed.

2.16.2 Feature Configurations

This section provides procedures to perform the CAT2 SS7 Security functionality.

CAT2 SS7 Security is configured using the vSTP managed objects and vSTP GUI. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.16.2.1 MMI Managed Objects for CAT2 SS7 Security Support

MMI information associated with CAT2 SS7 Security support is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* gets opened, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for CAT2 SS7 Security support:

Table 2-24 CAT2 SS7 Security support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
cat2imsi	Insert, Delete
cat2gta	Inser, Delete
gttactions	Insert, Delete, Update

cat2imsi - Insert, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ cat cat2imsi.json
{
"tadigitCode": "TEST",
"stadigitCode": "TEST",
"mccmnc": "12345"
}
```

Execute the following command on Active SOAM to update the data:

```
/vstp/cat2imsi -v POST -r cat2imsi.json
```

Sample Output:

```
{
"data": [
{
"mccmnc": "12345",
"stadigitCode": "TEST",
"tadigitCode": "TEST"
}
],
"links": {},
"messages": [],
"status": true
}
```

Cat2Gta - Insert, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$cat cat2gta.json
{
"gttStartAddress": "22345678",
 "uniqueIdentifier": "23405678-23405678-HLR",
 "stadigitCode": "TEST",
 "gttEndAddress": "22345678",
 "nodeType": "HLR",
```

```
 "tadigitCode": "TEST"
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/cat2gta -v POST -r cat2gta.json
```

Sample Output:

```
{
    "data": [
        {
            "gttEndAddress": "22345678",
            "gttStartAddress": "22345678",
            "nodeType": "HLR",
            "stadigitCode": "TEST",
            "tadigitCode": "TEST",
            "uniqueIdentifier": "22345678-22345678-HLR"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

gttactions - Insert

Execute the following command on Active SOAM to display table data:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ cat  gtt_act.json
{
"valType": "IR21ToTcap",
 "ndgt": "All",
 "actid": "actval1",
 "act": "Scpval"
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/gttactions -v POST -r gtt_act.json
```

Sample Output:

```
{
    "data": [
        {
            "act": "Scpval",
            "actid": "actval1",
            "defactid": "fallback",
```

```
            "ndgt": "All",
            "uimreqd": false,
            "useicmsg": false,
            "valType": "IR21ToTcap"
        }    ],
            "links": {},
            "messages": [],
            "status": true
}
```

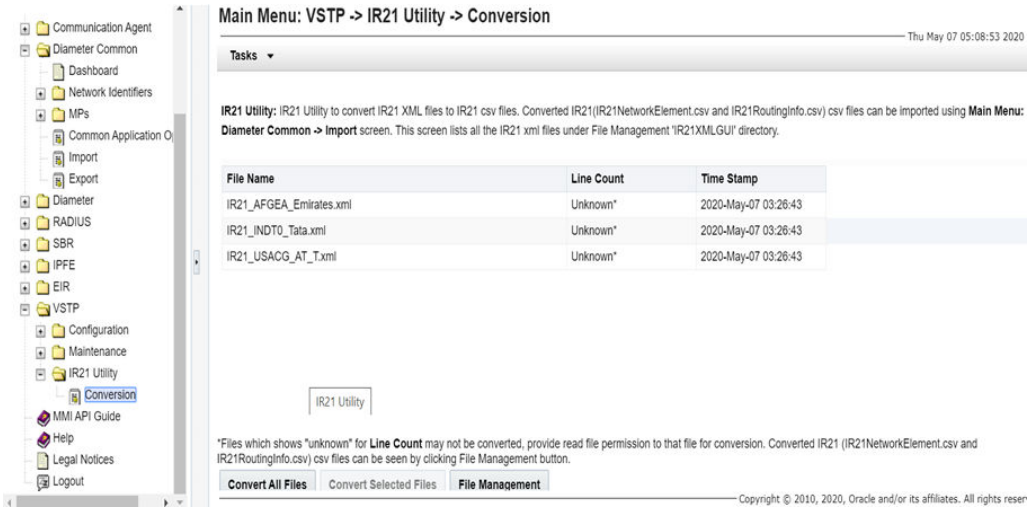

2.16.2.2 GUI Configurations for CAT2 SS7 Security Support

The CAT2 SS7 Security functionality can be configured from Active System OAM (SOAM).

To convert IR21 File

On the Active System OAM (SOAM), select **VSTP > IR21 Utility > Conversion**.

Figure 2-34 IR21 Utility



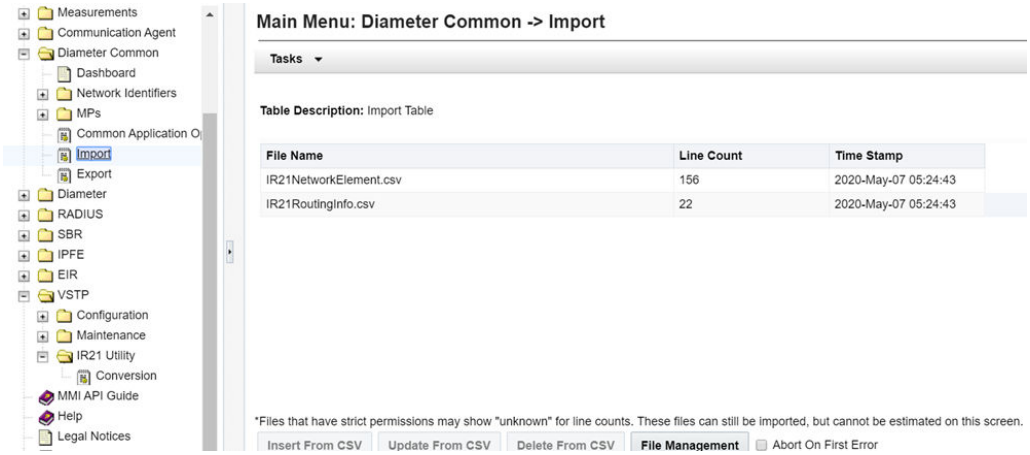
The IR21 Utility converts the IR21 XML files to CSV files.

Importing CSV Files

The converted `IR21NetworkElemet.csv` and `IR21RoutingInfo.csv` files can be imported from Active System OAM (SOAM).

The **Group Code** parameter must be configured in the **Local Signalling Points** and **Remote Signalling Points** options. Select **VSTP > Diameter Common > Import**. The page lists all the IR21 files under **File Management** > **IR21XMLGUI** directory.

Figure 2-35 Importing IR21 CSV Files



For more details on IR21 Utility GUI configurations, see IR21 Utility .

2.16.2.3 CAT2 SS7 Security Alarms and Measurements

Alarms and Events

There are no alarms or events specific to the CAT2 SS7 Security functionality.

Measurements

The following table lists the measurements specific to the CAT2 SS7 Security support for vSTP:

Measurement ID	Measurement Name
21971	VstpGttActScpvalCat2Total
21972	VstpGttActScpvalCat2Discard
21973	VstpGttActScpvalCat2NotApplied
21974	VstpCgpaGttActScpvalCat2Total
21975	VstpCgpaGttActScpvalCat2Discard
21976	VstpCgpaGttActScpvalCat2NotApplied

For more details related to measurements, refer to Measurement Reference document.

2.16.3 Troubleshooting CAT2 SS7 Security

In case of the error scenarios, the measurements specific to CAT2 SS7 Security feature are pegged. For information related to CAT2 SS7 Security measurements, see CAT2 SS7 Security Alarms and Measurements.

2.16.4 Dependencies

The CAT2 SS7 Security support for vSTP has no dependency on any other vSTP operation.

2.17 vSTP AINPQ/INPQ Feature

Throughout the world, wireline and wireless operators are receiving directives from their national regulators to support service provider number portability in their networks.

The INAP-based Number Portability (INP) and ANSI-41 Number Portability Query (AINPQ) features provide subscribers the ability to switch their telephone service to a new service provider while retaining their original telephone number. The vSTP INP/AINPQ features provide the following functionality:

- Enable subscribers to switch their telephone service to a new service provider while retaining their original telephone number.
- Detection and prevention of circular routes.
- Minimizez challenges for network operators while they plan to implement number portability for their subscribers.
- Number normalization allows the user to specify how certain NAI (Nature of Address Indicator) values are to be treated. This value treatment is performed by setting up rules that map incoming NAI values to internal SNAI (Service Nature of Address Indicator) values for the purpose of number conditioning.

2.17.1 INP and AINPQ Functions

INP and AINPQ functions minimize challenges for network operators while they plan to implement number portability for their subscribers.

INP and AINPQ functions are:

- Because the number lengths can vary between countries (sometimes even within a country), INP and AINPQ support numbers of varying lengths in a flexible way, without requiring software modifications. The maximum number length of 15 digits for ported numbers is supported.
  - INP performs number portability translations based on the received Called Party Number (CdPN) in the INAP portion of the message. For call-related messages, the database query is performed by using the digits from the Called Party Number parameter after converting them to an international number, if the number is not already in international format.
  - AINPQ performs number portability translations based on the received dialed digits (DGTSDIAL).
- The INP and AINPQ features can remove automatically the National Escape Code (NEC) that may be up to five hexadecimal digits.
- The INP and AINPQ features can help to avoid problem situations with number normalization.
  - Problems could occur where operators do not use NAI values that match the vSTP standard number conditioning process. For example, a switch might send an NAI of a subscriber and expect the number to be treated as a National number, leading to problems.
    Number normalization allows the user to specify how certain NAI (Nature of Address Indicator) values are to be treated. This value treatment is performed

by setting up rules that map incoming NAI values to internal SNAI (Service Nature of Address Indicator) values for the purpose of number conditioning.

- Number normalization lets INP and AINPQ accept queries either with or without special prefixes on the DN. Upon receipt, INP or AINPQ strips off the prefix if the DLTPFX configuration option is YES, converts the DN to an international number, performs the database query, and returns a response to the switch. The Called Party Chapter 2 Overview 2-3 Number (for the INP feature) or the dialed digits (for the AINPQ feature) in the response can include the special prefix or not, depending on how the operator configures the feature.

2.17.2 INP/AINPQ Message Protocol

INP/AINPQ support UDT SCCP messages and non-segmented XUDT messages.

INP and AINPQ support Rt-on-SSN and Rt-on GT messages.

For Rt-on GT, GTA digits must be present. INP and AINPQ support two TCAP protocols: INAP (for the INP feature) and ANSI-41 (for the AINPQ feature). The effective processing of the messages is the same for INAP and ANSI-41 protocols.

The functions are performed in following steps:

1. For INP, the leading digits of the CdPN number from the INAP portion of the message are compared to provisioned prefixes. If matching prefix digits are found, INP strips the prefix from the CdPN digits.
   For AINPQ, the leading digits of the Dialed Digits from the TCAP portion of the message are compared to any provisioned prefixes (dialpfx). If found, the prefix is stripped from the Dialed Digits.
2. If an NEC is provisioned and an NEC is present in the CdPN or dialled digits, it is stripped off.
3. Any stop digits that are present in the CdPN or dialled digits are removed.
4. For INP, after removing the prefix and NEC, INP maps the CdPN NAI to the Service NAI by doing a lookup in the MnpOptions table. If the CdPN NAI is found in the MnpOptions table, its corresponding SNAI value is used for number conditioning. Otherwise, INP treats the number as national (natl), unless the NAI field in the CdPN is subscriber (sub) or international (intl).
   For AINPQ, after removing the prefix, ST digits, and NEC from the Dialed Digits, the NAI is mapped to the Service NAI from the AINPOPTS table, and the corresponding SNAI value is used for number conditioning. If mapping is not found, AINPQ treats the number as National, unless the NAI field in the Dialed Digits is Subscriber or International.
5. If the INP Circular Route Prevention feature is turned on, the RN is matched with the Home RNs in the HomeEntity table. The Home RN that matches with the maximum number of leading digits of the CdPN is removed from the CdPN.

2.17.3 Feature Configuration

This section provides procedures to perform the INP/AINPQ functionality.

INP/AINPQ is configured using the vSTP managed objects and vSTP GUI. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

2.17.3.1 MMI Managed Objects for INP/AINPQ Support

MMI information associated with INP/AINPQ support is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* gets opened, use the application navigation to locate specific vSTP managed object information.

The following table lists the managed objects and operations supported for INP/AINPQ support:

Table 2-25 INP/AINPQ support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
sccpmnpoptions	Update
sccpserviceselectors	Inser, Update, Delete
homeentities	Insert, Update, Delete
sccpapplications	Insert, Delete
SccpAinpOptions	Display

sccpmnpoptions- Update

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat inpconf
{ “defmcc": “1",
“defndc": “23",
}
```

Execute the following command on Active SOAM to update the data:

```
/vstp/sccpmnpoptions -v PUT -r /<Absolute Path>/<File Name>
```

Sample Output:

```
{
"data": [
{
"aclen": 0,
"atiackimsi": "none",
"atiackmsisdn": "msisdn",
"atiackrn": "rn",
"atiackvlrnum": "rnspmsisdn",
"atidfltrn": "None",
"atidlm": "None",
"atientitylen": "None",
"atinptype": "any",
"atisnai": "nai",
"atisupplocinfo": "Off",
"ativlrnumlen": 40,
"cclen": 0,
```

```
"ccnc1-mccmnc1": "None",
"ccnc10-mccmnc10": "None",
"ccnc2-mccmnc2": "None",
"ccnc3-mccmnc3": "None",
"ccnc4-mccmnc4": "None",
"ccnc5-mccmnc5": "None",
"ccnc6-mccmnc6": "None",
"ccnc7-mccmnc7": "None",
"ccnc8-mccmnc8": "None",
"ccnc9-mccmnc9": "None",
"crptt": "None",
"defcc": "44",
"defmapvr": 1,
"defmcc": "None",
"defmnc": "None",
"defndc": "None",
"delccprefix": "pfxwcc",
"dngtzerofill": "No",
"encdnpsdnnotfound": "Off",
"encdnpsptnone": "Off",
"encodecug": "Off",
"encodenps": "On",
"gflexmaplayerrtg": "none",
"inpcutnpaste": "Off",
"inpdra": "rndn",
"inpdranai": "natl",
"inpdranp": "E164",
"inpnec": "36",
"inprelcause": 31,
"inpsnai1-cdpanai1": "natl-1",
"inpsnai2-cdpanai2": "None",
"inpsnai4-cdpanai4": "None",
"inpsnai5-cdpanai5": "None",
"inpsprestype": "continue",
"mnpcrp": "Off",
"mnpnpdbunavl": "dnnotfound",
"msisdntrunc": 0,
"msrndig": "rndn",
"msrnlen": 30,
"msrnnai": 1,
"msrnnp": 1,
"mtmmsackn": "ack",
"mtmmsentylen": "None",
"mtmmsgta": "1233445566",
"mtmmslen": "None",
"mtmmstype": "all",
"mtsmsackn": "nack",
"mtsmschksrc": "No",
"mtsmsdltr": "no",
"mtsmsdltrv": "9876",
"mtsmsimsi": "rn",
"mtsmsnakerr": 1,
"mtsmsnni": "rn",
"mtsmsnp": "On",
"mtsmstype": "all",
```

```
"multcc1": "11",
"multcc10": "10",
"multcc2": "2",
"multcc3": "3",
"multcc4": "4",
"multcc5": "5",
"multcc6": "6",
"multcc7": "7",
"multcc8": "None",
"multcc9": "9",
"serverpfx": "None",
"srfaddr": "None",
"srfnai": 0,
"srfnp": 0,
"sridn": "tcap",
"sridnnotfound": "gtt",
"srismdn": "sccp",
"srismgttrtg": "Off",
"srvcrelaymapset": "None"
}
],
"links": {},
"messages": [],
"status": true
}
```


sccpeserviceselectors - Insert, Update, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat srvcsel
{
"domain": "Ansi",
"globalTitleIndicator": "TtOnly",
"name": "SrvcSel_A",
"serviceName": "Inpq",
"ssn": "10",
"translationType": 20
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/sccpserviceselectors -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:


```
{
"data": [
{
"configurationLevel": "9",
"domain": "Ansi",
"globalTitleIndicator": "TtOnly",
```

```
"gttRequired": false,
"name": "SrvcSel_A",
"serviceName": "Inpq",
"ssn": "10",
"translationType": 20
},
```

homeentities - Insert, Update, Delete

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat inpqf1
{
"entityAddress": "03",
"entityType": “DialPfx",
"inpDelPfx": false,
"name": "entity03"
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/homeentities/ -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:

```
{
"entityAddress": "01",
"entityType": "DialPfx",
"inpDelPfx": false,
"name": "entity01"
},
{
"entityAddress": "47",
"entityType": "CdpnPfx",
"inpDelPfx": false,
"name": "entity1"
},
```

sccpapplications - Insert, Delete

Execute the following command on Active SOAM to display table data:

Create a file with following content. File name could be anything, for example option name can be used as filename:

```
$ Cat conf
{
"appType": "Inpq",
"ssn": 21
}
```

Execute the following command on Active SOAM to insert the data:

```
/vstp/sccpapplications -v POST -r /<Absolute Path>/<File Name>
```

Sample Output:

```
{
"data": [
{
"appType": "Inpq",
"ssn": 21
}
],
"links": {},
"messages": [],
"status": true
}
```

ainpoptions - Display

> **Note:**
>
> This object is specific to AINPQ feature.

Execute the following command on Active SOAM to display table data:

```
/vstp/ainpoptions
```

```
/vstp/ainpoptions
{
"data": [
{
"ainpdefrn": "None",
"ainplnpentpref": "asd",
"ainplnpnatldiglen": 10,
"ainplnpogdnnai": "inc",
"ainplnpoglrnnai": "inc",
"ainplnpsnai": "inc",
"ainplnpsubdiglen": 7,
"ainpnec": "None",
"ainprfmt": "asdrndn",
"ainprnai": "frmsg",
"ainprnp": "e164",
"ainpsnai1-dialnai1": "intl-1",
"ainpsnai2-dialnai2": "None",
"ainpsprestype": "rrwodgts"
}
```

2.17.3.2 GUI Configuration

The AINPQ functionality can be configured from Active System OAM (SOAM). Select **VSTP > Configuration** page.

Select **AINP Options** and configure the parameters.

For more details related to these parameters, see AINP Options.

2.17.3.3 INP/AINPQ Alarms and Measurements

Alarms and Events

The following table lists the Alarms/Events specific to the INP/AINPQ feature:

Alarm/ Event ID	Name
.70420	Unsupported ACN object ID length
70069	TCAP Invalid Parameter or Decode failure
70421	Failed to Decode TCAP parameters.
70422	INAP Called Party Number is missing
70505	Conv to intl num - Dflt CC not found
70504	Conv to intl num - Dflt NC not found
70302	Invalid length of conditioned digits
70310	Too many digits for DRA parameter
70292	SCCP Encode Failed
70304	MNP Circular Route detected

Measurements

The following table lists the measurements specific to the INP/AINPQ feature:

Measurement ID	Measurement Name
21685	VstpInpCirrouteDetected
21686	VstpInpSuccessReply
21687	VstpInpErrReplies
21688	VstpInpDiscardQuerieNoReply
21689	VstpInpQueryReceived

For more details related to measurements, refer to Measurement Reference document.

2.17.3.4 UDR Configuration for AINPQ/INPQ Feature

Configuring UDR fot AINPQ/INPQ involves adding vSTP MP(s) to UDR and then configuring UDR on the ComAgent server.

As a prerequisites for UDR configuration, it is assumed that the user is aware of UDR and ComAgent functionality. Also, UDR must be installed and the UDR topology must be configured.

Perform the following steps:

1. Add details about the vSTP MP on the ComAgent Remote Servers screen as a client by navigating to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and clicking **Insert** on an active OCUDR NOAMP.
2. Select the OCUDR server group from the *Available Local Server Groups* that needs to communicate with vSTP MP.
3. From the active OCUDR GUI, navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** and verify connection are `InService`.
4. From the active OCUDR GUI, navigate to **Communication Agent**, and then **Maintenance**, and then **Routed Services Status** and verify the *STPDbSvc* status is `Normal`.
5. From an active DSR NOAM, navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers** and click **Insert**.
6. Add the UDR NO IP in the ComAgent Remote Server screen as a Server.
7. Select the STP MP server group from the *Local SG* that needs to communicate with UDR.
8. Also add the Standby and DR NOs to the Local SG.
9. Navigate to **Communication Agent**, and then **Configuration**, and then **Connection Groups**, select *STPSvcGroup* and click **Edit**.
10. Add all available UDR NO servers.
11. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status**, select the server name, and check the connection status.

2.17.4 Troubleshooting AINPQ/INPQ Functionality

In case of the error scenarios, the measurements specific to AINPQ/INPQ feature are pegged. For information related to AINPQ/INPQ measurements, see INP/AINPQ Alarms and Measurements.

2.17.5 Dependencies

The AINPQ/INPQ functionality for vSTP has no dependency on any other vSTP operation.

3
MMI Managed Objects

This chapter provides basic information to access MMI configuration elements used by vSTP.

3.1 MMI Managed Objects

MMI information associated with vSTP is accessed from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* displays, use the application navigation to locate specific vSTP managed object information.

4
DSR Managed Objects

This chapter provides a basic overview of DSR system configuration elements used by vSTP.

> **Note:**
>
> Refer to the latest version of the *Operation, Administration, and Maintenance (OAM) Guide* for further details about DSR managed objects.

4.1 Users

The Users Administration page enables you to perform functions such as adding, modifying, enabling, or deleting user accounts. The primary purpose of this page is to set up users for logging into the system.

Each user is also assigned to a **group** or groups. Permissions to a set of functions are assigned to each group. The permissions determine the functions and restrictions for the users belonging to the group.

A user must have user/group administrative privileges to view or make changes to user accounts or groups. The administrative user can set up or change user accounts and groups, enable or disable user accounts, set password expiration intervals, and change user passwords.

4.2 Groups

The Groups Administration page enables you to create, modify, and delete user groups. From this screen, you can control vSTP managed object permissions.

A group is a collection of one or more users who need to access the same set of functions. Permissions are assigned to the group for each application function. All users assigned to the same group have the same permissions for the same functions. In other words, you cannot customize permissions for a user within a group.

You can assign a user to multiple groups. You can add, delete, and modify groups except for the pre-defined user and group that come with the system.

The default group, **admin**, provides access to all GUI options and actions on the GUI menu. You can also set up a customized group that allows administrative users in this new group to have access to a subset of GUI options/actions. Additionally, you can set up a group for non-administrative users, with restricted access to even more GUI options and actions.

For non-administrative users, a group with restricted access is essential. To prevent non-administrative users from setting up new users and groups, be sure **User** and **Group** in the Administration Permissions section are unchecked. Removing the check

marks from the Global Action Permissions section does not prevent groups and users from being set up.

Figure 4-1 Global Action and Administration Permissions

From the **Administration**, and then **Access Control**, and then **Groups** Insert page, mark the checkboxes to provide permissions and click **OK**. Return to the

Administration, and then **Access Control**, and then **Groups** page and click **Report** to display a list of permissions for a group.

These checkboxes are grouped according to the main menu's structure; most folders in the main menu correspond to a block of permissions. The exceptions to this are the permission checkboxes in the Global Action Permissions section.

The Global Action Permissions section allows you to control all insert (**Global Data Insert**), edit (**Global Data Edit**), and delete (**Global Data Delete**) functions on all GUI pages (except User and Group). For example, if the **Network Elements** checkbox is selected (in the Configurations Permissions section), but the **Global Data Insert** checkbox is not selected, the users in this group cannot insert a new Network Element.

By default, all groups have permissions to view application data and log files.

4.3 Networks

The Networks page is used to create the networks used for internal, external, and signaling communications. The networks are grouped into logical buckets called network elements. Only after creating these buckets can the networks themselves be defined. One advantage of this architecture is simplified network device configuration and service mapping.

The workflow is to first create the network elements and then define the individual networks inside each element.

4.4 Devices

The Devices page is used to configure and manage additional interfaces other than what was configured during the initial installation.

4.5 Routes

Use the route configuration page to define specific routes for traffic. You can specify routes for the entire network, specific servers, or specific server groups.

4.6 Services

This feature allows for flexible network deployment by allowing you to map an application service to a specific network. Additionally, this feature allows for the differentiation of intra- and inter-networks on a per service basis. This means that traffic from different services can be segmented, which allows for service specific-networks and routes. This is predicated on the creation of network elements, networks, and routes to support the segmentation of service traffic.

Geo-redundant (spare) nodes and dual-path monitoring are special code on the node at the spare site that continually monitors the availability of the database instances at the primary site to determine if an automatic failover should occur due to loss of the active site servers. In the event of a network outage, it is possible that if the system is monitoring a single network path only and intra- and inter-networks are differentiated, an erroneous condition might occur where both sites try to assume activity. Inherent dual-path monitoring protects against this scenario.

The core services are:

- OAM
- Replication
- Signaling
- HA_Secondary
- HA_MP_Secondary
- Replication_MP

For example, segregation of replication traffic might occur for inter-network (WAN) traffic only. Prerequisite configuration work would have included the creation of at least one LAN network and two WAN networks along with the related routes. For the purposed of this example, these could be named LAN1, WAN1, and WAN2. The services mapping might look similar to the settings in Table 4-1.

Table 4-1 Core Services

Name	Intra-NE Network	Inter-NE Network
OAM	Unspecified	Unspecified
Replication	LAN1	WAN1
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	LAN1	WAN2

Note:

Services might vary depending on the application. For example, DSR adds a service known as ComAgent to the existing core services. Additionally, workflow and provisioning instruction might differ from the direction provided here. Always follow the provisioning guidelines for your specific application and release.

4.7 Servers

Servers are the processing units of the application. Servers perform various roles within the application. The roles are:

- Network OAM&P (NOAMP) - The NOAMP is one active and one standby server running the NOAMP application and operating in a high availability global configuration. It also provides a GUI which is used for configuration, user administration and the viewing of alarms and measurements.
- System OAM (SOAM) - The SOAM is the combination of an active and a standby application server running the SOAM application and operating in a high availability configuration. SOAM also provides a GUI used for local configuration and viewing alarms and measurements details specific to components located within the frame (SOAM, MP). The SOAM supports up to 8 MPs.

> **Note:**
>
> SOAM is not an available role in systems that do not support SOAMs.

- MP - MPs are servers with the application installed and are configured for MP functionality.

The role you define for a server affects the methods it uses to communicate with other servers in the network. For more information about how each interface is used, refer to the Network Installation Guide that came with the product.

4.8 Server Groups

The Server Groups feature allows the user to assign a function, parent relationships, and levels to a group of servers that share the same role, such as NOAM, SOAM, and MP servers. For vSTP-MPs, MPs work as a vSTP server group can be configured as STP. The purpose of this feature is to define database relationships to support the high availability architecture. This relates to replication, availability, status, and reporting at the server level.

From the Server Groups page users can create new groups, edit groups, delete groups, and generate reports that contain server group data. Servers can be added or removed from existing groups using the edit function.

The Server Groups page can be accessed from the main menu by navigating to **Configuration**, and then **Server Groups**. The page displays a grid reflecting all currently configured server groups.

> **Note:**
>
> Depending on the application configuration, the preferred HA role preference, or NE HA Pref, may not be displayed.

5
GUI Configurations

The **VSTP** > **Configuration** GUI allows you to manage vSTP configuration. You can perform different tasks on an Active System OAM (SOAM).

5.1 Configuration

The **VSTP** > **Configuration** folder contains the tables used in vSTP operations. To configure a specific table, select the table name from the list to display the table details. The pages allow you to view the following information and perform the following actions:

5.1.1 Local Hosts

A Local Host is the vSTP's logical representation of a local node, accessible over one or more transport connections, with which the VSTP can transact VSTP messages. The Local Host managed object encapsulates all the characteristics of the local node that the VSTP must know about in order to communicate successfully with it.

Select the **VSTP**, and then **Configuration**, and then **Local Hosts** page. The page displays the elements on the **Local Hosts** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-1 Local Hosts Elements

Element	Description	Data Input Notes
Local Host Name	Unique name of the Local Host. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Local Host Port	Listen Port number of this Local Host. This is a mandatory field.	Format: Input text box Range = 1024 - 65535 characters
Primary Local Host IP Address	Primary IP Address of Local Host. This is a mandatory field.	Format: Drop down menu Range = 39 characters
Secondary Local Host IP Address	Secondary IP Address of Local Host.	

You can perform add, edit, or delete tasks on **VSTPConfigurationLocal Hosts** page.

Adding a Local Host

Perform the following steps to configure a new Local Host:

1. Click **Insert**.

> **Note:**
>
> The new Local Host must have a name that is unique across all Local Hosts at the SOAM. In addition, the Local Host's IP Port combination must also be unique across all Local Hosts configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Local Host

Use this procedure to change the field values for a selected Local Host. (The **Local Host Name** field cannot be changed.):

1. Select the **Local Host** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Local Host

Use the following procedure to delete a Local Host.

> **Note:**
>
> You cannot delete a Local Host if it is associated with the application.

1. Select the **Local Host** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.2 Remote Hosts

A Remote Host is the VSTP's logical representation of a remote node, accessible over one or more transport connections, with which the VSTP can transact Vstp messages. The Remote Host managed object encapsulates all the characteristics of the remote node that the VSTP must know about in order to communicate successfully with it.

Select the **VSTP**, and then **Configuration**, and then **Remote Hosts** page. The page displays the elements on the **Remote Hosts** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-2 Application IDs Elements

Element	Description	Data Input Notes
Remote Host Name	Unique name of the Remote Host. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Remote Host Port	Listen Port number of this Remote Host. This is a mandatory field.	Format: Input text box Range = 1024 - 65535 characters
Primary Remote Host IP Address	Primary IP Address of Remote Host. This is a mandatory field.	Format: Drop down menu Range = 39 characters
Secondary Remote Host IP Address	Secondary IP Address of Remote Host.	

You can perform add, edit, or delete tasks on **VSTPConfigurationRemote Hosts** page.

Adding a Remote Host

Perform the following steps to configure a new Remote Host:

1. Click **Insert**.

> **Note:**
>
> The new Remote Host must have a name that is unique across all Remote Hosts at the SOAM. In addition, the Remote Host's IP Port combination must also be unique across all Remote Hosts configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Remote Host

Use this procedure to change the field values for a selected Remote Host. (The **Remote Host Name** field cannot be changed.):

1. Select the **Remote Host** row to be edited.
2. Click **Edit**
3. Enter the updated values.

4. Click **OK**, **Apply**, or **Cancel**

Deleting a Remote Host

Use the following procedure to delete a Remote Host.

> **Note:**
>
> A Remote Host will only be deleted if all delete validation checks pass.

1. Select the **Remote Host** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.3 Local Signaling Points

A Signaling Point is a set of signaling equipment represented by a unique point code within an SS7 domain. A Local Signaling Point (LSP) is a logical element representing an SS7 Signaling Point assigned to an MP Server Group. An LSP has an SS7 domain and a true point code. The LSP may optionally be assigned up to two Capability Point Codes (CPCs), which are point codes that can be shared with other LSPs.

Select the **VSTP**, and then **Configuration**, and then **Local Signaling Points** page. The page displays the elements on the **Local Signaling Points** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-3 Local Signaling Points Elements

Element	Description	Data Input Notes
Local Signaling Point Name	Unique name of the Local Signaling Point. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
SS7 Domain type	This defines the type of SS7 domain. This is a mandatory field.	Format: Drop down menu Range = Ansi, Itui, Itun, Itun24, Itun_s, Itui_s
PC Type	This defines the types of point code. This is a mandatory field.	Format: Drop down menu Range = Tpc,Spc,Cpc
CPC Type	This defines the types of services or applications which are added in VSTP.	Format: Drop down menu Range = Stp, Eir, Gport, Inpq, Atinp

Table 5-3 (Cont.) Local Signaling Points Elements

Element	Description	Data Input Notes
MTP Point Code	The MTP Point Code that identifies this LSP. Only one LSP can have this MTP Point Code.The format differs according to Domain type. This is a mandatory field.	Valid characters are integers seperated with hyphen(-)
Group Code	The ITUN group code for duplicate point code feature. This is an optional field.	Format: Input Text Box Range = aa, zz Default Value: aa

You can perform add, edit, or delete tasks on **VSTPConfigurationLocal Signaling Points** page.

Adding a Local Signaling Point

Perform the following steps to configure a new Local Signaling Point:

1. Click **Insert**.

> **Note:**
>
> The new Local Signaling Point must have a name that is unique across all Local Signaling Points at the SOAM. In addition, the Local Signaling Point's IP Port combination must also be unique across all Local Signaling Points configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Local Signaling Point

Use this procedure to change the field values for a selected Local Signaling Point. (The **Local Signaling Point Name** field cannot be changed.):

1. Select the **Local Signaling Point** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Local Signaling Point

Use the following procedure to delete a Local Signaling Point.

> **Note:**
>
> You cannot delete a Local Signaling Point if it is part of the configuration of one or more Linksets.

1. Select the **Local Signaling Point** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.4 Remote Signaling Point

A Remote Signaling Point represents an SS7 network node (point code) with which a VSTP Local Node (/vstp/localhosts) communicates. A Remote Signaling Point resource encapsulates the characteristics required to route the signaling to the Remote Host (/vstp/remotehosts).

Select the **VSTP**, and then **Configuration**, and then **Remote Signaling Points** page. The page displays the elements on the **Remote Signaling Points** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-4 Remote Signaling Point Elements

Element	Description	Data Input Notes
Remote Signaling Point Name	Unique name of the Remote Signaling Point. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Point Code	mtpPointCode is the unique address for this Remote Signaling Point, and is used in MTP layer 3 to identify the destination of a Message Signal Unit (MSU). This is a mandatory field.	Format: Input text box Range = 1024 - 65535 characters
Domain Type	This defines the type of SS7 domain. This is a mandatory field.	Format: Drop down menu Range = Ansi, Itui, Itun, Itun24, Itun_s, Itui_s
Group Code	The ITUN group code for duplicate point code feature. This is an optional field.	Format: Input Text Box Range = aa, zz Default Value: aa
Alias Point Code 1	Alias Point Code1.	
Alias Point Code 2	Alias Point Code2.	
Alias Point 1 Group Code	This defines ITUN group code for duplicate point code feature.	
Alias Point Code 1 Domain	This defines the type of Alias Point Code1 domain.	Format: Drop down menu Range = Ansi, Itui, Itun, Itun24, Itun_s, Itui_s

Table 5-4 (Cont.) Remote Signaling Point Elements

Element	Description	Data Input Notes
Alias Point Code 2 Domain	Alias Point Code 2 Domain	
Broadcast Exception Indicator	When set to true, the VSTP does not broadcast TFP/TFA to the adjacent node whenever the Linksets (/vstp/linksets) status is changed.	Typical value is false.
Release Cause	Release cause. The condition that triggers the sending of a Release message. If the rlcopc parameter is specified and a value of 0-127 is specified for the rcause parameter, then the rcause parameter value overrides the values specified for the TIFOPTS rcausenp and rcausepfx parameters.	Default='None' Range=0-127
Split IAM	This parameter specifies when and how to split an ITU IAM message into 1 IAM message + 1 SAM message. This parameter applies only to ITU IAM messages.	Default='None' Range=15-31
NM bits reset	NM bits reset. This parameter specifies whether the NM bits should be set to 00.	Default='Off' Range=Off, On

You can perform add, edit, or delete tasks on **VSTPConfigurationRemote Signaling Points** page.

Adding a Remote Signaling Point

Perform the following steps to configure a new Remote Signaling Point:

1. Click **Insert**.

> **Note:**
>
> The new Remote Signaling Point must have a name that is unique across all Remote Signaling Points at the SOAM. In addition, the Remote Signaling Point's IP Port combination must also be unique across all Remote Signaling Points configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Remote Signaling Point

Use this procedure to change the field values for a selected Remote Signaling Point. (The **Remote Signaling Point Name** field cannot be changed.):

1. Select the **Remote Signaling Point** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Remote Signaling Point

Use the following procedure to delete a Remote Signaling Point.

> **Note:**
>
> You cannot delete a Remote Signaling Point if it is associated with the application.

1. Select the **Remote Signaling Point** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.5 Network Appearance

A Network Appearance identifies the SS7 network content of the message.

Select the **VSTP**, and then **Configuration**, and then **Network Appearance** page. The page displays the elements on the **Network Appearance** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-5 Network Appearance Elements

Element	Description	Data Input Notes
Network Appearance Name	Name for the network appearance. This is a mandatory field.	Format: Input text box;Valid names are strings between one and 9 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. Range = A 32-character string.

Table 5-5 (Cont.) Network Appearance Elements

Element	Description	Data Input Notes
Network Appearance	Network appearance. This is a mandatory field.	Format: Input text box Range = 4294967295, 0
Network Appearance Type	Network appearance type. This is a mandatory field.	Format: Drop down menu Range = Ansi, Itui, Itun, Itun24, Itun_s, Itui_s
Group Code	Group code of network appearance. This is an optional field.	Format: Input Text Box Range = aa, zz Default Value: aa

You can perform add, edit, or delete tasks on **VSTPConfigurationNetwork Appearance** page.

Adding a Network Appearance

Perform the following steps to configure a new Network Appearance:

1. Click **Insert**.

> **Note:**
>
> The new Network Appearance must have a name that is unique across all Network Appearance at the SOAM. In addition, the Network Appearance's IP Port combination must also be unique across all Network Appearance configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Network Appearance

Use this procedure to change the field values for a selected Network Appearance. (The **Network Appearance Name** field cannot be changed.):

1. Select the **Network Appearance** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Network Appearance

Use the following procedure to delete a Network Appearance.

> **Note:**
>
> You cannot delete a Network Appearance if it is associated with the application.

1. Select the **Network Appearance** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.6 Connections

A Connection is the VSTP's logical representation of an M3UA association or an MTPA assocation, accessible over one or more transport Connections, with which the VSTP can transact VSTP messages. The Connection resource encapsulates all the characteristics of the Connection that the VSTP must know about in order to communicate successfully with it.

Select the **VSTP**, and then **Configuration**, and then **Connections** page. The page displays the elements on the **Connections** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-6 Connections Elements

Element	Description	Data Input Notes
Connection Name	Unique name of the Connection. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Connection Mode	This defines the mode of the Connection.	Format: Drop down menu Range = Client, Server
Connection Type	This defines the type of the Connection. This is a mandatory field.	Format: Drop down menu Range = M3ua, M2pa
Local Host	This defines the Local Host assigned to this Connection. It must be unique within the VSTP site. This is a mandatory field.	Format: Drop down menu
Remote Host	This defines the Remote Host assigned to this Connection. It must be unique within the VSTP site. This is a mandatory field.	Format: Drop down menu
Connection Configuration Set	This defines the Connection Configuration Set assigned to this Connection.	Format: Drop down menu

You can perform add, edit, or delete tasks on **VSTPConfigurationConnections** page.

Adding a Connection

Perform the following steps to configure a new Connection:

1. Click **Insert**.

> **Note:**
>
> The new Connection must have a name that is unique across all Connections at the SOAM. In addition, the Connection's IP Port combination must also be unique across all Connections configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Connection

Use this procedure to change the field values for a selected Connection. (The **Connection Name** field cannot be changed.):

1. Select the **Connection** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Connection

Use the following procedure to delete a Connection.

> **Note:**
>
> If the Connection is part of the configuration of some other resource instance, the Connection cannot be deleted..

1. Select the **Connection** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.7 Connection Configuration Sets

Connection Configuration Sets provide a way to tailor a VSTP Connection to account for the network quality of service and Remote Node (/vstp/remotenodes) requirements. A Connection Configuration Set is simply a collection of Connection (/vstp/connections) parameters that are grouped so the set can be easily assigned to multiple Connections.

> **Note:**
>
> The Connection Configuration Set named **Default** is always available. The default Connection Configuration Set can be modified, but it cannot be deleted.

Select the **VSTP**, and then **Configuration**, and then **Connection Configuration Sets** page. The page displays the elements on the **Connection Configuration Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-7 Connection Configuration Sets Elements

Element	Description	Data Input Notes
Connection Configuration Set Name	Name associated with Connection configuration set which must be unique within the VSTP site. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Retransmission Initailization Timeout	Expected average network roundtrip time in milliseconds. This is a mandatory field.	Format: Input text box Range = Typical value is 120; Maximum: 5000, Minimum: 10
Retransmission Minimum Timeout	Minimum time (in milliseconds) to wait for an acknowledgment of a message sent. This is a mandatory field.	Format: Input text box Range = Typical value is 120; Maximum: 5000, Minimum: 10
Retransmission Maximum Timeout	Maximum time (in milliseconds) to wait for an acknowledgment of a message sent. This is a mandatory field.	Format: Input text box Range = Typical value is 120; Maximum: 10000, Minimum: 10
Retransmission Maximum Timeout Initialization	Maximum time (in milliseconds) to wait for an INIT to be acknowledged. This is a mandatory field.	Format: Input text box Range = Typical value is 120; Maximum: 10000, Minimum: 0
Retransmission Path Failure	Number of consecutive unsuccessful message retransmisssions that causes a path of the SCTP Connection (/vstp/connections) to be marked as failed. This is a mandatory field.	Format: Input text box Range = Typical value is 3; Maximum: 10, Minimum: 1

Table 5-7 (Cont.) Connection Configuration Sets Elements

Element	Description	Data Input Notes
Retransmission Association Failure	Number of consecutive message retransmissions that cause an SCTP Connection (/vstp/connections) to be marked as failed. This is a mandatory field.	Format: Input text box Range = Typical value is 5; Maximum: 20, Minimum: 1
Retransmission Initialization Failure	Number of consecutive retransmits for INIT and COOKIE-ECHO chunks that cause an SCTP Connection (/vstp/connections) to be marked as failed. This is a mandatory field.	Format: Input text box Range = Typical value is 8; Maximum: 20, Minimum: 1
SCTP Sack Delay	The number of milliseconds to delay after receiving a data chunk and before sending a SACK. This is a mandatory field.	Format: Input text box Range = Typical value is1000000. Maximum: 5000000, Minimum: 8000
SCTP Socket Send Size	Socket send buffer size (in bytes) for outgoing SCTP messages. This is a mandatory field.	Format: Input text box Range = Typical value is1000000. Maximum: 5000000, Minimum: 8000
SCTP Socket Recieve Size	Socket receive buffer size (in bytes) for incoming SCTP messages. This is a mandatory field.	Format: Input text box Range = Typical value is1000000. Maximum: 5000000, Minimum: 8000
SCTP Maximum Burst *	Specifies the maximum burst of packets that can be emitted by this Connection (/vstp/connections). This is a mandatory field.	Format: Input text box Range = Typical value is 4. Maximum: 4, Minimum: 1
SCTP Number of Inbound Streams	Maximum number of inbound SCTP streams supported locally by the SCTP Connection This is a mandatory field.	Format: Input text box Range = Typical value is 2. Maximum: 2, Minimum: 1
SCTP Number of Outbound Streams	Maximum number of outbound SCTP streams supported locally by the SCTP Connection This is a mandatory field.	Format: Input text box Range = Typical value is 2. Maximum: 2, Minimum: 1
SCTP Maximum Segment Size	The maximum size (in bytes) of any outgoing SCTP DATA chunk. If a message is larger than the sctpMaximumSegmentSize bytes, VSTP fragments the message into chunks not exceeding this size. This is a mandatory field.	Format: Input text box Range = Typical value is 0. Maximum: 1460, Minimum: 0

Table 5-7 (Cont.) Connection Configuration Sets Elements

Element	Description	Data Input Notes
SCTP Fragmentation Enabled	If true, a message exceeding the size of the path maximum transmission unit is fragmented and reassembled by the Remote Node (/vstp/remotenodes).	Typical value is true.
SCTP Data Chunk Delivery Ordered	If true, ordered delivery of the SCTP data chunk is performed; otherwise, delivery is unordered. This is a mandatory field.	Typical value is true.
SCTP Heartbeat Interval	The interval in milliseconds between sending SCTP heartbeat messages to a Remote Node (/vstp/remotenodes). This is a mandatory field.	Format: Input text box Range = Typical value is 1000. Maximum: 300000, Minimum: 0

You can perform add, edit, or delete tasks on **VSTPConfigurationConnection Configuration Sets** page.

Adding a Connection Configuration Set

Perform the following steps to configure a new Connection Configuration Set:

1. Click **Insert**.

> **Note:**
>
> The new Connection Configuration Set must have a name that is unique across all Connection Configuration Sets at the SOAM. In addition, the Connection Configuration Set's IP Port combination must also be unique across all Connection Configuration Sets configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Connection Configuration Set

Use this procedure to change the field values for a selected Connection Configuration Set. (The **Connection Configuration Set Name** field cannot be changed.):

1. Select the **Connection Configuration Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Connection Configuration Set

Use the following procedure to delete a Connection Configuration Set.

> **Note:**
>
> If the Connection Configuration Set is a part of the configuration of one or more Connections (/vstp/connections), the Connection Configuration Set cannot be deleted.

1. Select the **Connection Configuration Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.8 Links

A Link carries signaling within a Linkset using a specific Connection. A Link can belong to only one Linkset and one Connection. If a Link fails, the Signaling Network Interface attempts to divert signaling traffic to another Link in the same Linkset. Links cannot be edited. A Link can be changed only by deleting it and adding the changed Link.

Select the **VSTP**, and then **Configuration**, and then **Links** page. The page displays the elements on the **Links** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-8 Links Elements

Element	Description	Data Input Notes
Link Name	Unique name of the Link. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Link Set Name	Name of the LinkSet associated with Link. This is a mandatory field.	Format: Drop down menu
Connection Name	Name of the Connection associated with Link.	Format: Drop down menu
Channel Name	Name of the Channel (PCI Card Interafce) associated with Link.Channel. **Note:** This is supported for TDM only.	Format: Drop down menu

Table 5-8 (Cont.) Links Elements

Element	Description	Data Input Notes
Signaling Link Code	Signaling Link Code (SLC). This is a mandatory field.	Format: Input text box Range = 0-15

You can perform add, edit, or delete tasks on **VSTPConfigurationLinks** page.

Adding a Link

Perform the following steps to configure a new Link:

1. Click **Insert**.

> **Note:**
>
> The new Link must have a name that is unique across all Links at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Link

Use this procedure to change the field values for a selected Link. (The **Link Name** field cannot be changed.):

1. Select the **Link** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Link

Use the following procedure to delete a Link.

> **Note:**
>
> If the Link is enabled, the Link cannot be deleted. The Link must first be disabled, then it can be deleted from the configuration.

1. Select the **Link** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.9 Link Sets

A Link Set is a logical element representing link attributes assigned to a Link (/vstp/links) and a far-end point assigned to a Route.

Select the **VSTP**, and then **Configuration**, and then **Link Sets** page. The page displays the elements on the **Link Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-9 Link Sets Elements

Element	Description	Data Input Notes
Link Set Name	Unique name of Link Set. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
Adapter Type	Type of the VSTP adapter layer. **Note:**Mtp2 is supported for TDM only. This is a mandatory field.	Format: Drop down menu Range = M3ua, M2pa, Mtp2]
Local Signaling Point Name	Name of the Local Signaling Point associated with this Link Set. This is a mandatory field.	Format: Drop down menu Range = a-z,A-Z,_,0-9
Remote Signaling Points	Name of the Adjacent Remote Signaling Point associated with this Link Set This is a mandatory field.	Format: Input text box Range = Typical value is 120; Maximum: 10000, Minimum: 10
Link Transactions Per Second	Maximum Link transactions per second defined for the links of this Link Set. This is a mandatory field.	Format: Input text box Range = 1-10000
Routing Context	When the linkset type is M3ua, this value defines the routing context associated with the Link Set.	Format: Input text box Range = 0-4294967295
Number of Signaling Links Allowed Threshold	Threshold value for number of Links which can be allowed with this Link Set. This is applicable only for M3ua linksets.	Format: Input text box Range = 0-16

Table 5-9 (Cont.) Link Sets Elements

Element	Description	Data Input Notes
Number of Signaling Links Prohibited Threshold	Threshold value for number of Links which can be prohibited with this Link Set. This is applicable only for M3ua linksets	Format: Input text box Range = 0-16
Application Server Notification	Application Server (AS) notification.	Format: Drop down menu Range = true,false
Calling Party GT Modification Indicator	Calling party GT modification indicator.	Format: Drop down menu Range = true,false
Enable Broadcast Exception	When the linkset status changes, the VSTP broadcasts TFP/TFA to adjacent nodes.	Format: Drop down menu Range = true,false
GTT Mode	Global title translation mode. The GTT Mode hierarchy for this link set.	Format: Input text box Range = Cd, Fcd, Fcg, Fcgfcd, Fcdcg, Sysdflt
ITU Transfer Restricted	TU TFR (Transfer Restricted) indicator.	Format: Drop down menu Range = true,false
MTP Screening Set Name	Name of the MTP Screenset attached with this Linkset.	Format: Drop down menu Range = true,false
MTP Screening Set Test Mode	MTP Screening test mode. Specifies whether the MTP Screening Test Mode is true or false.	Format: Drop down menu Range = true,false
MTP Screening Event Logging	MTP Screening Event Logging. Specifies whether the MTP Screening Event Logging is true or false.	Format: Drop down menu Range = true,false
Adjacent SLS 8-bit Indicator	Adjacent SLS 8-bit indicator. This parameter specifies whether the adjacent node is sending MSUs with 8-bit SLSs.	Format: Drop down menu Range = true,false
Incoming SLS Rotated Signaling Bit	Incoming rotated sinaling link selection (SLS) bit. The bit (1-4) for ITU and (1-8) for ANSI link sets to rotate as the new SLS LSB (Least Significant Bit) of the incoming linkset.The SLS is not modified in the outgoing message.	Format: Drop down menu Range = 1 - 8
Random SLS	Random SLS (signaling link selection).This parameter is used to apply random SLS generation on a per linkset basis.	Format: Drop down menu Range = Off, All, Class0

Table 5-9 (Cont.) Link Sets Elements

Element	Description	Data Input Notes
Rotate SLS by 5 or 8 bits	Rotate SLS by 5 or 8 bits. This parameter specifies whether the signaling link selector (SLS) of the incoming ANSI linkset is rotated by 5 or 8 bits.	Format: Drop down menu Range = true, false
SLS Conversion Indicator	This parameter specifies whether the 5-bit to 8-bit SLS conversion feature is used to select links for outgoing messages direct to the given linkset.	Format: Drop down menu Range = true, false
Rotate SLS Bit	Rotated SLS (Signaling Link Selection) Bit. The bit (1-4) to rotate as the new SLS LSB (Least Significant Bit). The SLS is not modified in the outgoing message.	Format: Input text box Range = 1-4
Other CIC Bit	Other CIC (Circuit Identification Code) Bit. If the SLSOCB feature is turned on, this parameter specifies whether the Other CIC Bit option is to be used during link selection.	Format: Input text box Range = 5-16
L2 Timer Set Name	Configuration Timers associated with this Link Set.Timers can be of MTP2, M2PA or M3UA type based on the adaptor type present in linkset.	Format: Input text box Range = a-z,A-Z,0-9,_; Maximum Length = 32
L3 Timer Set Name	MTP3 Configuration Timers associated with linkset.	Format: Input text box RRange = a-z,A-Z,0-9 Maximum Length = 32

You can perform add, edit, or delete tasks on **VSTPConfigurationLink Sets** page.

Adding a Link Set

Perform the following steps to configure a new Link Set:

1. Click **Insert**.

> **Note:**
>
> The new Link Set must have a name that is unique across all Link Sets at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Link Set

Use this procedure to change the field values for a selected Link Set. (The **Link Set Name** field cannot be changed.):

1. Select the **Link Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Link Set

Use the following procedure to delete a Link Set.

> **Note:**
>
> If the Link Set is part of the configuration of one or more Links, the Link Set must first be removed from the Link.

1. Select the **Link Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.10 Routes

Routes provide a way to tailor a VSTP Connection to account for the network quality of service and Remote Node (/vstp/remotenodes) requirements. A Route is simply a collection of Connection (/vstp/connections) parameters that are grouped so the set can be easily assigned to multiple Connections.

Select the **VSTP**, and then **Configuration**, and then **Routes** page. The page displays the elements on the **Routes** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-10 Routes Elements

Element	Description	Data Input Notes
Linkset Name	Name of the Remote Signaling Point (/vstp/remotesignalingpoints) associated with this Route. This is a mandatory field.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.

Table 5-10 (Cont.) Routes Elements

Element	Description	Data Input Notes
Route Name	Unique Name for this Route This is a mandatory field. The value must be unique, and cannot be edited after it is created. .	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
RSP Name	Name of the Remote Signaling Point (/vstp/remotesignalingpoints) associated with this Route. This is a mandatory field	Format: Input text box Range = Typical value is 120; Maximum: 5000, Minimum: 10
Route Cost	The relative cost assigned to this route. Lower cost routes are preferred over higher cost routes. This is a mandatory field	Format: Input text box Range = Maximum: 99, Minimum: 0

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**Routes** page.

Adding a Route

Perform the following steps to configure a new Route:

1. Click **Insert**.

> **Note:**
>
> The new Route must have a name that is unique across all Routes at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Route

Use this procedure to change the field values for a selected Route. (The **Route Name** field cannot be changed.):

1. Select the **Route** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Route

Use the following procedure to delete a Route.

1. Select the **Route** to be deleted.

2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.11 GTT Sets

A GTT Set is a an entity to which Global Title Addresses (/vstp/globaltitleaddresses) and Selectors (/vstp/gttselectors) are assigned.

Select the **VSTP**, and then **Configuration**, and then **GTT Sets** page. The page displays the elements on the **GTT Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-11 GTT Sets Elements

Element	Description	Data Input Notes
GTT Set Name	Unique name of the GTT Set. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = A 32-character string.
NP SN Name	GTT set name (Not Present Set Name). Listen Port number of this GTT Set.	Format: Drop down menu Range = msi,Msisdn,Vlrnb,Smrpoa,Smrpda
Gtt Set Domain	Defines the type of incoming message network domain. This is a mandatory field.	Format: Drop down menu
Gtt Set Type	Defines the type of GTT Set. This is a mandatory field.	Format: Drop down menu

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**GTT Sets** page.

Adding a GTT Set

Perform the following steps to configure a new GTT Set:

1. Click **Insert**.

> **Note:**
>
> The new GTT Set must have a name that is unique across all GTT Sets at the SOAM. In addition, the GTT Set's IP Port combination must also be unique across all GTT Sets configured at the SOAM.

2. Enter the applicable values.

3. Click **OK**, **Apply**, or **Cancel**

Editing a GTT Set

Use this procedure to change the field values for a selected GTT Set. (The **GTT Set Name** field cannot be changed.):

1. Select the **GTT Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a GTT Set

Use the following procedure to delete a GTT Set.

> **Note:**
>
> If the GTT Set is part of the configuration of one or more GTT Selector (/vstp/gttselector) or Global Title Address (/vstp/globaltitleaddresses) instances, the GTT Set must first be removed from the GTT Selector (/vstp/gttselector) and Global Title Address (/vstp/globaltitleaddresses).

1. Select the **GTT Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.12 SCCP GTT Selectors

An SCCP Global Title Translation (GTT) Selector is an entity assigned to a GTT set (/vstp/gttsets).

Select the **VSTP**, and then **Configuration**, and then **SCCP GTT Selectors** page. The page displays the elements on the **SCCP GTT Selectors** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-12 SCCP GTT Selectors Elements

Element	Description	Data Input Notes
SCCP GTT Selector Name	Unique name of the SCCP GTT Selector. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box; Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = 1 - 9 character string.

Table 5-12 (Cont.) SCCP GTT Selectors Elements

Element	Description	Data Input Notes
CdPA GTT Set Name	CdPA GTT set name (/vstp/gttsets) associated with this GTT Selector.	Format: Drop down menu
CgPA GTT Set Name	CgPA GTT set name (/vstp/gttsets) associated with this GTT Selector.	Format: Drop down menu
CgPA Subsystem Number	CgPA subsystem number.	Format: Input text box Range = Maximum: 255, Minimum: 0
Domain	Defines the type of incoming message network domain.	Format: Drop down menu
Global Title Indicator	Defines the domain for this GTT Selector.	Format: Drop down menu
GTT Set Name	Linkset name (/vstp/linksets) associated with this GTT Selector.	Format: Drop down menu
Linkset Name	Linkset name (/vstp/linksets) associated with this GTT Selector.	Format: Drop down menu
Nature of Address Indicator	Defines Nature of Address indicator for this GTT Selector.	Format: Drop down menu
Nature of Address Indicator Value	Value for the nature of Address indicator.	Format: Input text box Range = Maximum: 127, Minimum: 0
Numbering Plan	Defines Numbering plan (NP) for this GTT Selector.	Format: Drop down menu
Numbering Plan Value	Value for the numbering plan.	Format: Input text box Range = Maximum: 15, Minimum: 0
Selector Id	Selector ID. Maximum: 65534, Minimum: 0	Format: Input text box Range = Maximum: 65534, Minimum: 0
Translation Type	Defines the translation type (TT) for this GTT Selector. Maximum: 255, Minimum: 0	Format: Input text box Range = Maximum: 255, Minimum: 0

You can perform add, edit, or delete tasks on **VSTPConfigurationSCCP GTT Selectors** page.

Adding a SCCP GTT Selector

Perform the following steps to configure a new SCCP GTT Selector:

1. Click **Insert**.

> **Note:**
>
> The new SCCP GTT Selector must have a name that is unique across all SCCP GTT Selectors at the SOAM. In addition, the SCCP GTT Selector's IP Port combination must also be unique across all SCCP GTT Selectors configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP GTT Selector

Use this procedure to change the field values for a selected SCCP GTT Selector. (The **SCCP GTT Selector Name** field cannot be changed.):

1. Select the **SCCP GTT Selector** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP GTT Selector

Use the following procedure to delete a SCCP GTT Selector.

> **Note:**
>
> You cannot delete an SCCP GTT Selector if it is associated with a GTT Set.

1. Select the **SCCP GTT Selector** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.13 GTT Actions

A GTT Action entry consists of an Action ID, an action, and action-specific data. The action specified in the entry determines the actions to be performed on MSU during translation.

Select the **VSTP**, and then **Configuration**, and then **GTT Actions** page. The page displays the elements on the **GTT Actions** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-13 GTT Actions Elements

Element	Description	Data Input Notes
GTT Action Name	This parameter specifies the Action ID associated with the GTT action entry. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = 1 leading alphabetic character and up to 8 following alphanumeric characters. ; Maximum Length is 9.
GTT Action Type	The action applied to the message. This is a mandatory field.	Format: Drop down menu Range = Disc, Dup, Fwd, Scpval, Sfthrot, Tcaperr, Sfapp, Udts
Handle Response	Handle Response.	Format: Drop down menu Range = Yes, No
ATI GTT Mod Name	Calling party global title modification name for ATI. The GTMOD Name to be associated with the calling party of a SFAPP GTT Action entry.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. ; Maximum Length is 9.
PSI GTT Mod Name	Calling party global title modification name for PSI. The GTMOD Name to be associated with the calling party of a SFAPP GTT Action entry.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. ; Maximum Length is 9.
ANSI TCAP Error	The reason for discarding the message containing the ANSI TCAP portion that is associated with the TCAP GTT Action.	Format: Input text box Range = 0-255
Called Part GTT Mod Name	This parameter specifies the CDPA GtMod Name associated with the GTT action entry.	Format: Drop down menu Range = 1 leading alphabetic character and up to 8 following alphanumeric characters. ; Maximum Length is 9.
Calling Part GTT Mod Name	This parameter specifies the CGPA GtMod Name associated with the GTT action entry.	Format: Drop down menu Range = 1 leading alphabetic character and up to 8 following alphanumeric characters. ; Maximum Length is 9.
Calling Party Point Code	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm).	Format: Input text box Range = Valid characters are numeric seperated by plus sign(+) or hyphen(-)

Table 5-13 (Cont.) GTT Actions Elements

Element	Description	Data Input Notes
Calling Party Point Code in Outgoing Message	The data that is used as the Calling Party Point Code in the outgoing message.	Format: Drop down menu Range = Dflt, Cgpcicmsg, Opcicmsg, Provcgpc, Remove
Default Actions	The default action that is performed when the fwd GTT Action fails to route the MSU.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. ; Maximum Length = 9
Domain	This defines the type of CGPC domain.	Format: Drop down menu Range = Ansi, Itui, Itun, Itun24, Itui_s, Itun_s
Fail Action GTT	Fail Action Name. The default action that is performed to route the message when the VLR Validation fails on Stateful App.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
Forward GTT	Forward GTT. The forward GTT Action Name that is to be used to route the MSU.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
HLR Address	This defines address of the HLR for the ATI message.	Format: Drop down menu Default = Usecdpa; Range = Usecdpa, Tcapparm, Fwdact
ITU TCAP Error GTT Action	The reason for discarding the message containing the ITU TCAP portion that is associated with the TCAPERR GTT Action.	Format: Input text box Range = 0-255
Loop Set	Name for the Loop set associated with GTA, it must be unique within the VSTP site.	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. ; Maximum Length = 9
Map Set	This parameter specifies the Mated Application Set ID.	Format: Input text box Range = 1-6000
Mrn Set	The Mated Relay Node Set ID.	Format: Input text box Range = 1-1500

Table 5-13 (Cont.) GTT Actions Elements

Element	Description	Data Input Notes
Number of Digits to be matched	Number of digits to be matched. This parameter is used to specify the number of digits that needs to be matched between SCCP parameter and MAP parameter.	Format: Input text box Range = 1-21, All
Routing Indicator	The routing indicator in the SCCP called party address of the duplicated copy of MSU.	Format: Drop down menu Range = Gt, Ssn]
Remote Signaling Point	This defines the Remote Signaling Point name associated with this Global Title Address (GTA).	Format: Drop down menu Range = Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
SCF Address	This defines the GSM SCFAddressparameter must be specified when sfapp action needs to be performed.	Format: Input text box Range = Valid characters are numeric only and maximum length is 18.
SCCP Parameters	This SCCP parameter is used to decide whether the SCCP NP, NAI and GTA shall be picked up from CDPA or CGPA for comparing.	Format: Drop down menu Range = Cggta, Cdgta
SSN	The subsystem number in the SCCP called party address of the MSU.	Format: Input text box Range = 2-255
Translation Type	New Translation Type.	Format: Input text box Range = 2-255
Threshold	If the number of MSUs serviced by the SFTHROT action exceeds threshold value, MSUs are discarded.	Format: Drop down menu Range= Range = 1-4294967295
Throttle Action Index	Throttle Action Index for Measurements.	Format: Drop down menu Range = Valid characters are integers.

You can perform add, edit, or delete tasks on **VSTPConfigurationGTT Actions** page.

Adding a GTT Action

Perform the following steps to configure a new GTT Action:

1. Click **Insert**.

> **Note:**
>
> The new GTT Action must have a name that is unique across all GTT Actions at the SOAM. In addition, the GTT Action's IP Port combination must also be unique across all GTT Actions configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a GTT Action

Use this procedure to change the field values for a selected GTT Action. (The **GTT Action Name** field cannot be changed.):

1. Select the **GTT Action** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a GTT Action

Use the following procedure to delete a GTT Action.

> **Note:**
>
> GTT Action cannot be removed if it is being used by GTT Action Set.

1. Select the **GTT Action** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.14 GTT Action Sets

A GTT Action Set consists of an Action Set name and a group of actions. The specified actions determine what actions are applied to the MSU during translation.

Select the **VSTP**, and then **Configuration**, and then **GTT Action Sets** page. The page displays the elements on the **GTT Action Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-14 GTT Action Sets Elements

Element	Description	Data Input Notes
GTT Action Set Name	This parameter specifies the Action ID associated with the GTT Action Set entry. This is a mandatory field. The value must be unique, and cannot be edited after it is created.	Format: Input text box Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range = 1 leading alphabetic character and up to 8 following alphanumeric characters
GTT Action ID 1	GTT Action ID 1 (/vstp/gttactions). The first action ID associated with the GTT action set. This is a mandatory field.	1 leading alphabetic character and up to 8 following alphanumeric characters.
GTT ACtion ID 2	GTT Action ID 2 (/vstp/gttactions). The second action ID associated with the GTT action set.	1 leading alphabetic character and up to 8 following alphanumeric characters.
GTT ACtion ID 3	GTT Action ID 3 (/vstp/gttactions). The third action ID associated with the GTT action set.	1 leading alphabetic character and up to 8 following alphanumeric characters.

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**GTT Action Sets** page.

Adding a GTT Action Set

Perform the following steps to configure a new GTT Action Set:

1. Click **Insert**.

> **Note:**
>
> The new GTT Action Set must have a name that is unique across all GTT Action Sets at the SOAM. In addition, the GTT Action Set's IP Port combination must also be unique across all GTT Action Sets configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a GTT Action Set

Use this procedure to change the field values for a selected GTT Action Set. (The **GTT Action Set Name** field cannot be changed.):

1. Select the **GTT Action Set** row to be edited.
2. Click **Edit**

3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a GTT Action Set

Use the following procedure to delete a GTT Action Set.

> **Note:**
>
> If the GTT Action Set is part of the configuration of one or more Global Title Address (/vstp/globaltitleaddresses) instances, the GTT Action Set must first be removed from the Global Title Address (/vstp/globaltitleaddresses).

1. Select the **GTT Action Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.15 Global Title Addresses

A Global Title Address (GTA) is an entity assigned to the GTT Set (/vstp/gttsets) and GTT Selector (/vstp/gttselectors).

Select the **VSTP**, and then **Configuration**, and then **Global Title Addresses** page. The page displays the elements on the **Global Title Addresses** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-15 Global Title Addresses Elements

Element	Description	Data Input Notes
GTT Set	Defines the GTT Set name associated with this Global Title Address (GTA). This is a mandatory field.	Range = 1 leading alphabetic character and up to 8 following alphanumeric characters. A value is required.
Translate Indicator	Defines translation actions and routing actions for this Global Title Address (GTA). This is a mandatory field.	Range = Dpc, Dpcngt, Dpcssn, None A value is required.
Application Context Name	Application context name. This parameter specifies the ITU TCAP acn field in the incoming MSU.	This supports up to 7 subfields separated by dash (e.g., 1-202-33-104-54-26-007). Range = Valid characters are integers, asterik (*) and None. Maximum allowed length is 27

Table 5-15 (Cont.) Global Title Addresses Elements

Element	Description	Data Input Notes
GTT Action Set Name	This defines Gtt Action Set associated with Global Title Address.	Range = 1 leading alphabetic character and up to 8 following alphanumeric characters
Cancel Called GTI	This parameter defines Cancel called global title indicator.	Default = false; Range = true, false
Calling Party GT Modification Indicator	Calling party GT modification indicator. This parameter specifies whether calling party global title modification is required.	Default = false; Range = true, false
CdPA Selector ID	CdPA Selector ID.	Range = 0-65534
Starting CdPA subsystem number	Starting CdPA subsystem number.	Range = 0-255
CgPA conversion Set Name	CgPA conversion Set Name.	Range = 1 leading alphabetic character and up to 8 following alphanumeric characters
Calling Party Point Code	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). .	Range = Valid characters are numeric seperated by hyphen(-) and plus(+) sign.
Calling Party Point Code Action	This parameter is used to provide the required abilities, indicating what any particular translation needs to do with CgPA PC.	Default = Dflt; Range = Dflt, Ignore, Remove
CgPA Selector ID	CgPA Selector ID.	Range = 0-65534
Starting CgPA subsystem number	Starting CgPA subsystem number.	Range = 0-255
Default Map Version	Default MAP version for MBR opcodes. This parameter is used to provide the default MAP version for supported MBR opcodes if Application Context Name (acn) is not present in an incoming MAP message.	Default = V3; Range = V1, V2, V3
Domain	This defines the type of SS7 domain. This is applicable to CgPA Point Code and OPC.	Range = Ansi, Itui, Itun, Itun24, Itui_s, Itun_s
Ending CdPA subsystem number	Ending CdPA subsystem number.	Range = 0-255
Ending CgPA subsystem number	Ending CgPA subsystem number.	Range = 0-255
MAP End Address	MAP End Address (similar to endAddress). This parameter specifies the end of a range of MAP digits (IMSI/MSISDN).	Range = Valid characters are a-f, A-F and 0-9. Maximum allowed length is 21
End global title address	End global title address. This parameter specifies the end of a range of global title digits.	Range = Valid characters are a-f, A-F and 0-9. Maximum allowed length is 21

Table 5-15 (Cont.) Global Title Addresses Elements

Element	Description	Data Input Notes
Fallback Option	Fallback option. The action taken when the final translation does not match while performing GTT using a FLOBR-specific GTT mode.	Default = Sysdflt; Range = Sysdflt, Yes, No
ANSI TCAP Family	The ANSI TCAP family field in the incoming MSU.	Range = Valid characters are integers, asterik (*) and None. Maximum allowed length is 4
GTT Mod	Defines the GT Mod name associated with this Global Title Address (GTA).	Range = 1 leading alphabetic character and up to 8 following alphanumeric characters.
Local Signaling Point Name	Defines the Local Signaling Point name associated with this Global Title Address (GTA).	Range = Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**Global Title Addresses** page.

Adding a Global Title Address

Perform the following steps to configure a new Global Title Address:

1. Click **Insert**.

> **Note:**
>
> The new Global Title Address must have a name that is unique across all Global Title Addresses at the SOAM. In addition, the Global Title Address's IP Port combination must also be unique across all Global Title Addresses configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Global Title Address

Use this procedure to change the field values for a selected Global Title Address. (The **Global Title Addresses Name** field cannot be changed.):

1. Select the **Global Title Addresses** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Global Title Address

Use the following procedure to delete a Global Title Address.

> **Note:**
>
> If the Global Title Address is part of the configuration of one or more Global Title Address (/vstp/globaltitleaddresses) instances, the Global Title Address must first be removed from the Global Title Address (/vstp/globaltitleaddresses).

1. Select the **Global Title Addresses** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.16 SCCP GTT Mods

A Global Title Translation (GTT) Modification is an entity assigned to a GTT set (/vstp/globaltitleaddresses) and GTT Actions (/vstp/gttactions).

Select the **VSTP**, and then **Configuration**, and then **SCCP GTT Mods** page. The page displays the elements on the **SCCP GTT Mods** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-16 SCCP GTT Mods Elements

Element	Description	Data Input Notes
cgpassn	CgPA subsystem number.	Maximum: 255 Minimum: 2
gtZeroFill	GT filler indicator in case of GTI change	
Name	Unique name for SCCP GTT MOD. This is a mandatory field.	Valid names are strings between one and 9 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
newGTI	Defines the new Global Title Indicator for this GTT Mod.	
newNAI	Defines new Nature of Address indicator for this GTT Mod.	Range= Maximum: 127 Minimum: 0
newNP	Defines new Numbering plan (NP) for this GTT Mod.	Range= Maximum: 15 Minimum: 0

Table 5-16 (Cont.) SCCP GTT Mods Elements

Element	Description	Data Input Notes
newTT	Defines the new translation type (TT) for this GTT Mod.	Maximum: 255 Minimum: 0
npdd	Number of prefix digits to be deleted. The number of digits to be deleted from the prefix of the received GT address.	Maximum: 21 Minimum: 1
npds	New prefix digits string. The digits to be prefixed to the received GT address.	
nsdd	Number of suffix digits to be deleted. The number of digits to be deleted from the suffix of the received GT address.	Maximum: 21 Minimum: 1
nsds	New suffix digits string. The digits to be suffixed to the received GT address.	
sfxFirst	Suffix Prefix processing Precedence indicator.	default: false

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP GTT Mods** page.

Adding a SCCP GTT Mod

Perform the following steps to configure a new SCCP GTT Mod:

1. Click **Insert**.

> **Note:**
>
> The new SCCP GTT Mod must have a name that is unique across all SCCP GTT Mods at the SOAM. In addition, the SCCP GTT Mod's IP Port combination must also be unique across all SCCP GTT Mods configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP GTT Mod

Use this procedure to change the field values for a selected SCCP GTT Mod. (The **SCCP GTT Mod Name** field cannot be changed.):

1. Select the **SCCP GTT Mod** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP GTT Mod

Use the following procedure to delete a SCCP GTT Mod.

> **Note:**
>
> If the GTT Modification is associated with a GTT Set (/vstp/gttsets), the GTT Modification cannot be deleted.

1. Select the **SCCP GTT Mod** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.17 SCCP Map Sets

A Mated Application Part (MAP) Set is a logical grouping of Remote Signaling Points (/vstp/remotesignalingpoints) referred to as a load sharing group. The Default MAP Set (the MAP Set with mapSetId equal to 0) can have multiple load sharing groups. All other MAP Sets can have only one load sharing group associated with them. A load sharing group can have at most 32 RSPs.

Select the **VSTP**, and then **Configuration**, and then **SCCP Map Sets** page. The page displays the elements on the **SCCP Map Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-17 SCCP Map Sets Elements

Element	Description	Data Input Notes
Map Set Id	Id of this Map Set must be unique across MAP Sets. If a mate RSP is being added to an existing MAP Set, the mapSetId must be the same as assigned to the MAP Set instance containing the primary RSP. This is a mandatory field.	Range = 1,36000
RSP Name	Defines the Remote Signaling Point name associated with this MAP Set. This is a mandatory field.	
SSN	Defines the application's subsystem number. This is a mandatory field.	Range 2,255

Table 5-17 (Cont.) SCCP Map Sets Elements

Element	Description	Data Input Notes
Relative Cost	Defines the relative cost of the route for the RSP of this MAP Set. For the primary RSP, the default value is 10 and for a mate RSP the default value is 50. This is a mandatory field.	Range 0,99
Weight	Defines the weight assigned to the primary RSP of this MAP Set. Weight is not applicable for solitary and dominant modes. Weight is only valid for load sharing mode and its default is 1.	Range 1,99
Threshold	Defines the in-service threshold assigned to each combination of RSP and SSN in this MAP Set having the same relativeCost. The Weighted GTT Loadsharing feature must be enabled (using the GTT Feature Control before this parameter can be specified. If this parameter is not specified, a value of 1% is assigned to each RSP in this MAP Set.	Range 1,100
Message Route Congest	Must be set to Yes if the Class 0 messages to the specified RSP can be routed to the next preferred node/ subsystem when that RSP is congested. No otherwise. If domain of RSP is ANSI, Default is equivalent to Yes. If domain of RSP is ITU, Defalut is equivalent to No.	If not specified by user the value for messageRouteCongestion is set to Default.
Sub System Routing Message	Must be set to Yes if the subsystem routing messages (SBR, SNR) are transmitted between the mated applications, No otherwise. If domain of RSP is ANSI, Default is equivalent to Yes. If domain of RSP is ITU, Defalut is equivalent to No.	If not specified by user the value for subsystemRoutingMessage is set to Default.
Sub System Status Option	Must be set to Yes if the RSP specified by rspName initiates a subsystem test when a RESUME message is received, No otherwise.	Default is equivalent to No. If not specified by user the value for subsystemStatusOption is set to Default.

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP Map Sets** page.

Adding a SCCP Map Set

Perform the following steps to configure a new SCCP Map Set:

1. Click **Insert**.

> **Note:**
>
> The combination of mapSetId, rspName and ssn must be unique across all MAP Set entries at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP Map Set

Use this procedure to change the field values for a selected SCCP Map Set. (The **SCCP Map Set Name** field cannot be changed.):

1. Select the **SCCP Map Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP Map Set

Use the following procedure to delete a SCCP Map Set.

> **Note:**
>
> If only one RSP is associated with the MAP Set, it is deleted and the groupId and mapSetId assigned to this MAP Set becomes available to configure a new MAP Set.

1. Select the **SCCP Map Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

Map Set Id*	Id of this Map Set must be unique across MAP Sets. If a mate RSP is being added to an existing MAP Set, the mapSetId must be the same as assigned to the MAP Set instance containing the primary RSP. Range 1,36000 A value is required.
RSP Name*	Defines the Remote Signaling Point name associated with this MAP Set. A value is required.
SSN*	Defines the application's subsystem number.Range 2,255 A value is required.

Relative Cost*	Defines the relative cost of the route for the RSP of this MAP Set. For the primary RSP, the default value is 10 and for a mate RSP the default value is 50. Range 0,99 A value is required.
Weight	Defines the weight assigned to the primary RSP of this MAP Set. Weight is not applicable for solitary and dominant modes. Weight is only valid for load sharing mode and its default is 1. Range 1,99
Threshold	Defines the in-service threshold assigned to each combination of RSP and SSN in this MAP Set having the same relativeCost. The Weighted GTT Loadsharing feature must be enabled (using the GTT Feature Control before this parameter can be specified. If this parameter is not specified, a value of 1% is assigned to each RSP in this MAP Set. Range 1,100
Message Route Congest	Must be set to Yes if the Class 0 messages to the specified RSP can be routed to the next preferred node/subsystem when that RSP is congested. No otherwise. If domain of RSP is ANSI, Default is equivalent to Yes. If domain of RSP is ITU, Defalut is equivalent to No. If not specified by user the value for messageRouteCongestion is set to Default.This attribute is NOT currently in use. Will be used in future..
Sub System Routing Message	Must be set to Yes if the subsystem routing messages (SBR, SNR) are transmitted between the mated applications, No otherwise. If domain of RSP is ANSI, Default is equivalent to Yes. If domain of RSP is ITU, Defalut is equivalent to No. If not specified by user the value for subsystemRoutingMessage is set to Default.This attribute is NOT currently in use. Will be used in future.
Sub System Status Option	Must be set to Yes if the RSP specified by rspName initiates a subsystem test when a RESUME message is received, No otherwise. Default is equivalent to No. If not specified by user the value for subsystemStatusOption is set to Default.This attribute is NOT currently in use. Will be used in future.

5.1.18 SCCP Mrn Sets

A Mated Relay Node (MRN) Set is a logical grouping of Remote Signaling Points (/vstp/remotesignalingpoints) referred as a load sharing group. The Default MRN Set (the MRN Set with mrnSetId equal to 0) can have multiple load sharing groups. All other MRN Sets can have only one load sharing group. A load sharing group can have at most 32 RSPs.

Select the **VSTP**, and then **Configuration**, and then **SCCP Mrn Sets** page. The page displays the elements on the **SCCP Mrn Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-18 SCCP Mrn Sets Elements

Element	Description	Data Input Notes
MrnSet Id	Id of this MRN Set. mrnSetId can be any integer in the range. It must be unique across MRN sets. This is a mandatory field.	Range= Maximum: 1500 Minimum: 1
Relative Cost	Defines the relative cost of the route for the RSP (/vstp/remotesignalingpoints) of this MRN Set. This is a mandatory field.	Maximum: 99 Minimum: 0
RSP Name	Defines the Remote Signaling Point name (/vstp/remotesignalingpoints) associated with this MRN Set. This is a mandatory field.	
Threshold	Defines the in-service threshold for all RSP (/vstp/remotesignalingpoints) in this MRN Set having the same relativeCost.	Maximum: 100 Minimum: 1
Weight	Defines the weight assigned to the RSP (/vstp/remotesignalingpoints) of this MRN Set.	Maximum: 99 Minimum: 1

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP Mrn Sets** page.

Adding a SCCP Mrn Set

Perform the following steps to configure a new SCCP Mrn Set:

1. Click **Insert**.

> **Note:**
>
> The combination of mrnSetId, groupId and rspName must be unique across all MRN Set entries at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP Mrn Set

Use this procedure to change the field values for a selected SCCP Mrn Set. (The **SCCP Mrn Set Name** field cannot be changed.):

1. Select the **SCCP Mrn Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP Mrn Set

Use the following procedure to delete a SCCP Mrn Set.

> **Note:**
>
> If only one RSP is associated with the MRN Set, it is deleted and the groupId and mrnSetId assigned to this MRN Set becomes available to configure a new MRN Set.

1. Select the **SCCP Mrn Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.19 MTP Screen Sets

A MTP Screen Set is an entity which are assigned to MTP Screening Rules (/vstp/mtpscrrules) and used by MTP OPC Rule type, MTP SIO Rule type, MTP DPC Rule type,MTP BLKOPC Rule type, MTP BLKDPC Rule type or MTP DSTFLD Rule type.

Select the **VSTP**, and then **Configuration**, and then **MTP Screen Sets** page. The page displays the elements on the **MTP Screen Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-19 MTP Screen Sets Elements

Element	Description	Data Input Notes
Mtp Screen Set Name	Name for the VSTP MTP Screen Set, which must be unique within the VSTP site. This is a mandatory field.	Valid screen set names are strings between one and 8 characters, inclusive. Valid characters are alphanumeric. The screensetname must contain at least one alpha and must not start with a digit.

Table 5-19 (Cont.) MTP Screen Sets Elements

Element	Description	Data Input Notes
NSFI	The NSFI defines the next screening category that is used in the gateway screening process,or it indicates that the gateway screening process should stop.	Range=Dpc,Opc,Sio,BlkOpc,BlkDpc
Next Scr Rule Group Name	Allowed next screening rule group name. This is a mandatory field.	Range= 1 alphabetic character followed by up to 7 alphanumeric characters.

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**MTP Screen Sets** page.

Adding a MTP Screen Set

Perform the following steps to configure a new MTP Screen Set:

1. Click **Insert**.

> **Note:**
>
> The MTP Screen Set name must be unique across all MTP Screen Sets at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a MTP Screen Set

Use this procedure to change the field values for a selected MTP Screen Set. (The **MTP Screen Set Name** field cannot be changed.):

1. Select the **MTP Screen Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a MTP Screen Set

Use the following procedure to delete a MTP Screen Set.

> **Note:**
>
> If the MTP Screen Set is part of the configuration of one or more MTP Selector (/vstp/mtpselectors) and MTP OPC Rule (/vstp/mtpopcrules) and/or MTP SIO Rule (/vstp/mtpsiorules) and/or MTP DPC Rule and/or MTP BLKOPC Rule and/or MTP BLKDPC Rule and/or MTP DSTFLD Rule, the MTP Screen Set must first be removed from the MTP Selector (/vstp/mtpselectors) and MTP OPC Rule (/vstp/mtpopcrules) and/or MTP SIO Rule (/vstp/mtpsiorules) and/or MTP DPC Rule and/or MTP BLKOPC Rule and/or MTP BLKDPC Rule and/or MTP DSTFLD Rule.

1. Select the **MTP Screen Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.20 MTP Screening Rules

A MTP Screening Rule is an entity to configure all the screening rules for a Screen Set (/vstp/mtpscreensets/).

Select the **VSTP**, and then **Configuration**, and then **MTP Screening Rules** page. The page displays the elements on the **MTP Screening Rules** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-20 MTP Screening Rules Elements

Element	Description	Data Input Notes
MTP Screening Name	This defines MTP screening rule name. This is a mandatory field.	Range = 1 leading alphabetic character and up to 7 following alphanumeric characters]
NSFI	This parameter specifies the next screening category that is used in the MTP screening process, or it indicates that the MTP screening process should stop. This is a mandatory field.	Range = AftDstn, BlkDpc, BlkOpc, Dpc, Fail, Opc, Sio, Stop
Screening Rule Group Type	This parameter indicates type of the screening rule group. This is a mandatory field.	Range = AftDstn, BlkDpc, BlkOpc, Dpc, Opc, Sio
MTP Screening Rule Group	This defines allowed screening rule group name. .] This is a mandatory field.	Range = 1 leading alphabetic character and up to 7 following alphanumeric characters]

Table 5-20 (Cont.) MTP Screening Rules Elements

Element	Description	Data Input Notes
SCCP Stop Action Screening	This specifies whether the given MTP Screening Rule will include SCCP Stop Action screening.	Default = false; Range = true, false;
TIF Stop Action	TIF Stop Action (This field is only valid for SIO if si equals 5. Only valid when nsfi=STOP).	Range = Tif_Ruleset_1, Tif_Ruleset_2, Tif_Ruleset_3
ITU International Area	This defines ITU international area. The area in the point code represented by zone-area-id.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
H0 Heading code	This defines H0 Heading code. New H0 heading code for SSNM message.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range. Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[0-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$\|^[*]$'
H1 Heading code	This defines H1 Heading code. New H0 heading code for SSNM message.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range.Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[0-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$\|^[*]$'
ITU International ID	This parameter defines ITU international ID. The ID in the point code represented by zone-area-id.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 3. Regular expression to represent the range is '^(([0-7])(-))?([0-7])$\|^[*]$|^[D]$'

Table 5-20 (Cont.) MTP Screening Rules Elements

Element	Description	Data Input Notes
ITU National Main Number Area	This parameter defines 16-bit ITU national main number area. The mna in the point code represented by un-sna-mna.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 5. Regular expression to represent the range is '^((([0-2]?[0-9])|([3][0-1]))(-))?(([0-2]?[0-9])|([3][0-1]))$\|^[*]$|^[D]$'
ITU National Signaling Area	This parameter defines 24-bit ITU-national main signaling area value. The msa of the point code represented by msa-ssa-sp.	Range = Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[D]$'
ITU National Point Code	This parameter defines ITU national point code.	Range = Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 11. Regular expression to represent the range is '^((([0]?[0-9]{1,4})|([1][0-5][0-9]{1,3})|(16[0-2][0-9]{1,2})|(163[0-7][0-9])|(1638[0-3]))(-))?(([0]?[0-9]{1,4})|([1][0-5][0-9]{1,3})|(16[0-2][0-9]{1,2})|(163[0-7][0-9])|(1638[0-3]))$\|^[D]$'
Network Cluster	This parameter defines Network cluster value. This parameter specifies one or more nc values for the network indicator and network cluster member values specified in the ni and ncm parameters. It specifies the nc of the point code represented by ni-nc-ncm.	Range = Valid characters are integers seperated by hyphen (-),asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'

Table 5-20 (Cont.) MTP Screening Rules Elements

Element	Description	Data Input Notes
Network Cluster Member	This parameter defines Network cluster member value. This parameter specifies one or more ncm values for the network indicator and network cluster values identified in the ni and nc parameters. It specifies the ncm of the point code represented by ni-nc-ncm.	Range = Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
Network Indicator	This parameter defines Network indicator value. This parameter specifies one or more ni values for the network cluster and network cluster member values identified in the nc and ncm parameters. It specifies the ni of the point code represented by ni-nc-ncm.	Range = Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
Network Indicator Code	This parameter defines Network indicator code. The NIC is the last 2 bits of the subservice field of an SIO.	Range = Valid characters are integers seperated by hyphen (-) and asterik (*) to mark full range. Maximum allowed length is 3. Regular expression to represent the range is '^(([0-3])(-))?([0-3])$\|^[*]$'
Next Screening Rule Group	This defines allowed next screening rule group name.	Range = 1 leading alphabetic character and up to 7 following alphanumeric characters
Message Priority	This parameter defines message priority.	Range = Valid characters are integers seperated by hyphen (-) and asterik (*) to mark full range. Maximum allowed length is 3. Regular expression to represent the range is '^(([0-3])(-))?([0-3])$\|^[*]$'
Service Indicator	This parameter defines Service indicator. The SI is the first 4 bits of an SIO. The SS7 code directs the message to the MTP-user at the destination code.	Range = Valid characters are integers seperated by hyphen (-). Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[3-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$'

Table 5-20 (Cont.) MTP Screening Rules Elements

Element	Description	Data Input Notes
ITU National Signaling Point	This parameter defines 24-bit ITU national signaling point. This parameter specifies the sp in the point code represented by msa-ssa-sp.	Range = Valid characters are integers seperated by hyphen (-),asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
ITU National Sub Number Area	This parameter defines 16-bit ITU national sub number area. The sna in the point code represented by un-sna-mna.	Range = Valid characters are integers seperated by hyphen (-),asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[0-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$\|^[*]$|^[D]$'
ITU National Sub Signaling Area	This parameter defines 24-bit ITU national sub signaling area. The ssa in the point code represented by msa-ssa-sp.	Range = Valid characters are integers seperated by hyphen (-),asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
ITU National Unit Number	This parameter defines 16-bit ITU-national unit number. The un of the point code represented by un-sna-mna.	Range = Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 7. Regular expression to represent the range is '^((([0]?[0-9]?[0-9])|([1][0-1][0-9])|(12[0-7]))(-))?(([0]?[0-9]?[0-9])|([1][0-1][0-9])|(12[0-7]))$\|^[D]$'
ITU International Zone	This parameter defines ITU international zone. This parameter specifies the zone in the point code represented by zone-area-id.	Range = Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 3. Regular expression to represent the range is '^(([0-7])(-))?([0-7])$\|^[D]$'

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**MTP Screening Rules** page.

Adding a MTP Screening Rule

Perform the following steps to configure a new MTP Screening Rule:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a MTP Screening Rule

Use this procedure to change the field values for a selected MTP Screening Rule. (The **MTP Screening Rule Name** field cannot be changed.):

1. Select the **MTP Screening Rule** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a MTP Screening Rule

Use the following procedure to delete a MTP Screening Rule.

> **Note:**
>
> A MTP Screening Rule can only be deleted if all delete validation checks pass.

1. Select the **MTP Screening Rule** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.21 Home Entities

A Home Entity (/vstp/homeentities) is added for two different types 'HomeRN'and 'HomeSMSC'.

Select the **VSTP**, and then **Configuration**, and then **Home Entities** page. The page displays the elements on the **Home Entities** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-21 Home Entities Elements

Element	Description	Data Input Notes
Home Entity	Name for this Home Entity. This is a mandatory field.	Range = Valid names are strings between one and 12 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
Entity Address	Entity Address prefix digit string. This is a mandatory field.	Range = Allowed maximum length is 21 and the regular expresson to be followed is "^((0x|0X)?[a-fA-F0-9]*)$"
Entity Type	This defines the type of entity. This is a mandatory field.	Range = "HomeRn","HomeSmsc", "CdpnPfx"
Delete Prefix	Delete prefix. This parameter specifies whether to delete the CdpnPfx.	Default = false ; Range = true, false

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**Home Entities** page.

Adding a Home Entity

Perform the following steps to configure a new Home Entity:

1. Click **Insert**.

> **Note:**
>
> The Home Entity must be unique at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Home Entity

Use this procedure to change the field values for a selected Home Entity. (The **Home Entity Name** field cannot be changed.):

1. Select the **Home Entity** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Home Entity

Use the following procedure to delete a Home Entity.

> **Note:**
>
> A Home Entity can only be deleted if all delete validation checks pass.

1. Select the **Home Entity** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.22 SCCP Mnp Options

The Mobile Number Portability (MNP) Options are those configuration values that govern the overall MNP functionality . There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The MNP Options resources can only be updated. The MNP Options cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **SCCP Mnp Options** page. The page displays the elements on the **SCCP Mnp Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-22 SCCP Mnp Options Elements

Element	Description	Data Input Notes
Aclen	The length of area code.	Default - 0 , [Minimum,Maximum] - [0,8]
Cclen	The length of the country code.	Default - 0 [Minimum,Maximum] - [0,3]
Intlunknnai	This parameter specifies whether InternationalNAIs (nai=intl) are included in Unknown NAIs(nai=unkn) and should be considered for country code CgPN (cccgpn) conditioning.	
Srfaddr	Entity address of the MNP_SRF node	
Srfnai	The nature of address indicator value of the MNP_SRF.	Default - 0 , [Minimum,Maximum] - [0,127]
Srfnp	The numbering plan value of the MNP_SRF. Default - 0 , [Minimum,Maximum] - [0,15]	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Mosmsbpartygttset	MO SMS B-Party Routing GTT Set name. The GTT set where Global Title Translation lookup on B-Party digits is performed	
Mosmsbpartychk	MO SMS B-Party PPSMS Check. This parameter specifies whether a prepaid check on the B-Party is performed on an incoming MO SMS message.	
Mosmsdefrn	Default routing number. A default routing number used for own-network subscribers.	
Mosmsaclen	The number of the digits that are taken from the MO SMS CgPA and used as the Area Code in the MO SMS CdPA.	Default - 0 , [Minimum,Maximum] - [0,8]
Mosmsdigmat	MO-based SMS Home SMSC match. The method used by the Portability Check for MO SMS or the MObased GSM SMS NP feature to find a Home SMSC match.	
Mosmsfwd	MO-based SMS forward. This parameter specifies whether the value of the SCCP CDPA in the MO-based SMS message is modified to the GTA value that is specified by the mosmsgta parameter.	
Mosmsgta	MO-based SMS GTA. The GTA value that is used to replace the SCCP CDPA value in the MO-based SMS message.	This parameter can't be changed back to None once it is set other values.
Mosmsgttdig	MO SMS B-Party Routing GTT digits. The digits used for Global Title Translation.	
Mosmsnai	MO-based SMS NAI. The number conditioning performed on the SMS message destination address before lookup in the number portability database is performed.	
Mosmssa	MO-based SMS sub-address. This parameter specifies whether the sub-address is searched in the SMS called party (destination address).	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Mosmstcapseg	MO-based SMS TCAP Segmentation for GSM. This parameter specifies whether Mobile-Originated segmented TCAP messages are supported.	
Mosmstype	MO-based SMS type. The value of the entity type that indicates that a successful lookup occurred in the number portability database.	
Mosmsspfill	This parameter specifies whether the Numbering Plan Processor (NPP) can populate SP and RN entities for own network subscribers at the same time.	
Msrndig	The routing number to be used as is or concatenated with the MSISDN.	
Msrnlen	The number of digits in the MAP Routing Info portion of the returned SRI_ACK message.	Default - 30 , [Minimum,Maximum] - [1,30]
Msrnnai	The nature of address indicator value for the MSRN.	Default - 0 , [Minimum,Maximum] - [0,7]
Msrnnp	The numbering plan value for the MSRN. Default - 0 , [Minimum,Maximum] - [0,15]	
Msisdntrunc	MSISDN truncation digits.	Default - 0 , [Minimum,Maximum] - [0,5]
Defmapvr	Default MAP version.	Default - 1 , [Minimum,Maximum] - [1,3]
Sridn	The Send Routing Information Dialed Number location.	
Multcc1	Multiple country code.	
Multcc2	Multiple country code.	
Multcc3	Multiple country code.	
Multcc4	Multiple country code.	
Multcc5	Multiple country code.	
Multcc6	Multiple country code.	
Multcc7	Multiple country code.	
Multcc8	Multiple country code.	
Multcc9	Multiple country code.	
Multcc10	Multiple country code.	
Serverpfx	Server SRI prefix.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Sridnnotfound	The processing used when G-Port encounters an RTDB query result that indicates that the specified directory number is not known.	
Crptt	Circular Route Prevention Translation Type.	
Defcc	Default country code.	
Defndc	Default network destination code.	
Defmcc	E212 default mobile country code. It should support any 3 digits hexa-decimal number or None.	
Defmnc	E212 default mobile network code. It should support any 2 or 3 digits hexa-decimal number or None.	
Dngtzerofill	MT-Based SMS check source. This parameter specifies whether the SCCP CgPA GTA of a SRI_SM message is validated to determine if the source of the message is a Home SMSC.	
ccnc1-mccmnc1	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc2-mccmnc2	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc3-mccmnc3	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
ccnc4-mccmnc4	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc5-mccmnc5	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc6-mccmnc6	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc7-mccmnc7	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc8-mccmnc8	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
ccnc9-mccmnc9	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
ccnc10-mccmnc10	Combination of E214 country code/network code and E212 mobile country code/mobile network code. The values for ccnc and mccmnc must be separated by a hyphen (-). 'None' must be specified to unconfigure this parameter.	
Delccprefix	This parameter specifies how to apply the DELCCPREFIX digit action to a Called Party Global Title Address (CdPA GTA).	
Encdnpsdnnotfound	Specifies whether the NPSI is included in SRI Ack messages when the DN is not found.	
Encdnpsptnone	Specifies whether the NPSI is included in SRI Ack messages when the PT has a value of none (255).	
Encodecug	Specifies whether the Closed User Group (CUG) Checkinfo from the SRI message is included in the SRI Ack message.	
Encodenps	Specifies whether the Number Portability Status Indicator (NPSI) is included in SRI Ack messages when the portability type (PT) has a value of 0, 1, 2 or 36.	
Srismgttrtg	Specifies whether the SRI_SM routing feature is on.	
Mtsmsimsi	MT-Based SMS IMSI. The required format of digits that are encoded in the 'IMSI' parameter of the SRI_SM response message.	
Mtsmsnni	MT-Based SMS network node indicator. The required format of digits that are encoded in the 'Network NodeNumber' parameter of the SRI_SM response message.	
Mtsmstype	MT-Based SMS type. The value of the entity type that indicates that a successful lookup occurred in the number portability database for messages that are modified by the MT-Based GSM SMS NP feature.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Mtsmsackn	MT-Based SMS acknowledgement. The message generated in response to a successful number portability database lookup for an SRI_SM message from a Home SMSC.	
Mtsmsdltr	MT-Based SMS delimiter. This parameter specifies whether to insert a delimiter digit string before or after the routing number (RN) if the RN is used in the outbound digit format.	
Mtsmsdltrv	MT-Based SMS delimiter value. The delimiter digit string that is inserted before or after the RN when the RN is used in the outbound digit format.	
Mtsmsnakerr	MT-Based SMS negative acknowledgement error. The TCAP error choice code used in the NACK response message generated for SRI_SM messages.Default - 1, [Minimum,Maximum] - [0,255]	
Mtsmschksrc	MT-Based SMS check source. This parameter specifies whether the SCCP CgPA GTA of a SRI_SM message is validated to determine if the source of the message is a Home SMSC.	
Mtsmsnp	Specifies whether the MT bases SMS NP feature is activated.	
Mnpcrp	Specifies whether the MNP Circular Route feature is activated.	
Mnpnpdbunavl	This option indicates action to be taken by MNP service when the Number Portability Database is Unavailable.	
Srvcrelaymapset	This option specifies the Load sharing MAPSET ID to be used for routing the MNP relayed messages.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Srismdn	SRI_SM DN location. This parameter specifies whether the MT-Based GSM SMS NP feature selects the MSISDN from the TCAP or SCCP CdPA section of the SRI_SM message.	
Mtmmsgta	MT-Based MMS GTA. The GTA that is compared with the SCCP CgPA GTA of an SRI_SM message to determine whether the originator of the message is a Home MMSC.	
Mtmmstype	MT-Based SMS type. The value of the entity type that indicates that a successful lookup occurred in the number portability database for messages that are modified by the MT-Based GSM SMS NP feature.	
Mtmmsackn	MT-Based MMS acknowledgement. The message that is generated in response to a successful number portability database lookup for an SRI_SM message from a Home MMSC.	
Mtmmsentylen	MT-Based MMS Entity length. The maximum number of digits used from the entity value of a returned RN, SP, or SRFIMSI entity for Multimedia Service (MMS) processing.	
Mtmmslen	MT-Based MMS Length. The maximum number of digits used in the returned IMSI and/or NNI fields for MMS processing.	
Atiackimsi	ATIACK IMSI parameter for ATI ACK response message. This parameter specifies formatting of IMSI digits in the ATI ACK response message.	
Atiackmsisdn	MSISDN parameter for ATI ACK response message. This parameter specifies the formatting of MSISDN parameter in the ATI ACK response message.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Atiackrn	Routing number parameter for ATI ACK response message. This parameter specifies the formatting of the routing number parameter in the ATI ACK response message.	
Atiackvlrnum	The formatting of the VLR-number in the ATI ACK response message.	
Atidfltrn	Default Routing Number. The routing number to be used in outgoing message formats while encoding outgoing digit formats in the ATI ACK response in cases where an RN is not returned from an RTDB lookup.	
Atidlm	Outbound message digits delimiter. This delimiter is used in outgoing message formats while encoding outbound digits in the ATI ACK response.	
Atinptype	Number Portability Type. The criteria for a successful RTDB lookup.	
Atientitylen	Entity Length. The maximum number of digits to be used from entity data (SRFIMSI or entity ID) in the specified encoding format.	
Atisupplocinfo	Specifies whether the Location Information shall be processed by ATINP subsystem or not.	
Atisnai	Service NAI. The number conditioning that is performed on the MSISDN digits in the incoming ATI query message before RTDB lookup is performed.	
Ativlrnumlen	The maximum number of digits that can be encoded as the VLR-number in ATI ACK message. Default - 1 , [Minimum,Maximum] - [1,40]	
Inpdranai	INPOPTS DRANAI Destination Routing Address Nature of Address Indicator.	
Inpdranp	INPOPTS Destination Routing Address Numbering Plan.	
Inpdra	INPTOPTS Destination Routing Address Format.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Inpnec	National Escape Code.	
Inprelcause	Release Cause to be used in RELEASECALL operation.	Default: 1 Range: 31,127
Inpcutnpaste	This parameter should appear immeditately following the DRA digits in the CONNECT response.	
Inpsprestype	INP option that indicates the type of message the EAGLE is to send when an IDP message is received for INP service, the DN digits match, and the HLR ID is present.	
Inpsnai1-cdpanai1	Combination of Service Nature of Address Indicator and Called Party Number Nature of Address Indicator. The values for snai and cdpanai must be separated by a hyphen (-). Allowable values for inpsnai1 are [sub,natl,intl,unknown,none] and for cdpanai the range is 0 to 127. 'None' must be specified to unconfigure this parameter.	
Inpsnai2-cdpanai2	Combination of Service Nature of Address Indicator and Called Party Number Nature of Address Indicator. The values for snai and cdpanai must be separated by a hyphen (-). Allowable values for inpsnai1 are [sub,natl,intl,unknown,none] and for cdpanai the range is 0 to 127. 'None' must be specified to unconfigure this parameter.	
Inpsnai3-cdpanai3	Combination of Service Nature of Address Indicator and Called Party Number Nature of Address Indicator. The values for snai and cdpanai must be separated by a hyphen (-). Allowable values for inpsnai1 are [sub,natl,intl,unknown,none] and for cdpanai the range is 0 to 127. 'None' must be specified to unconfigure this parameter.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Inpsnai4-cdpanai4	Combination of Service Nature of Address Indicator and Called Party Number Nature of Address Indicator. The values for snai and cdpanai must be separated by a hyphen (-). Allowable values for inpsnai1 are [sub,natl,intl,unknown,none] and for cdpanai the range is 0 to 127. 'None' must be specified to unconfigure this parameter.	
Inpsnai5-cdpanai5	Combination of Service Nature of Address Indicator and Called Party Number Nature of Address Indicator. The values for snai and cdpanai must be separated by a hyphen (-). Allowable values for inpsnai1 are [sub,natl,intl,unknown,none] and for cdpanai the range is 0 to 127. 'None' must be specified to unconfigure this parameter.	
Gflexmaplayerrtg	G-Flex MAP layer routing. The message parameter used in the database lookup performed during G-Flex MAP layer routing.	
Maplyrrtg_regss	This parameter is use to turn on/off G-flex MLR functionality for Register Supplementary Service.	
Maplyrrtg_actss	This parameter is use to turn on/off G-flex MLR functionality for Active Supplementary Service.	
Maplyrrtg_dactss	This parameter is use to turn on/off G-flex MLR functionality for Deactivate Supplementary Service.	
Maplyrrtg_intss	This parameter is use to turn on/off G-flex MLR functionality for Interrogate Supplementary Service.	
Maplyrrtg_procunstrqt	This parameter is use to turn on/off G-flex MLR functionality for Process Unstructured SS Request.	

Table 5-22 (Cont.) SCCP Mnp Options Elements

Element	Description	Data Input Notes
Maplyrrtg_sriloc	This parameter is use to turn on/off G-flex MLR functionality for Send Routing Information for Location Service.	
Maplyrrtg_purgmobss	This parameter is use to turn on/off G-flex MLR functionality for Purge Mobile Subscriber	
Maplyrrtg_rstdata	This parameter is use to turn on/off G-flex MLR functionality for Restore Data.	
Maplyrrtg_rdyforsm	This parameter is use to turn on/off G-flex MLR functionality for Ready For Short Message.	
Maplyrrtg_authfailrpt	This parameter is use to turn on/off G-flex MLR functionality for Authentication Failure Report.	

You can perform edit task on **VSTP**>**Configuration**>**SCCP Mnp Options** page.

Editing a SCCP Mnp Option

Use this procedure to change the field values for a selected SCCP Mnp Option. :

1. On the **VSTP**>**Configuration**>**SCCP Mnp Options** page, enter the updated values in the input fields.
2. Click **OK**, **Apply**, or **Cancel**

5.1.23 SCCP Options

The SCCP Options are those configuration values that govern the overall SCCP functionality . There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The SCCP Options resources can only be updated. The SCCP Options cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **SCCP Options** page. The page displays the elements on the **SCCP Options** View and Edit pages.

Table 5-23 SCCP Options Elements

Element	Description	Data Input Field
Allow Msg During Rsmbly Err	It specifies whether message will be allowed or discarded during reassembly failure. If alwMsgDuringRsmblyErr is True then message will be forwarded to upper layer for further processing. If alwMsgDuringRsmblyErr is false then message will be discarded and an XUDTS will be generated (provided return on error is set in the XUDT message).	Default - False
Class 1 Message Sequencing	Enables or disables Class 1 message sequencing. When set to Enabled, Class 1 messages are guaranteed to be sequenced, but the messages are not load shared. When set to Disabled, Class 1 message sequencing is not guaranteed, but the messages might be load shared (if appropriate configuration exists).	
Default fallback	Default fallback option. This parameter specifies the action that is taken if the last translation doesn't match when performing GTT using a FLOBR-specific GTT mode. When set to false, GTT fails and the MSU is discarded. When set to true, GTT is performed based on the last matched entry.	Default - False
Default GTT mode	Default GTT mode. The system default value of the GTT mode hierarchy used by the DSR when performing GTT.i	Default - Cd
XUDT Segmentation feature	It specifies whether the XUDT Segmentation feature is enabled. If isSegXUDTfeatureEnable is true then the feature is enabled.	Default - False
MTP Routed GTT	System-wide option for MTP Routed GTT, used to define GTT behavior on MTP Routed MSUs.	Default - Off

Table 5-23 (Cont.) SCCP Options Elements

Element	Description	Data Input Field
MTP Routed GTT fallback	System-wide option for MTP Routed GTT fallback, used to define error handling in case of failure for MTP routed MSUs.	Default - Mtproute
Reassembly timer duration for ANSI	Reassembly timer duration for ANSI domain. Time period after recieving the first segment, while waiting to recieve all the remaining segments related to same ANSI XUDT segmented message.	Default - 5000 , [Minimum,Maximum] - [5000,20000]
Reassembly timer duration for ITU	Reassembly timer duration for ITU domain. Time period after recieving the first segment, while waiting to recieve all the remaining segments related to same ITU XUDT segmented message.	Default - 10000 , [Minimum,Maximum] - [10000,20000]
Length of Segmented MSU	Length of Segmented MSU.	Default - 200 , [Minimum,Maximum] - [200,272]
Transaction-based GTT loadsharing is enabled for UDTS and Class0 UDT messages	When set to Udt, transaction-based GTT loadsharing is enabled for UDTS and Class0 UDT messages. When set to Xudt, transaction-based GTT loadsharing is enabled for XUDTS and Class0 XUDT messages. When set to Both, transaction-based GTT loadsharing is enabled for UDTS, XUDTS, Class0 UDT and Class0 XUDT messages. When set to None, transaction-based GTT loadsharing is disabled for UDTS, XUDTS, Class0 UDT and Class0 XUDT messages. To update this parameter, the Transaction Based GTT Loadsharing feature must be enabled (using the GTT Feature Control (/vstp/featureadminstates)).	

Table 5-23 (Cont.) SCCP Options Elements

Element	Description	Data Input Field
Transaction-based GTT loadsharing is enabled for UDTS and Class1 UDT messages	When set to Udt, transaction-based GTT loadsharing is enabled for UDTS and Class1 UDT messages. When set to Xudt, transaction-based GTT loadsharing is enabled for XUDTS and Class1 XUDT messages. When set to Both, transaction-based GTT loadsharing is enabled for UDTS, XUDTS, Class1 UDT and XUDT messages. When set to None, transaction-based GTT loadsharing is disabled for UDTS, XUDTS, Class1 UDT and Class1 XUDT messages. To update this parameter, the Transaction Based GTT Loadsharing feature must be enabled (using the GTT Feature Control (/vstp/featureadminstates)).	
Transaction parameter for incoming UDT(S) messages	Defines the transaction parameter for incoming UDT(S) messages. Messages with this parameter are routed to the same load-shared remote Point Code within a MAPGROUP or MRNGROUP. When set to Mtp, transaction-based GTT loadsharing is performed using the MTP algorithm. When set to Tcap, transaction-based GTT loadsharing is performed using the TCAP algorithm. When set to Sccp, transaction-based GTT loadsharing is performed using the SCCP algorithm. When set to Enhmtp, transaction-based GTT loadsharing is performed using the ENHMTP algorithm. To update this parameter, the Transaction Based GTT Loadsharing feature must be enabled (using the GTT Feature Control (/vstp/featureadminstates)).	

Table 5-23 (Cont.) SCCP Options Elements

Element	Description	Data Input Field
Transaction parameter for incoming XUDT(S) messages	Defines the transaction parameter for incoming XUDT(S) messages. Messages with this parameter are routed to the same load-shared remote Point Code within a MAPGROUP or MRNGROUP. When set to Mtp, transaction-based GTT loadsharing is performed using the MTP algorithm. When set to Sccp, transaction-based GTT loadsharing is performed using the SCCP algorithm. When set to Enhmtp, transaction-based GTT loadsharing is performed using the ENHMTP algorithm. To update this parameter, the Transaction Based GTT Loadsharing feature must be enabled (using the GTT Feature Control (/vstp/featureadminstates)).	
Velocity of Travelling	Defines the velocity of travelling.	Default - NA , [Minimum,Maximum] - [1,700]

You can perform edit task on **VSTP**>**Configuration**>**SCCP Mnp Options** page.

Editing a SCCP Mnp Option

Use this procedure to change the field values for a selected SCCP Mnp Option. :

1. On the **VSTP**>**Configuration**>**SCCP Mnp Options** page, enter the updated values in the input fields.
2. Click **OK**, **Apply**, or **Cancel**

5.1.24 AINP Options

The AINP Options are those configuration values that govern the overall AINP functionality . There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The AINP Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **AINP Options** page. The page displays the elements on the **AINP Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-24 AINP Options Elements

Element	Description	Data Input Notes
Ainplnpnatldiglen	LNP national digit length.	Default - 10 , [Minimum,Maximum] - [1,15].
Ainpccp	Copy charge parameters. When this parameter has a value of yes, the system copies the Charge Number and Charge Party Station type from an LNP AIN query (if present) to the LNP AIN Response message.	
Ainplnpsubdiglen	LNP subscriber digit length.	Default - 7 , [Minimum,Maximum] - [1,15].
Ainpnec	National Escape Code.	
Ainpdefrn	Default routing number. A default routing number used for own-network subscribers.	
Ainplnpogdnnai	LNP outgoing DN nature of address indicator. This parameter overrides the outgoing Nature of Number if DN is being returned.	
Ainplnpoglrnnai	LNP outgoing LRN nature of address indicator. This parameter overrides the outgoing Nature of Number if LRN is being returned.	
Ainplnpsnai	LNP outgoing LRN nature of address indicator. This parameter overrides the outgoing Nature of Number if LRN is being returned.	
Ainprnai	Routing Nature of Address Indicator.	
Ainprnp	Routing numbering plan.	
Ainpsprestype	SP response type. The type of message sent by the system if an NPREQ message is received, the DN digits match, and the HLR ID is present.	
Ainplnpentpref	LNP entity preference is the first preference for the RTDB data / entity associated with a DN to be used as LRN.	

Table 5-24 (Cont.) AINP Options Elements

Element	Description	Data Input Notes
Ainpsnai1-dialnai1	Combination of Service Nature of Address Indicator and Digits dialed Nature of Address Indicator.	The values for ainpnai and dialnai must be separated by a hyphen (-). Allowable values for ainpnai are [sub,natl,intl,unknown,none] and for dialnai the range is 0 to 1. 'None' must be specified to unconfigure this parameter.
Ainpsnai2-dialnai2	Combination of Service Nature of Address Indicator and Digits dialed Nature of Address Indicator.	The values for ainpnai and dialnai must be separated by a hyphen (-). Allowable values for ainpnai are [sub,natl,intl,unknown,none] and for dialnai the range is 0 to 1. 'None' must be specified to unconfigure this parameter.
Ainprfmt	Routing address format. This parameter specifies the routing address format that is suported in the AINPQ Return Result response messages.	

You can perform edit task on **VSTP**>**Configuration**>**AINP Options** page.

Editing a AINP Option

Use this procedure to change the field values for a selected AINP Option. (The **AINP Option Name** field cannot be changed.):

1. Select the **AINP Option** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.25 SCCP Applications

An Sccp Application is used to trigger an specific application of vSTP.

Select the **VSTP**, and then **Configuration**, and then **SCCP Applications** page. The page displays the elements on the **SCCP Applications** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-25 SCCP Applications Elements

Element	Description	Data Input Notes
Type of Application	Type of Appplication. This is a mandatory field.	Range = Eir, Atinp, Inpq, Sfapp
Sub System Number	Sub System Number. This is a mandatory field.	Range = maximum:255, minimum:2

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP Applications** page.

Adding a SCCP Application

Perform the following steps to configure a new SCCP Application:

1. Click **Insert**.

> **Note:**
>
> The Application Type must be unique across all Application at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP Application

Use this procedure to change the field values for a selected SCCP Application. :

1. Select the **SCCP Application** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP Application

Use the following procedure to delete a SCCP Application.

> **Note:**
>
> A SCCP Application can only be deleted if all delete validation checks pass.

1. Select the **SCCP Application** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.26 SCCP Service Selectors

A Sccp Service Selector is an entity assigned to a Sccp Service.

Select the **VSTP**, and then **Configuration**, and then **SCCP Service Selectors** page. The page displays the elements on the **SCCP Service Selectors** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-26 SCCP Service Selectors Elements

Element	Description	Data Input Notes
Sccp Service Selector Name	Name for this Sccp Service Selector. This is a mandatory field.	Valid names are strings between one and 10 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
Global Title Indicator	Global Title Indicator Conversion. This is a mandatory field.	
Domain Type	Defines the type of incoming message network domain. This is a mandatory field.	Default is Ansi.
Nature of Addres Indicator	Defines Nature of Address indicator for this GTT Selector.	
Nature of Address Indicator Value	Value for the nature of Address indicator.	Maximum: 127, Minimum: 0
Numbering Plan	Defines Numbering plan (NP) for this GTT Selector.	
Numbering Plan Value	Value for the numbering plan.	
Translation Type	Defines the translation type (TT) for this Service Selector. This is a mandatory field.	Maximum: 255, Minimum: 0 [
Service Subsystem Number	Service Subsystem number. This is a mandatory field.	
Service Interprated Nature of address Indicator	Defines the Service Interpreted Nature of address Indicator.	
Service Interprated Numbering Plan	Defines the Service Interpreted Numbering Plan	
Service Name	Service Name Associated with service. This is a mandatory field.	

Table 5-26 (Cont.) SCCP Service Selectors Elements

Element	Description	Data Input Notes
If message should fallback to GTT after Service?	Defines if message should fallback to GTT after Service.	Default: false

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP Service Selectors** page.

Adding a SCCP Service Selector

Perform the following steps to configure a new SCCP Service Selector:

1. Click **Insert**.

> **Note:**
>
> he Sccp Service Selector name must be unique as it refers to the Service name at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP Service Selector

Use this procedure to change the field values for a selected SCCP Service Selector. (The **SCCP Service Selector Name** field cannot be changed.):

1. Select the **SCCP Service Selector** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP Service Selector

Use the following procedure to delete a SCCP Service Selector.

> **Note:**
>
> if the Sccp Service Selector is associated with a Service , the Sccp Service Selector cannot be deleted.

1. Select the **SCCP Service Selector** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.27 SCCP Loop Sets

A SCCP Loop Sets define all the data related to SccpLoopSet entry.

Select the **VSTP**, and then **Configuration**, and then **SCCP Loop Sets** page. The page displays the elements on the **SCCP Loop Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-27 SCCP Loop Sets Elements

Element	Description	Data Input Notes
Action	Action to be taken when Sccp Loop is detected.	Format: Drop down menu Range = notifyOnly, discardOnly
Domain	Defines the type of incoming message network domain. This is a mandatory field.	Format: Drop down menu Range = Ansi Itun Itui Itun24 Itui_s Itun_s Itun16
Loop Set Name	Name for this Sccp loopset, which must be unique within the VSTP site. This is a mandatory field.	Valid names are strings between one and 10 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
Point Code 1	List of signaling Pointcodes.	
Point Code 2	List of signaling Pointcodes.	
Point Code 3	List of signaling Pointcodes.	
Point Code 4	List of signaling Pointcodes.	
Point Code 5	List of signaling Pointcodes.	
Point Code 6	List of signaling Pointcodes.	
Point Code 7	List of signaling Pointcodes.	
Point Code 8	List of signaling Pointcodes.	
Point Code 9	List of signaling Pointcodes.	
Point Code 10	List of signaling Pointcodes.	
Point Code 11	List of signaling Pointcodes.	
Point Code 12	List of signaling Pointcodes.	

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**SCCP Loop Sets** page.

Adding a SCCP Loop set

Perform the following steps to configure a new SCCP Loop set:

1. Click **Insert**.

> **Note:**
>
> he SCCP Loop set name must be unique as it refers to the Service name at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SCCP Loop set

Use this procedure to change the field values for a selected SCCP Loop set. (The **SCCP Loop set Name** field cannot be changed.):

1. Select the **SCCP Loop set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SCCP Loop set

Use the following procedure to delete a SCCP Loop set.

> **Note:**
>
> if the SCCP Loop set is associated with a Service , the SCCP Loop set cannot be deleted.

1. Select the **SCCP Loop set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.28 NPP Action Sets

A Numbering Plan Processor (NPP) Action Set is a collection of Conditioning Actions (CAs), Service Actions (SAs), and Formatting Actions (FAs).

Select the **VSTP**, and then **Configuration**, and then **NPP Action Sets** page. The page displays the elements on the **NPP Action Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-28 NPP Action Sets Elements

Element	Description	Data Input Notes
NPP Action Set Name	Name for this NPP Action Set. This is a mandatory field.	Valid names are strings between one and 10 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.
CA List	Conditioning Action list. This CA list can be applied to an incoming digit string. Up to 12 CAs can be specified in the list. The CAs are processed in the order they are specified in the list.	Range = "Ac1", "Ac2", "Ac3", "Ac4", "Ac5", "Ac6", "Ac7", "Ac8","Accgpn", "Accgpn1", "Accgpn2","Accgpn3","Accgpn4","Accgpn5","Accgpn6","Accgpn7","Accgpn8", "Acdef", "Aclac", "Cc1", "Cc2", "Cc3", "Ccdef","Cccgpn","Dn1","Dn2", "Dn3","Dn4","Dn5","Dn
SA List	Service Action list. This SA list can be applied to an incoming digit string. Up to 8 SAs can be specified in the list. The SAs must be specified in high-to-low precedence order in the list, and cannot be duplicated in the list.	Range = "Asdlkup", "Blklstqry", "Blklstrly", "Blnfndrls", "Blrls", "Cdial", "Ccncchk", "Cdpnnp", "Cgpnasdrqd", "Cgpngrnrqd", "Cgpnnp", "Cgpnrtg", "Cgpnsvcrqd", "Crp", "Fpfxrls", "Fraudchk", "Fwdscs", "Grnlkup", "Inprtg", "Lacck", "Migrate", "Nocgpnrls", "Npnrls", "Nprelay", "Nprls", "Nscgpn", "Nscdpn", "Pprelay", "Rtdbtrn", "Rtdbtsp", "Rtdbtrnsp", "Skgtartg", "Snscgpn"
FA List	Formatting Action list. This FA list can be applied to the outgoing digit string. Up to 12 FAs can be specified in the list. The FAs are processed in the order they are specified in the list and cannot be duplicated.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
Fane	Formatting Action list type Fane. Formatting Action List when the SP and RN entities are not associated with the DN in the RTDB.	[Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"]
Fanf	Formatting Action list type Fanf. Formatting Action when the DN is not present in the RTDB.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"
Farn	Formatting Action list type Farn. Formatting Action List when the RN network entity is associated with the DN in the RTDB.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"
Fasp	Formatting Action list type Fasp. Formatting Action List when the SP network entity is associated with the DN in the RTDB.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
Fascrcd	Formatting Action list type Fascrcd. Formatting Action List to format ISUP CdPN digits when CdPN is Screened and SA(X)VAL is none.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"
Fascrcg	Formatting Action list type Fascrcg. Formatting Action List to format ISUP CgPN digits when CdPN is Screened and SA(X)VAL is none.	Range = "Ac", "Asd", "Asdother", "Cc", "Dlma", "Dlmb", "Dlmc", "Dlmd", "Dlme", "Dlmf", "Dlmg", "Dlmh", "Dlmi", "Dlmj", "Dlmk", "Dlml", "Dlmm", "Dlmn", "Dlmo", "Dlmp", "Dn", "Fpfx", "Grn", "Grnother", "Orig", "Pfxa", "Pfxb", "Pfxc", "Pfxd", "Pfxe", "Pfxf", "Rn", "Rnospodn", "Rnosposn", "Rnospozn", "Sn", "Sp", "Srfimsi", "Vmid", "Zn"
SA 1 Numerical Value	Service Action 1 numerical values list. A comma-separated numerical values list that can be used with the first SA. Two values can be provided at maximum	Range = 0-65534
SA 2 Numerical Value	Service Action 2 numerical values list. A comma-separated numerical values list that can be used with the second SA. Two values can be provided at maximum[	Range = 0-65534
SA 3 Numerical Value	Service Action 3 numerical values list. A comma-separated numerical values list that can be used with the third SA. Two values can be provided at maximum	Range = 0-65534
SA 4 Numerical Value	Service Action 4 numerical values list. A comma-separated numerical values list that can be used with the fourth SA. Two values can be provided at maximum	Range = 0-65534

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
SA 5 Numerical Value	Service Action 5 numerical values list. A comma-separated numerical values list that can be used with the fifth SA. Two values can be provided at maximum	Range = 0-65534
SA 6 Numerical Value	Service Action 6 numerical values list. A comma-separated numerical values list that can be used with the sixth SA.	Range = 0-65534
SA 7 Numerical Value	Service Action 7 numerical values list. A comma-separated numerical values list that can be used with the seventh SA.	Range = 0-65534
SA 8 Numerical Value	Service Action 8 numerical values list. A comma-separated numerical values list that can be used with the eighth SA. Two values can be provided at maximum.	Range = 0-65534
SA 1 Digit String	Service Action 1 digit string. This parameter specifies a digit string that can be used with the first SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 2 Digit String	Service Action 2 digit string. This parameter specifies a digit string that can be used with the second SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 3 Digit String	Service Action 3 digit string. This parameter specifies a digit string that can be used with the third SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 4 Digit String	Service Action 4 digit string. This parameter specifies a digit string that can be used with the fourth SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 5 Digit String	Service Action 5 digit string. This parameter specifies a digit string that can be used with the fifth SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 6 Digit String	Service Action 6 digit string. This parameter specifies a digit string that can be used with the sixth SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
SA 7 Digit String	Service Action 7 digit string. This parameter specifies a digit string that can be used with the seventh SA.	Range = a-f,A-F, 0-9 Maximum Length = 8

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
SA 8 Digit String	Service Action 8 digit string. This parameter specifies a digit string that can be used with the eighth SA.	Range = a-f,A-F, 0-9 Maximum Length = 8
OFNAI	Outgoing filter nature of address indicator. The filter nature of address indicator (FNAI) class of the outgoing digit string.	Range = 'Intl', 'Natl', 'Nai1', 'Nai2', 'Nai3', 'Unkn', 'Inc'

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**NPP Action Sets** page.

Adding a NPP Action Set

Perform the following steps to configure a new NPP Action Set:

1. Click **Insert**.

> **Note:**
> The set name must be unique across all NPP Action Sets at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a NPP Action Set

Use this procedure to change the field values for a selected NPP Action Set. (The **NPP Action Set Name** field cannot be changed.):

1. Select the **NPP Action Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a NPP Action Set

Use the following procedure to delete a NPP Action Set.

> **Note:**
> NPP Action Set cannot be removed if it is being used by NPP Service Rule Set.

1. Select the **NPP Action Set** to be deleted.

2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.29 NPP Service Rule Sets

A A NPP Service Rule Set (SRS) is a collection of NPP Rules that are associated with a NPP Service (/vstp/nppservices). A NPP Rule is an association between a single NPP filter and a single NPP Action Set(/vstp/nppactionsets).

Select the **VSTP**, and then **Configuration**, and then **NPP Service Rule Sets** page. The page displays the elements on the **NPP Service Rule Sets** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-29 NPP Service Rule Sets Elements

Element	Description	Data Input Notes
Service	Name for this NPP Service Rule Set. This is a mandatory field.	Range = 'Idprcdpn', 'Idprcgpn', 'Mosmsgcdpn', 'Mosmsgcgpn', 'Idprcdpn2', 'Idprcdpn3', 'Idprcdpn4'] [A value is required.
FNAI	Filter nature of address indicator. The filter Nature of Address Indicator (NAI) class. This is a mandatory field.	Range = 'Unkn', 'Intl', 'Natl', 'Nai1', 'Nai2', 'Nai3'] [A value is required.
Service	Filter prefix. The prefix used to filter incoming digit strings. This is a mandatory field.	Range = Valid characters are a-f, A-F, 0-9, question mark(?)and asterik(*). Maximum allowed length is 16 and the regular expression to be followed : ^([a-fA-F0-9]*)$\|^([A-Fa-f0-9]*(\?){0,15}[a-fA-F0-9])*$|^(*)$] [A value is required.
FNAI	Filter digit length. This parameter specifies the number of digits on the incoming digit string that is filtered by the NPP. This is a mandatory field.	Range = Valid characters are 0-9 and asterik(*). Maximum allowed length is 32 and the regular expression to be followed : ^(*)$\|^([0-9]*)$] [A value is required.
FPFX	Action set name. This parameter specifies the name of the AS. This is a mandatory field.	Range = Allowable values are 1 alphabetic character followed by up to 9 alphanumeric characters.] [A value is required.

Table 5-29 (Cont.) NPP Service Rule Sets Elements

Element	Description	Data Input Notes
FDL	Invoke service name. The name of the NPP service to be invoked. This is a mandatory field.	Default = 'None'; Range = 'None', 'Idprcdpn', 'Idprcgpn', 'Mosmsgcdpn', 'Mosmsgcgpn', 'Idprcdpn2', 'Idprcdpn3', 'Idprcdpn4'

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**NPP Service Rule Sets** page.

Adding a NPP Service Rule Set

Perform the following steps to configure a new NPP Service Rule Set:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a NPP Service Rule Set

Use this procedure to change the field values for a selected NPP Service Rule Set. (The **NPP Service Rule Set Name** field cannot be changed.):

1. Select the **NPP Service Rule Set** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a NPP Service Rule Set

Use the following procedure to delete a NPP Service Rule Set.

> **Note:**
>
> Npp Service Rule Set can only be deleted if all delete validation checks pass.

1. Select the **NPP Service Rule Set** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.30 NPP Services

Numbering Plan Processor (NPP) service entry uses the NPP to assist with the processing of digit strings.

The NPP Services can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **NPP Services** page. The page displays the elements on the **NPP Services** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-30 NPP Services Elements

Element	Description	Data Input Notes
SRVN	The name of the NPP Service.	The name cannot be changed. Range: tif, tif2, tif3, tifcgpn, tifcgpn2, tifcgpn3
DLMA	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMB	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMC	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMD	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLME	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMF	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMG	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMH	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf

Table 5-30 (Cont.) NPP Services Elements

Element	Description	Data Input Notes
DLMI	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMJ	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMK	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLML	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMM	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMN	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMO	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
DLMP	A delimiter that is used to format the outgoing dialed number.	1-16 hexadecimal digits. Valid digits are 0-9, a-f, A-F. none - deletes the current value of the delimiter. For example - adf123,123adf
INTL	International. This parameter maps an International FNAI class to the NAI of the incoming digit string.	[Min,Max] = [0,255] and none. Default - No change to the current value
NAI1	This parameter maps an NAI-1 FNAI class to the NAI of the incoming digit string.	; [Min,Max] = [0,255] and none. Default - No change to the current value
NAI2	This parameter maps an NAI-2 FNAI class to the NAI of the incoming digit string.	; [Min,Max] = [0,255] and none. Default - No change to the current value

Table 5-30 (Cont.) NPP Services Elements

Element	Description	Data Input Notes
NAI3	This parameter maps an NAI-3 FNAI class to the NAI of the incoming digit string.	; [Min,Max] = [0,255] and none. Default - No change to the current value
NATL	This parameter maps a National FNAI class to the NAI of the incoming digit string.	; [Min,Max] = [0,255] and none. Default - No change to the current value
Rule Count	This parameter configures count of NPP Rules.	DEFAULT = 0, [MIN,MAX] = [0,4096]
Status*	This parameter specifies whether the service can be processed by the NPP.	Default - Off [A value is required.]
SDWC Count	This parameter configures count of SDWC.	DEFAULT = 0, [MIN,MAX] = [0,25]
UNKN	This parameter maps an Unknown FNAI class to the NAI of the incoming digit string.	DEFAULT = 0, [MIN,MAX] = [0,255]

You can perform edit task on **VSTP**>**Configuration**>**NPP Services** page.

Editing a NPP Service

Use this procedure to change the field values for a selected NPP Service. (The **NPP Service Name** field cannot be changed.):

1. Select the **NPP Service** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.31 PPS Relays

Prepaid Short Message Service relays (PPSRELAY). This creates the PPSOPTS entries that correspond to Intelligent Network (IN) platforms.

Select the **VSTP**, and then **Configuration**, and then **PPS Relays** page. The page displays the elements on the **PPS Relays** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-31 PPS Relays Elements

Element	Description	Data Input Notes
Prepaid Portablility Type	Prepaid portability type. The IN platform where the incoming message is sent. Either PPT or GTA can be specified at a time. This is a mandatory field.	Valid entry is an integer. Maximum: 32, Minimum: 1
Global Title Address	Global title address. The entity address for an IN platform. Determines whether an incoming message receives PPSMS screening.	Either PPT or GTA can be specified at a time. Valid entry is a hexadecimal number of upto 15 digits
Remote Signaling Point Name	Defines the Remote Signaling Point name.	
Routing Indicator	Routing indicator. The IN platform routing indicator.	
Map Set ID / MRN Set ID	Set ID. The MAP set ID.	
Subsystem Number	The Subsystem number.	Range=maximum: 255, minimum: 2

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**PPS Relays** page.

Adding a PPS Relay

Perform the following steps to configure a new PPS Relay:

1. Click **Insert**.

> **Note:**
>
> The PPT and GTA value must be unique across all PPS Relays at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a PPS Relay

Use this procedure to change the field values for a selected PPS Relay. (The **Prepaid Portablility Type** and **Global Title Address** fields cannot be changed.):

1. Select the **PPS Relay** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a PPS Relay

Use the following procedure to delete a PPS Relay.

1. Select the **PPS Relay** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.32 Common Screening Lists

A Common Screening List (CSL) is a collection of screening entries for the specified feature and screening list name, or a specific DS(digit string) for a particular feature and screening list name.

Select the **VSTP**, and then **Configuration**, and then **Common Screening Lists** page. The page displays the elements on the **Common Screening Lists** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-32 Common Screening Lists Elements

Element	Description	Data Input Notes
Digit String	Digit string. A unique string of digits that is used by the specified screening feature.	
Feature	The name of the enabled feature for which the command is entered.	
List	The name of the Common Screening List associated with the feature. This is a mandatory field.	'default': 'lmsipfx'
P1	Parameter Value 1. This parameter is specific to the feature and list that use the parameter.	Allowed values are prepaid1 contibued to prepaid32 and prepaidno.
P2	Parameter Value 2.	Allowed values are idprcdpn, idprcdpn2, idprcdpn3, idprcdpn4 only. {'default': 'idprcdpn'}
Scpgta	Signaling Control Point (SCP) Global Title Address (GTA).	Range: 1 - 21 digits, none (1 - 21 hexadecimal digits. Valid digits are 0-9, a-f, A-F)

You can perform add, edit, or delete tasks on **VSTP**>**Configuration**>**Common Screening Lists** page.

Adding a Common Screening List

Perform the following steps to configure a new Common Screening List:

1. Click **Insert**.

> **Note:**
>
> The Common Screening List name must be unique across all Common Screening Lists at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Common Screening List

Use this procedure to change the field values for a selected Common Screening List:

1. Select the **Common Screening List** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Common Screening List

Use the following procedure to delete a Common Screening List.

1. Select the **Common Screening List** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.33 TIF Options

Select the **VSTP**, and then **Configuration**, and then **TIF Options** page. The page displays the elements on the **TIF Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-33 TIF Options Elements

Element	Description	Data Input Notes
CondCGPN	The preconditioning required when a CgPN lookup is needed.	Default='None' Range = 'Addcc', 'None'

Table 5-33 (Cont.) TIF Options Elements

Element	Description	Data Input Notes
CRPREL	The ISUP Release cause for a message that is determined to be circular routed.	Default=31 Range = 0-255
Default Routing Number	Default routing number. This parameter provides a set of digits to substitute for a signaling point.This parameter is used with both calling party and called party numbers.	Default: 'None' Range = a-f, A-F, 0-9 and Maximum Length = 15
DLMA	Delimiter A. The digits used for Delimiter A in an NPP Formatting Action.	Default='None' Range = a-f, A-F, 0-9 and Maximum Length = 16
DLMB	Delimiter B. The digits used for Delimiter B in an NPP Formatting Action.	Default='None' Range = a-f, A-F, 0-9 and Maximum Length = 16
DLMC	Delimiter C. The digits used for Delimiter C in an NPP Formatting Action.	Default='None' Range = a-f, A-F, 0-9 and Maximum Length = 16
IAMCGPN	The format of the outgoing CgPN digits.	Default='Dn' Range : 'Rn', 'Rndn', 'Dn'
MATCHSEQ	The DN lookup mechanism.	Default='Dn' Range = 'Nptype', 'Dn'

Table 5-33 (Cont.) TIF Options Elements

Element	Description	Data Input Notes
NPFLAG	This parameter specifies whether the nm parameter is modified in the IAM message to show that NP lookup has been performed. The nm parameter exists only in incoming and outgoing IAM messages.	Default='None' Range = 'None', 'Nm'
NPTYPECGPN	NP entity type for the CgPN. The entity type of the DN that is used to indicate that a successful NP lookup occurred.	Default='Sprn' Range = 'Sp', 'Rn', 'Sprn', 'All', 'Rnspdn', 'Any'
NPTYPERLS	The entity type of the DN that is used to indicate that a successful NP lookup occurred for the NPRLS and NPNRLS Service Actions.	Default='Sprn' Range = 'Sp', 'Rn', 'Sprn', 'All', 'Rnspdn', 'Any'
NPTYPERLY	The entity type of the DN that is used to indicate that a successful NP lookup occurred for the NPRELAY Service Action.	Default='Sprn' and Range = 'Sp', 'Rn', 'Sprn', 'All', 'Rnspdn', 'Any'
NSADDLDATA	This parameter specifies whether the incoming IAM Calling Party Category should be compared with the value for the nspublic parameter before performing Calling Party number substitution.	Default='No' and Range = 'Yes', 'No'

Table 5-33 (Cont.) TIF Options Elements

Element	Description	Data Input Notes
NSPUBLIC	The value of the Calling Party Category that indicates that the Calling Party number is public.	Default=0 and Range = 0-255
RCAUSENP	The value used for the release cause in an REL message when number portability occurs.	Default=0 and Range = 0-127
RCAUSEPFX	The value used for the release cause in an REL message when number portability does not occur.	Default=0 and Range = 0-127
RLCOPC	This parameter specifies whether the value specified for the rcause parameter overrides the values specified for the rcausenp and rcausepfx parameters.	Default='Off' and Range = 'Off', 'On'
RNRQD	This parameter specifies whether the redirection number is included in the release message when release handling is indicated.	Default='Yes' and Range = 'Yes', 'No'
SNSCGPNDFLT	The digits to be used in calling number simple number substitution.	Default='None' and Range = a-f, A-F, 0-9 and Maximum Length = 32
SPFILL	This parameter specifies whether the sp entity type is populated if the value specified for the defltrn or grn parameter is used for NPP processing.	Default='Off' and Range = 'Off', 'On'

Table 5-33 (Cont.) TIF Options Elements

Element	Description	Data Input Notes
SPLITIAM	This parameter specifies when to split the IAM into IAM + 1 SAM.	Default='None' and Range = 15-31

You can perform edit task on **TIF Options** page.

Editing a Common Screening List

Use this procedure to change the field values for a selected Common Screening List:

1. Select the **TIF Options** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.34 IDPR Options

The Initial Detection Point Relay (IDPR) Options are those configuration values that govern the overall IDPR SMS. There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The IDPR Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **IDPR Options** page. The page displays the elements on the **IDPR Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-34 IDPR Options Elements

Element	Description	Data Input Notes
Cdcnp	Specifies whether the CutAndPaste parameter is included in the CONNECT message generated by the INPRTG Service Action based on the CdPN RTDB lookup.	Default='Off' Range= On,Off
Cddnnotfndrsp	The system response for an IDP message processed by the IDPR/TTR service when the Called Party Number (CdPN) is not found in the RTDB.	Default='Release' Range= Connect, Continue, Relay, Release

Table 5-34 (Cont.) IDPR Options Elements

Element	Description	Data Input Notes
Cddra	The destination routing address (DRA) used in the CONNECT message generated by the INPRTG Service Action based on the CdPN RTDB lookup.	Default='Rndn' Range=Rn, Rndn, Grn, Rnasd, Asdrn, Rngrn, Grnrn, Ccrndn, Rnasddn, Asdrndn, Ccrnasddn, Ccasdrndn, Asdrnccdn, Rnasdccdn, Rngrndn, Grnrndn, Ccrngrndn, Ccgrnrndn, Grnrnccdn, Rngrnccdn, Grndn, Ccgrndn
Cddranai	The DRA nature of address indicator used in the CONNECT response generated by the INPRTG Service Action based on the CdPN RTDB lookup.	Default='Natl' Range='Sub', 'Unknown', 'Natl', 'Intl', 'Ntwk'
Cddranp	The DRA numbering plan used in the CONNECT response generated by the INPRTG Service Action based on the CdPN RTDB lookup.	Default='E164' Range='E164', 'X121', 'F69'
Cdnoentityrsp	The system response for an IDP message processed by the IDPR/TTR service when neither the RN nor SP entity is found in the CdPN RTDB.	Default='Continue' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cdrelcause	The cause parameter value for the RELEASECALL message generated by the INPRTG Service Action based on the CdPN RTDB lookup.	Default=31 Range= 1-127
Cdrnrsp	The system response for an IDP message processed by the IDPR/TTR service when the CdPN is associated with an RN entity.	Default='Connect' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cdsprsp	The system response for an IDP message processed by the IDPR/TTR service when the CdPN is associated with an SP entity.	Default='Relay' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cgcnp	Specifies whether the CutAndPaste parameter is included in the CONNECT message generated by the INPRTG Service Action based on the CgPN RTDB lookup.	Default='Off' Range= 'On','Off'

Table 5-34 (Cont.) IDPR Options Elements

Element	Description	Data Input Notes
Cgdnnotfndrsp	The system response for an IDP message processed by the IDPR/TTR service when the Calling Party Number (CgPN) is not found in the RTDB.	Default='Release' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cgdra	The DRA used in the CONNECT response generated by the INPRTG Service Action based on the CGPN RTDB lookup.	Default='Rndn' Range='Rn', 'Rndn', 'Grn', 'Rnasd', 'Asdrn', 'Rngrn', 'Grnrn', 'Ccrndn', 'Rnasddn', 'Asdrndn', 'Ccrnasddn', 'Ccasdrndn', 'Asdrnccdn', 'Rnasdccdn', 'Rngrndn', 'Grnrndn', 'Ccrngrndn', 'Ccgrnrndn', 'Grnrnccdn', 'Rngrnccdn', 'Grndn', 'Ccgrndn'
Cgdranai	The NAI option used in the CONNECT response generated by the INPRTG Service Action based on the CgPN lookup.	Default='Natl' Range='Sub', 'Unknown', 'Natl', 'Intl', 'Ntwk'
Cgdranp	The DRA NP used in the CONNECT response generated by the INPRTG Service Action based on the CgPN lookup.	Default='E164' Range='E164', 'X121', 'F69'
Cgnoentityrsp	The system response for an IDP message processed by the IDPR/TTR service when neither the RN nor SP entity is found in the CgPN RTDB.	Default='Continue' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cgnptype	CgPN database lookup type. The entity type that is considered a success when used for RTDB lookup.	Default='Rnsp' Range= 'Sp', 'Rn', 'Rnsp', 'Anymatch', 'Always', 'Rnspdn'
Cgpaccck	CgPA country code check. This parameter specifies whether a DEFCC check is performed on the incoming CgPA.	Default='Nonintl' Range= 'Nonintl', 'Off', 'Always'
Cgpnskrtg	This parameter specifies whether SK routing occurs if IDP A-Party routing fails.	Default='No' Range= 'No', 'Yes'
Cgrelcause	The cause parameter value in the RELEASECALL message generated by an INPRTG Service Action based on the CgPN RTDB lookup.	Default=31 Range= 1-127

Table 5-34 (Cont.) IDPR Options Elements

Element	Description	Data Input Notes
Cgrnrsp	The system response for an IDP message processed by the IDPR/TTR service when the CgPN is associated with an RN entity.	Default='Connect' Range= 'Connect', 'Continue', 'Relay', 'Release'
Cgsnai	Calling party number nature of address indicator. The CgPN NAI that is used during number conditioning.	Default='Incoming' Range='Incoming', 'Unkn', 'Natl', 'Intl'
Cgsprsp	The system response for an IDP message processed by the IDPR/TTR service when the CgPN is associated with an RN entity.	Default='Connect' Range= 'Connect', 'Continue', 'Relay', 'Release'
Dfltrn	Default routing number. The default RN used when a value of sp or rnsp is specified for the nptype parameter, and the CdPN RTDB lookup returns entity type SP.	Default='None' Range= a-f, A-F, 0-9, 'None', Maximum Length=15
Dlma	Delimiter A. The first delimiter used to format the outgoing TCAP DN.	Default='None' Range= a-f, A-F, 0-9, 'None', Maximum Length = 16
Dlmb	Delimiter B. The second delimiter used to format the outgoing TCAP DN.	[Default='None', Range= a-f, A-F, 0-9, 'None', Maximum Length = 16]
Dlmc	Delimiter C. The third delimiter used to format the outgoing TCAP DN.	[Default='None', Range= a-f, A-F, 0-9, 'None', Maximum Length = 16]
Drafrmt	DRA digit format. The format of the DRA digits.	[Default='Grn', Range= 'Grn', 'Grndn', 'Dngrn', 'Ccgrndn', 'Grnccdn']
Dranai	DRA nature of address indicator. The DRA NAI that is used during number conditioning.	[Default=3, Range= 1-127]
Nai2ton	NAI to TON Mapping. NAI and TON values are separated by '-'. Multiple mappings can be provided separated by ','.	[Range= Valid values for NAI lies between 1 to 127. Valid values for TON lies between 0 and 7.]
Nptype	Entity type for CdPN RTDB lookup. The entity type that is considered a success when used for RTDB lookup.	[Default='Rnsp', Range= 'Sp', 'Rn', 'Rnsp', 'Anymatch', 'Always', 'Rnspdn']
Rnspfill	This parameter specifies whether the RN and SP entities are set to the value of the RN or SP digits from the RTDB when certain conditions are met.	[Default='Off', Range= 'On','Off']

Table 5-34 (Cont.) IDPR Options Elements

Element	Description	Data Input Notes
Spfill	This parameter specifies whether the SP entity type is populated if the value specified for the dfltrn or grn parameter is used for NPP processing.	[Default='Off', Range= 'On','Off']
Snai	CdPN nature of address indicator. The CdPN NAI used during number conditioning.	[Default='Incoming', Range='Incoming', 'Unkn', 'Natl', 'Intl']
Ton2nai	TON to NAI Mapping. TON and NAI values are separated by '-'. Multiple mappings can be provided separated by ','.	[Range= Valid value for TON lies between 0 and 7. Valid values for NAI lies between 1 to 127.]

You can perform edit task on **VSTP**>**Configuration**>**IDPR Options** page.

Editing an IDPR Option

Use this procedure to change the field values for a selected IDPR Option.:

1. Select the **IDPR Option** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.35 Interface Mapping

An Interface Mapping is a mapping between MTP2 and PCI interfaces.

Select the **VSTP**, and then **Configuration**, and then **Interface Mapping** page. The page displays the elements on the **Interface Mapping** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-35 Interface Mapping Elements

Element	Description	Data Input Notes
Channel Name *	This is the name assigned to interface mapping.	[Default = n/a; Range = Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.] [A value is required.]
Link Type *	This defines the types of links which are added in VSTP.	[Default = n/a; Range = T1, E1, E1_hsl, T1_hsl] [A value is required.]
Speed *	This defines the type of speed enums and their corresponding values.	[Default = n/a; Range = Lsl_56k, Lsl_64k, Hsl_2048k, Hsl_1536k] [A value is required.]
Host Name *	The hostName is the name of the server associated with the interface mapping.	[Default = n/a; Range = Valid names are strings between one and 40 characters, inclusive. Valid characters are alphanumeric and hyphen. The name must start with one alphanumeric and must not start with a hyphen.] [A value is required.]
Time Slot	This defines the time slot. Zero is not allowed value.	[Default = n/a; Range = 1-31]
Port	The defines the value of port assigned to interface mappping. This is a mandatory field.	[Default = n/a; Range = 0-7]
Sequence Length	This defines the sequence bit length of the link.	[Default = n/a; Range = 7_BIT, 10_BIT, 12_BIT]

You can perform add, edit, or delete tasks on **VSTPConfigurationInterface Mapping** page.

Adding an Interface Mapping

Perform the following steps to configure a new Interface Mapping:

1. Click **Insert**.

> **Note:**
>
> The new Interface Mapping must have a name that is unique across all Interface Mapping at the SOAM. In addition, the Interface Mapping's IP Port combination must also be unique across all Interface Mapping configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Interface Mapping

Use this procedure to change the field values for a selected Interface Mapping. (The **Interface Mapping Name** field cannot be changed.):

1. Select the **Interface Mapping** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Interface Mapping

Use the following procedure to delete a Interface Mapping.

> **Note:**
>
> You cannot delete a Interface Mapping if it is part of the configuration of one or more Linksets.

1. Select the **Interface Mapping** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.36 M2PA Config

A M2pa Config is an entity to configure all the m2pa timers.

Select the **VSTP**, and then **Configuration**, and then **M2PA Config** page. The page displays the elements on the **M2PA Config** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-36 M2PA Config Elements

Element	Description	Data Input Notes
Name	Name for this M2PA Config, which must be unique within the VSTP site. This is a mandatory field.	Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. [A value is required.]

Table 5-36 (Cont.) M2PA Config Elements

Element	Description	Data Input Notes
T1 Timer	Timer 1 - Changeover delay. Also used as isolation timer for ITU MTP Restart.	Typical value is 10000. default: 10000, minimum: 1000, maximum: 350000
T2 Timer	Timer 2 - Wait for changeover acknowledgement (COA).	Typical value is 2000. default: 10000, minimum: 5000, maximum: 15000
T3 Timer	Timer 3 - Time controlled diversion on changeback	. Typical value is 2000. default: 10000, minimum: 1000, maximum: 60000
T4 Emergency Timer	Timer 4 - Emergency Proving Timer.	Typical value is 500. default: 500, minimum: 400, maximum: 5000
T4 Normal Timer	Timer 4 - Normal Proving Timer.	Typical value is 10000. default: 10000, minimum: 1000, maximum: 70000
T5 Timer	Timer 5 - Wait for changeback acknowledgement (CBA) #2.	Typical value is 100. default: 1000, minimum: 80, maximum: 10000
T6 Timer	Timer 6 - Controlled reroute.	Typical value is 3000. default: 3000, minimum: 1000, maximum: 6000
T7 Timer	Timer 7 - Excessive acknowledgement delay timer.	Typical value is 1200. default: 1200, minimum: 200, maximum: 2000
T16 Timer	Timer 16 - Wait for route set congestion test (RSCT) updates.	Typical value is 200000. default: 200000, minimum: 100, maximum: 500000
T17 Timer	Timer 17 - Delay to avoid oscillation of initial alignment failure.	Typical value is 250. default: 250, minimum: 100, maximum: 500

You can perform add, edit, or delete tasks on **VSTPConfigurationM2PA Config** page.

Adding a M2PA Config

Perform the following steps to configure a new M2PA Config:

1. Click **Insert**.

> **Note:**
>
> The new M2PA Config must have a name that is unique across all M2PA Config at the SOAM. In addition, the M2PA Config's IP Port combination must also be unique across all M2PA Config configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a M2PA Config

Use this procedure to change the field values for a selected M2PA Config. (The **M2PA Config Name** field cannot be changed.):

1. Select the **M2PA Config** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a M2PA Config

Use the following procedure to delete a M2PA Config.

> **Note:**
>
> You cannot delete a M2PA Config if it is part of the configuration of one or more Linksets.

1. Select the **M2PA Config** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.37 M3UA Config

A M3ua Config is an entity to configure all the m3ua timers.

Select the **VSTP**, and then **Configuration**, and then **M3UA Config** page. The page displays the elements on the **M3UA Config** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-37 M3UA Config Elements

Element	Description	Data Input Notes
Name	Name for this Mtp2 Config, which must be unique within the VSTP site. This is a mandatory field.	Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit.

Table 5-37 (Cont.) M3UA Config Elements

Element	Description	Data Input Notes
Excessive acknowledgement delay time	Excessive acknowledgement delay timer. The amount of time (in milliseconds) for which M2PA waits between transmission of a user data message and receipt of an acknowledgement for that message from the peer. If this timer expires, the link is taken out of service.	Typical value is 300. Minimum 500, Maximum: 10000

You can perform add, edit, or delete tasks on **VSTPConfigurationM3UA Config** page.

Adding a M3UA Config

Perform the following steps to configure a new M3UA Config:

1. Click **Insert**.

> **Note:**
>
> The new M3UA Config must have a name that is unique across all M3UA Config at the SOAM. In addition, the M3UA Config's IP Port combination must also be unique across all M3UA Config configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a M3UA Config

Use this procedure to change the field values for a selected M3UA Config. (The **M3UA Config Name** field cannot be changed.):

1. Select the **M3UA Config** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a M3UA Config

Use the following procedure to delete a M3UA Config.

> **Note:**
>
> You cannot delete a M3UA Config if it is part of the configuration of one or more Linksets.

1. Select the **M3UA Config** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.38 M3rl Options

The Message Transfer Part level 3 (MTP3) Options are configuration values that govern the overall MTP3 functionality.

The M3rl Options resources can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **M3rl Options** page. The page displays the elements on the **M3rl Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-38 M3rl Options Elements

Element	Description	Data Input Notes
CnvAInat	This parameter sets the value of the called party/calling party address Reserved for National Use bit when the message is routed to the ITU national network.	Default - 1 , Minimum,Maximum - 0,1
CnvCgda	This parameter enables discarding of the CGPA point code in SCCP messages if the destination network type is Ansi, and the point code or alias point code of the destination network type is not defined.	
CnvCgdi	This parameter enables discarding of the CGPA point code in SCCP messages if the destination network type is Itui, and the point code or alias point code of the destination network type is not defined.	
CnvCgdn	This parameter enables discarding of the CGPA point code in SCCP messages if the destination network type is Itun, and the point code or alias point code of the destination network type is not defined.	

Table 5-38 (Cont.) M3rl Options Elements

Element	Description	Data Input Notes
CnvCgdn24	This parameter enables discarding of the CGPA point code in SCCP messages if the destination network type is Itun24, and the point code or alias point code of the destination network type is not defined.	
CnvClgItu	This parameter enables or disables the CGPA conversion for Itui/Itui_s/Itun/Itun_s domain crossing during SCCP conversion.	
GtCnvDflt	This parameter enables routing of SCCP messages using system defaults when an appropriate entry is not found in the Default GT Conversion Table.	
Incoming SLS Bit Rotation	This parameter indicates whether an Incomig SLS Bit Rotation is enabled or not.If it is turned on and Incoming SLS Bit Rotation is applied to an MSU then the outgoing SLS bit rotation is not applied for that MSU.	
Linkset On Hold timer	Link addition/deletion changeover timer duration. This timer introduces a delay to help prevent message mis-sequencing on link add/deletion.	Typical value is 60. Range = 10,2000
Randsls	Random SLS (signaling link selection).This parameter is used to apply random SLS generation on a per linkset basis.	
Signaling Link Supervision Timer	Supervision timer for signaling link test acknowledgement message.	Typical value is 12000.Range = 4000,12000
Signaling Link Interval Timer	Interval timer for sending signaling link test messages. Typical value is 30000.Range = 30000,90000	
SlsRotation	This parameter specifies whether the signaling link selector (SLS) of the incoming ANSI linkset is rotated before routing the messages to network. When set to true, 8 bit SLS of the incoming linkset is considered for bit rotation.	

Table 5-38 (Cont.) M3rl Options Elements

Element	Description	Data Input Notes
Slscnv	This parameter is used as Per node SLS conversion indicator.	
SlsReplace	This parameter allows to replace the SLS for an ANSI message with a random generated SLS value by Random SLS feature	
SlsocbEnabled	This parameter turns on the Other CIC (Circuit Identification Code) Bit Used feature	
Timer 10	Timer 10 - Wait to repeat signaling route set test (SRST) message.	Typical value is 30000 Range = 20000,90000
Timer 11	Timer 11 - Transfer restricted; in milliseconds.	Typical value is 30000 Range = 1000,90000
Timer 15	Timer 15 - Wait for repeat route set congestion test (RSCT).	Typical value is 3000 Range = 200,4000
Timer 16	Timer 16 - Wait for route set congestion test (RSCT) updates.	Typical value is 1400 Range = 200,3000
Timer 18	Timer 18 - Repeat transfer restricted (TFR) once by response method.	Typical value is 10000 Range = 2000,20000
Timer 1	Timer 1 - Changeover delay. Also used as isolation timer for ITU MTP Restart.	Typical value is 800 Range = 100,2000
Timer 2	Timer 2 - Wait for changeover acknowledgement (COA).	Typical value is 1400 Range = 100,3000
Timer 3	Timer 3 - Time controlled diversion on changeback.	Typical value is 800 Range = 100,2000
Timer 4	Timer 4 - Wait for changeback acknowledgement (CBA) #1.	Typical value is 800 Range = 100,2000
Timer 5	Timer 5 - Wait for changeback acknowledgement (CBA) #2.	Typical value is 800 Range = 100,2000
Timer 6	Timer 6 - Controlled reroute.	Typical value is 800 Range = 100,2000
Timer 8	Timer 8 - Transfer prohibited (TFP) inhibit.	Typical value is 800 Range = 500,2000
SparePCSupportEnabled	Checks whether the support for ITUN-Spare and ITUI-Spare is enabled or disabled	

You can perform edit task on **VSTP**>**Configuration**>**M3rl Options** page.

Editing a M3rl Option

Use this procedure to change the field values for a selected M3rl Option. :

1. On the **VSTP**>**Configuration**>**M3rl Options** page, enter the updated values in the input fields.
2. Click **OK**, **Apply**, or **Cancel**

5.1.39 MTP3 Config

A Mtp3 Config is an entity to configure all the m3rl timers.

Select the **VSTP**, and then **Configuration**, and then **MTP3 Configs** page. The page displays the elements on the **MTP3 Configs** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-39 MTP3 Configs Elements

Element	Description	Data Input Notes
Name *	Name for this M3rl Config, which must be unique within the VSTP site.	Valid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. [A value is required.]
Linkset On Hold timer	Link addition/deletion changeover timer duration. This timer introduces a delay to help prevent message mis-sequencing on link add/ deletion.	Typical value is 60. [MIN,MAX] = [10,2000]
Signaling Link Test T1 Timer	Supervision timer for signaling link test acknowledgement message.	Typical value is 12000. [MIN,MAX] = [4000,12000]
Signaling Link Test T2 Timer	Interval timer for sending signaling link test messages.	Typical value is 30000. [MIN,MAX] = [30000,90000]
Signaling Link Test T17 Timer	SLT T17 timer set.	Typical value is 2000. [MIN,MAX] = [500,2000]
Timer 10	Timer 10 - Wait to repeat signaling route set test (SRST) message.	Typical value is 30000. [MIN,MAX] = [20000,90000]
Timer 11	Timer 11 - Transfer restricted; in milliseconds.	Typical value is 30000. [MIN,MAX] = [1000,90000]
Timer 12	Timer 12 - Linkset inhibited; in milliseconds.	Typical value is 800. [MIN,MAX] = [800,1500]

Table 5-39 (Cont.) MTP3 Configs Elements

Element	Description	Data Input Notes
Timer 13	Timer 13 - Linkset inhibited; in milliseconds.	Typical value is 800. [MIN,MAX] = [800,1500]
Timer 15	Timer 15 - Wait for repeat route set congestion test (RSCT).	Typical value is 3000. [MIN,MAX] = [200,4000]
Timer 16	Timer 16 - Wait for route set congestion test (RSCT) updates.	Typical value is 1400. [MIN,MAX] = [200,3000]
Timer 17	Timer 17 - Delay to avoid oscillation of initial alignment failure.	Typical value is 2000. [MIN,MAX] = [500,2000]
Timer 18	Timer 18 - Repeat transfer restricted (TFR) once by response method.	Typical value is 10000. [MIN,MAX] = [2000,20000]
Timer 1	Timer 1 - Changeover delay. Also used as isolation timer for ITU MTP Restart.	Typical value is 800. [MIN,MAX] = [100,2000]
Timer 2	Timer 2 - Wait for changeover acknowledgement (COA).	Typical value is 1400. [MIN,MAX] = [100,3000]
Timer 23	Timer 23 - Linkset inhibited; in milliseconds.	Typical value is 180000. [MIN,MAX] = [180000,360000]
Timer 3	Timer 3 - Time controlled diversion on changeback.	Typical value is 800. [MIN,MAX] = [100,2000]
Timer 4	Timer 4 - Wait for changeback acknowledgement (CBA) #1.	Typical value is 800. [MIN,MAX] = [100,2000]
Timer 5	Timer 5 - Wait for changeback acknowledgement (CBA) #2.	Typical value is 800. [MIN,MAX] = [100,2000]
Timer 6	Timer 6 - Controlled reroute.	Typical value is 800. [MIN,MAX] = [100,2000]
Timer 8	Timer 8 - Transfer prohibited (TFP) inhibit.	Typical value is 800. [MIN,MAX] = [500,2000]

You can perform add, edit, or delete tasks on **VSTPConfigurationMTP3 Configs** page.

Adding a MTP3 Config

Perform the following steps to configure a new MTP3 Config:

1. Click **Insert**.

> **Note:**
>
> The new MTP3 Config must have a name that is unique across all MTP3 Configs at the SOAM. In addition, the MTP3 Config's IP Port combination must also be unique across all MTP3 Configs configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a MTP3 Config

Use this procedure to change the field values for a selected MTP3 Config. (The **MTP3 Config Name** field cannot be changed.):

1. Select the **MTP3 Config** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a MTP3 Config

Use the following procedure to delete a MTP3 Config.

> **Note:**
>
> You cannot delete a MTP3 Config if it is part of the configuration of one or more Linksets.

1. Select the **MTP3 Config** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.40 MTP2 Config

A Mtp2 Config is an entity to configure all the mtp2 timers.

Select the **VSTP**, and then **Configuration**, and then **MTP2 Config** page. The page displays the elements on the **MTP2 Config** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-40 MTP2 Config Elements

Element	Description	Data Input Notes
Name	ame for this Mtp2 Config, which must be unique within the VSTP site. This is a mandatory field.	NValid names are strings between one and 32 characters, inclusive. Valid characters are alphanumeric and underscore. The name must contain at least one alpha and must not start with a digit. [A value is required.]

Table 5-40 (Cont.) MTP2 Config Elements

Element	Description	Data Input Notes
T1 Timer	Alignment Ready timer. The amount of time (in milliseconds) MTP2 waits to receive a Link Status Ready message from the peer.	Typical value is 9000. Minimum: 5000, Maximum: 350000
T2 Timer	Not Aligned timer.	Typical value is 9000 Minimum: 5000, Maximum: 48000
T3 Timer	Alignment timer. The amount of time (in milliseconds) MTP2 waits to receive Link Status Proving message from the peer.	Typical value is 9000. Minimum: 1000, Maximum: 20000
T4 Emergency Timer	Emergency proving timer. The amount of time (in milliseconds) MTP2 sends Link Status Proving messages during emergency proving.	Typical value is 600. Minimum: 200, Maximum: 10000
T4 Normal Timer	Normal proving timer. The amount of time (in milliseconds) MTP2 sends Link Status Proving messages during normal proving.	Typical value is 2300. Minimum: 500, Maximum: 70000
T5 Timer	Sending SIB timer.	Typical value is 90. Minimum: 40, maximum: 500
T6 Timer	Remote congestion timer. The amount of time (in milliseconds) that a congested link will remain in service.	Typical value is 4000. Minimum: 1000, Maximum: 10000
T7 Timer	Excessive acknowledgement delay timer. The amount of time (in milliseconds) for which M2PA waits between transmission of a user data message and receipt of an acknowledgement for that message from the peer. If this timer expires, the link is taken out of service.	Typical value is 300. Minimum: 200, maximum: 3000

You can perform add, edit, or delete tasks on **VSTPConfigurationMTP2 Config** page.

Adding a MTP2 Config

Perform the following steps to configure a new MTP2 Config:

1. Click **Insert**.

> **Note:**
>
> The new MTP2 Config must have a name that is unique across all MTP2 Config at the SOAM. In addition, the MTP2 Config's IP Port combination must also be unique across all MTP2 Config configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a MTP2 Config

Use this procedure to change the field values for a selected MTP2 Config. (The **MTP2 Config Name** field cannot be changed.):

1. Select the **MTP2 Config** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a MTP2 Config

Use the following procedure to delete a MTP2 Config.

> **Note:**
>
> You cannot delete a MTP2 Config if it is part of the configuration of one or more Linksets.

1. Select the **MTP2 Config** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.41 MTP2 Board

A Mtp2Board is used to store the Board Data Information. All these configurations go into VstpMtp2BoardMergeData table.

Select the **VSTP**, and then **Configuration**, and then **MTP2 Board** page. The page displays the elements on the **MTP2 Board** page.

> **Note:**
>
> This is a read-only page.

Table 5-41 MTP2 Board Elements

Element	Description
Source Node	Name of the originating node.
Board Type	Defines the type of Board.
MRL	MRL Value of the Board.
Serial Number	Serial Number of the Board.
PORM Version	PORM version of the Board.
MACH Version	MACH version of the Board.
Number of E1/T1 Ports	Number of E1/T1 ports.
Number of Ethernet Ports	Number of Ethernet ports.

5.1.42 VLR Profile

A VLR Profile is an entity which helps in getting information about a mobile subscriber in order to locate the user while in roaming.

Select the **VSTP**, and then **Configuration**, and then **VLR Profile** page. The page displays the elements on the **VLR Profile** page.

> **Note:**
>
> This is a read-only page.

Table 5-42 VLR Profile Elements

Element	Description
Vlr	VLR Number.
Filter	The filter determines the category in which the number falls into. It can any of the following: • Whitelist • Blacklist • Greylist
Last Used Time	The date/time the status for this Link was last updated by the vSTP.
Success Count	Number for the vSTP VLR Profile, which must be unique within the vSTP site. Valid vlr number are hexadecimal number between one and 16 characters, inclusiv maxLength, pattern, and type.
Filure Count	VLR failure count

5.1.43 VLR Roaming

A VLR Roaming is an entity which is used for roaming for mobile subscribers.

Select the **VSTP**, and then **Configuration**, and then **VLR Roaming** page. The page displays the elements on the **VLR Roaming** page.

> **Note:**
>
> This is a read-only page.

Table 5-43 VLR Roaming Elements

Element	Description
New VLR	VLR Number to which mobile subscriber has moved.
Old VLR	VLR Number from which mobile subscriber has moved.
Entry Usage Count	Entry usage time.
Last Used Time	The date/time the status for this Link was last updated by the vSTP.
Time	This determines the time duration for which roaming must occur.
Unique Identifier	Defines a unique identifier for VLR Roaming. The unique identifier value is a combination of old and new VLR names.

5.1.44 Whitelist VLR Profiles

A VLR Profile is an entity which helps in getting information about a mobile subscriber in order to locate the user while in roaming.

Select the **VSTP**, and then **Configuration**, and then **Whitelist VLR Profiles** page. The page displays the elements on the **Whitelist VLR Profiles** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-44 Whitelist VLR Profiles Elements

Element	Description	Data Input Notes
VLR	Number for the VSTP VLR Profile, which must be unique within the VSTP site.	Valid vlr number are hexadecimal number between one and 16 characters, inclusive. [A value is required.]
Filter	The filter determines the category in which the number falls into.	

You can perform add, edit, or delete tasks on **VSTPConfigurationWhitelist VLR Profiles** page.

Adding a Whitelist VLR Profile

Perform the following steps to configure a new Whitelist VLR Profile:

1. Click **Insert**.

> **Note:**
>
> The new Whitelist VLR Profile must have a name that is unique across all Whitelist VLR Profiles at the SOAM. In addition, the Whitelist VLR Profile's IP Port combination must also be unique across all Whitelist VLR Profiles configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Whitelist VLR Profile

Use this procedure to change the field values for a selected Whitelist VLR Profile. (The **Whitelist VLR Profile Name** field cannot be changed.):

1. Select the **Whitelist VLR Profile** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Whitelist VLR Profile

Use the following procedure to delete a Whitelist VLR Profile.

> **Note:**
>
> You cannot delete a Whitelist VLR Profile if it is part of the configuration of one or more Linksets.

1. Select the **Whitelist VLR Profile** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.45 Mate STP

A Mate Stp is an entity which holds point code entries which is used to route reponses to queries generated by the VSTP for SFAPP.

Select the **VSTP**, and then **Configuration**, and then **Mate STP** page. The page displays the elements on the **Mate STP** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-45 Mate STP Elements

Element	Description	Data Input Notes
Domain	This defines the type of domain.	Range = Ansi, Itui, Itun, Itun24, Itun16, Itui_s, Itun_s
Point Code	The point code identifies the Mate Stp. Only one Mate Stp can have this point code .	Range = Numeric values seperated by hyphen(-); Maximum Length=12;

You can perform add, edit, or delete tasks on **VSTPConfigurationMate STP** page.

Adding a Mate STP

Perform the following steps to configure a new Mate STP:

1. Click **Insert**.

> **Note:**
>
> The new Mate STP must have a name that is unique across all Mate STP at the SOAM. In addition, the Mate STP's IP Port combination must also be unique across all Mate STP configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Mate STP

Use this procedure to change the field values for a selected Mate STP. (The **Mate STP Name** field cannot be changed.):

1. Select the **Mate STP** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Mate STP

Use the following procedure to delete a Mate STP.

> **Note:**
>
> You cannot delete a Mate STP if it is part of the configuration of one or more Linksets.

1. Select the **Mate STP** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.46 SFAPP Options

The Sfapp Options are those configuration values that govern the overall Sfapp functionality. There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The SFAPP Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **SFAPP Options** page. The page displays the elements on the **SFAPP Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-46 SFAPP Options Elements

Element	Description	Data Input Notes
Aging Timer	This parameter defines value for aging.	[Default=n/a; Range= None, 1-65535]
Failure Threshold	This parameter defines the failed validation threshold.	[Default=n/a; Range= None, 1-65535]
Learn Timer	New learning possible in this mode. No validation performed.	[Default=8; Range= None, 4-12]
Sfapp Mode	Provides the option to turn off dynamic learning,test the learning algorithm, and move the system in operation using various modes.	[Default='Off'; Range= 'Off', 'Learn', 'Test', 'Active']
Success Threshold	This parameter defines the successful validation threshold.	[Range= None, 1-65535]
Velocity Threshold	This parameter defines the number of velocity check attempts.	[Range= None, 1-65535]
Maximum Profile Limit	Maximum Profile Limit.	[Default='No', Range= 'No', 'Yes']
Maximum Roaming Limit	Maximum Roaming Limit.	[Default='No', Range= 'No', 'Yes']

You can perform edit task on **VSTP**>**Configuration**>**SFAPP Options** page.

Editing a SFAPP Option

Use this procedure to change the field values for a selected SFAPP Option. (The **SFAPP Option Name** field cannot be changed.):

1. Select the **SFAPP Option** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.47 CAT2 IMSI

A CAT2 IMSI is an entity which are used to perform Category 2 securiry check for IMSI based. It will be used for IR21 upload feature.

Select the **VSTP**, and then **Configuration**, and then **CAT2 IMSIs** page. The page displays the elements on the **CAT2 IMSIs** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-47 CAT2 IMSIs Elements

Element	Description	Data Input Notes
mccmnc	E212 mobile country code/ mobile network code.	
TA Digit Code	Name of TA Digit code.	Valid names are strings between one and 5 characters, inclusive. Valid characters are alphanumeric. The name must contain at least one alpha and must not start with a digit.
Sender TA Digit Code	Name of Sender TA Digit code.	Valid names are strings between one and 5 characters, inclusive. Valid characters are alphanumeric. The name must contain at least one alpha and must not start with a digit.
Gta Length	Represent the length of a gta for a particular STADIG Code.	Range: 1,15

You can perform add, edit, or delete tasks on **VSTPConfigurationCAT2 IMSIs** page.

Adding a CAT2 IMSI

Perform the following steps to configure a new CAT2 IMSI:

1. Click **Insert**.

> **Note:**
>
> The new CAT2 IMSI must have a name that is unique across all CAT2 IMSIs at the SOAM. In addition, the CAT2 IMSI's IP Port combination must also be unique across all CAT2 IMSIs configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a CAT2 IMSI

Use this procedure to change the field values for a selected CAT2 IMSI. (The **CAT2 IMSI Name** field cannot be changed.):

1. Select the **CAT2 IMSI** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a CAT2 IMSI

Use the following procedure to delete a CAT2 IMSI.

> **Note:**
>
> You cannot delete a CAT2 IMSI if it is part of the configuration of one or more Linksets.

1. Select the **CAT2 IMSI** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.48 CAT2 GTA

A CAT2 GTA is an entity which are used to perform Category 2 securiry check for GTA based. It will be used for IR21 upload feature.

Select the **VSTP**, and then **Configuration**, and then **CAT2 GTAs** page. The page displays the elements on the **CAT2 GTAs** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-48 CAT2 GTAs Elements

Element	Description	Data Input Notes
TA Digit code	Name of TA Digit code.	Valid names are strings between one and 5 characters, inclusive. Valid characters are alphanumeric. The name must contain at least one alpha and must not start with a digit.
Sender TA Digit code	Name of Sender TA Digit code.	Valid names are strings between one and 5 characters, inclusive. Valid characters are alphanumeric. The name must contain at least one alpha and must not start with a digit.
Start Global Title Address	Defines the start of a range of this Global Title Address.	
End Global Title Address	End global title address. This parameter specifies the end of a range of global title digits.	
Node Type	Type Of Node	Valid values are: HLR, MGT

You can perform add, edit, or delete tasks on **VSTPConfigurationCAT2 GTAs** page.

Adding a CAT2 GTA

Perform the following steps to configure a new CAT2 GTA:

1. Click **Insert**.

> **Note:**
>
> The new CAT2 GTA must have a name that is unique across all CAT2 GTAs at the SOAM. In addition, the CAT2 GTA's IP Port combination must also be unique across all CAT2 GTAs configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a CAT2 GTA

Use this procedure to change the field values for a selected CAT2 GTA. (The **CAT2 GTA Name** field cannot be changed.):

1. Select the **CAT2 GTA** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a CAT2 GTA

Use the following procedure to delete a CAT2 GTA.

> **Note:**
>
> You cannot delete a CAT2 GTA if it is part of the configuration of one or more Linksets.

1. Select the **CAT2 GTA** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.49 MP Leader

An MP leader is an MP designated as a leader in an MP server group. The MP leader is used internally by software for status reporting.

The page displays name of the vSTP MP Leader.

5.1.50 Default Conversions

A Default Conversion entry consists of parameters such as dir, gtixlat, tta, tti, nai, np and other conversion-specific data.

Select the **VSTP**, and then **Configuration**, and then **Default Conversions** page. The page displays the elements on the **Default Conversions** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-49 Default Conversions Elements

Element	Description	Data Input Notes
Default Conversion Name	Name of default conversion.	Upto 20 characters allowed.
Direction of Conversion	Direction of Conversion	
Global Title Indicator Conversion	Global Title Indicator conversion.	
ANSI Translation Type	ANSI Translation Type. Upto 3 characters allowed.	
ITU Translation Type	ITU Translation Type. Upto 3 characters allowed.	

Table 5-49 (Cont.) Default Conversions Elements

Element	Description	Data Input Notes
Nature of Address Indicator	Nature of Address Indicator. This parameter is mandatory when gtixlat=24 is specified, and not specified when gtixlat=22 is specified.	Upto 2 characters allowed.
Numbering Plan	Numbering Plan. This parameter is mandatory when gtixlat=24 is specified, and not specified when gtixlat=22 is specified.	Upto 2 characters allowed.
Number of Prefix Digits to be Deleted	Number of prefix digits to be deleted. The number of digits to be deleted.	These digits will be replaced with the new prefix digits string (npds). Min, Max: 0,21]
New prefix digits string	New prefix digits string. The new prefix digits string that will replace the received prefix digits string.	Upto 21 characters allowed.
Number of Suffix Digits to be Deleted	Number of suffix digits to be deleted. This parameter identifies the new suffix digits to be deleted that will replace the received suffix digits to be deleted.	Min, Max: 0,21]
New suffix Digits String	New suffix digits string. The new suffix digits string that will replace the received suffix digits string.	Upto 21 characters allowed

You can perform add, edit, or delete tasks on **VSTPConfigurationDefault Conversions** page.

Adding a Default Conversion

Perform the following steps to configure a new Default Conversion:

1. Click **Insert**.

> **Note:**
>
> The new Default Conversion must have a name that is unique across all Default Conversions at the SOAM. In addition, the Default Conversion's IP Port combination must also be unique across all Default Conversions configured at the SOAM.

2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Default Conversion

Use this procedure to change the field values for a selected Default Conversion. (The **Default Conversion Name** field cannot be changed.):

1. Select the **Default Conversion** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Default Conversion

Use the following procedure to delete a Default Conversion.

> **Note:**
>
> You cannot delete a Default Conversion if it is part of the configuration of one or more Linksets.

1. Select the **Default Conversion** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.51 Feature Admin State

Feature Admin States provides the administrative state of the VSTP Features. The VSTP Features are initially in the disabled administrative state when the system is installed.

The Feature Admin State can be enabled or disabled from this page.

Select the **VSTP**, and then **Configuration**, and then **Feature Admin State** page. The page displays the features.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-50 Feature Admin State Elements

Element	Description	Data Input Notes
Feature Name	The name of the VSTP Feature.	
Feature Status	A vSTP Feature's administrative state can either be Enabled or Disabled.	A VSTP Feature is initially in the Disabled administrative state when the system is installed and it cannot be Disabled once Enabled.

You can perform edit task on **VSTP**>**Configuration**>**Feature Admin State** page.

Editing a Feature Admin State

Use this procedure to change the field values for a selected Feature Admin State. (The **Feature Admin State Name** field cannot be changed.):

1. Select the Feature to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.1.52 VSTP Capacity

VSTP Capacity provides information about maximum allowed, currently configured, and utilisation percentage of Diameter resources. This information is available system-wide.

Select the **VSTP**, and then **Configuration**, and then **VSTP Capacity** page. The page displays the elements on the **VSTP Capacity** page.

> **Note:**
>
> This is a read-only page.

Table 5-51 VSTP Capacity Elements

Element	Description
Resource Name	Resource name
Scope	
Scope Name	
Used Capacity	Number of entries that are already configured for the resourceName.
Free Capacity	Free space.
Maximum Capacity	Maximum number of entries for the resourceName that can be configured in Diameter.

5.1.53 Alarm Aggregator Options

The VSTP Alarm Aggregation Options are those configuration values that manages aggregation of vstp alarms . There is a single instance of this resource, which contains each of the individual options that can be retrieved and set. .

The Alarm Aggregator Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **Alarm Aggregator Options** page. The page displays the elements on the **Alarm Aggregator Options** View, Insert, and Edit pages.

> **Note:**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-52 Alarm Aggregator Options Elements

Element	Description	Data Input Notes
Association Major Agg Alarm Threshold	When the number of Connection (/vstp/connections) failure alarms raised by a single VSTP-MP exceeds this threshold: 1) all individual Connection failure alarms raised to that point are cleared, and 2) a single aggregate Connection failure alarm of major severity is raised by the SOAM against that VSTP-MP. The value of associationMajorAggAlarmThreshold is included in the available alarm budget, multiplied by the number of VSTP-MP in the DSR. So the sum of (associationMajorAggAlarmThreshold * # VSTP-MPs), (linkMajorAggAlarmThreshold * # VSTP-MPs), linksetCriticalAggAlarmThreshold, routeCriticalAggAlarmThreshold, and rspCriticalAggAlarmThreshold cannot exceed alarmBudget.	Default - 100. [Min,Max] = [1,3000]
Association Critical Agg Alarm Threshold	hen the number of Connection (/vstp/connections) failure alarms raised by a single VSTP-MP exceeds this threshold: 1) the already-raised major aggregate Connection failure alarm for that VSTP-MP is cleared, and 2) a single aggregate Connection failure alarm of critical severity is raised by the SOAM against that VSTP-MP. The value of associationCriticalAggAlarmThreshold is not included in the available alarm budget. Set associationCriticalAggAlarmThreshold to zero to prevent entirely the raising of a critical aggregate alarm for Connection failures.	W Default - 200. [Min,Max] = [0,3000]

Table 5-52 (Cont.) Alarm Aggregator Options Elements

Element	Description	Data Input Notes
Link Major Agg Alarm Threshold	When the number of Link (/vstp/links) failure alarms raised by a single VSTP-MP exceeds this threshold: 1) all individual Link failure alarms raised to that point are cleared, and 2) a single aggregate Link failure alarm of major severity is raised by the SOAM against that VSTP-MP. The value of linkMajorAggAlarmThreshold is included in the available alarm budget, multiplied by the number of VSTP-MP in the DSR. So the sum of (associationMajorAggAlarmThreshold * # VSTP-MPs), (linkMajorAggAlarmThreshold * # VSTP-MPs), linksetCriticalAggAlarmThreshold, routeCriticalAggAlarmThreshold, and rspCriticalAggAlarmThreshold cannot exceed alarmBudget.	Default - 100. [Min,Max] = [1,3000] [A value is required.]
Link Critical Agg Alarm Threshold	When the number of Link (/vstp/links) failure alarms raised by a single VSTP-MP exceeds this threshold: 1) the already-raised major aggregate Link failure alarm for that VSTP-MP is cleared, and 2) a single aggregate Link failure alarm of critical severity is raised by the SOAM against that VSTP-MP. The value of linkCriticalAggAlarmThreshold is not included in the available alarm budget. Set linkCriticalAggAlarmThreshold to zero to prevent entirely the raising of a critical aggregate alarm for Link failures.	Default - 200. [Min,Max] = [0,3000] [A value is required.]

Table 5-52 (Cont.) Alarm Aggregator Options Elements

Element	Description	Data Input Notes
Linkset Critical Agg Alarm Threshold	When the number of Linkset (/vstp/linksets) failure alarms raised by the VSTP exceeds this threshold: 1) all individual Linkset failure alarms raised to that point are cleared, and 2) a single aggregate Linkset failure alarm of critical severity is raised by the SOAM. So the sum of (associationMajorAggAlarmThreshold * # VSTP-MPs), (linkMajorAggAlarmThreshold * # VSTP-MPs), linksetCriticalAggAlarmThreshold, routeCriticalAggAlarmThreshold, and rspCriticalAggAlarmThreshold cannot exceed alarmBudget.	Default - 300.[MIN,MAX] = [Min,Max] = [1,3000] [A value is required.]
Route Critical Agg Alarm Threshold *	When the number of Route (/vstp/routes) failure alarms raised by the VSTP exceeds this threshold: 1) all individual Route failure alarms raised to that point are cleared, and 2) a single aggregate Route failure alarm of critical severity is raised by the SOAM. So the sum of (associationMajorAggAlarmThreshold * # VSTP-MPs), (linkMajorAggAlarmThreshold * # VSTP-MPs), linksetCriticalAggAlarmThreshold, routeCriticalAggAlarmThreshold, and rspCriticalAggAlarmThreshold cannot exceed alarmBudget.	Default - 600. [Min,Max] = [1,3000] [A value is required.]

Table 5-52 (Cont.) Alarm Aggregator Options Elements

Element	Description	Data Input Notes
Rsp Critical Agg Alarm Threshold *	When the number of Remote Signaling Point (/vstp/remotesignalingpoints) failure alarms raised by the VSTP exceeds this threshold: 1) all individual Remote Signaling Point failure alarms raised to that point are cleared, and 2) a single aggregate Remote Signaling Point failure alarm of critical severity is raised by the SOAM. So the sum of (associationMajorAggAlarmThreshold * # VSTP-MPs), (linkMajorAggAlarmThreshold * # VSTP-MPs), linksetCriticalAggAlarmThreshold, routeCriticalAggAlarmThreshold, and rspCriticalAggAlarmThreshold cannot exceed alarmBudget.	Default - 600. [Min,Max] = [1,3000] [A value is required.]

You can perform edit task on **VSTP**>**Configuration**>**Alarm Aggregator Options** page.

Editing a Alarm Aggregator Options

Use this procedure to change the field values for a selected Alarm Aggregator Options. (The **Alarm Aggregator Options Name** field cannot be changed.):

1. Select the **Alarm Aggregator Options** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

5.2 Maintenance

The **VSTP** > **Maintenance** pages display status information for Links, RSPs, Connections, Linksets, and SCCP applications.

The **VSTP** > **Maintenance** pages allow you to view the following information and perform the following actions:

5.2.1 vSTP Maintenance Link Status

The **VSTP** > **Maintenance** > **Link Status** page allows you to view information about existing links, including the operational status of each link.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of links to display only the desired Connections.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Link Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable Links
- Disable Links

vSTP Maintenance Link Status Elements

The following describes fields on the Link Status maintenance page:

Field	Description
Link Name	Name of the link.
mp Server Host Name	Hostname of the MP server from which status is reported.
Admin State	A Link's administrative state can be: • Enabled: the Link is Enabled • Disabled: the Link is Disabled • Unk: unknown; the state of the Link is not available in the database
Operational Status	A Link's administrative state can be: • Available: the Link is available for routing • Degraded: the Link is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Link is unavailable. The Operational Reason field provides additional information on this status.
Operational Reason	Reason for the Operational Status.
Link Type	Link type.
Linkset Name	Name of the associated linkset.
Time of Last Update	Time stamp that shows the last time the status information was updated.
Status Known	The status can be: • True: The Link status is available. • False: The Link status is not available. The value depends on the Operational Status, mp Server Host Name, Time of Last Update, or Operational Reason.

Enabling Links

Use the following steps to enable one or more links:

1. Click **VSTP** > **Maintenance** > **Link Status**.
2. Select 1 - 20 links to enable.
   To select multiple links, press CTRL when selecting each connection. To select multiple contiguous links, click the first connection you want, then press SHIFT and select the last link you want. All the links in between are also selected.
3. Click **Enable**.

4. Click **OK** on the confirmation screen to enable the selected links. If any of the selected links no longer exist (they have been deleted by another user), an error message displays, but any selected links that do exist are enabled.

Disabling Links

Use the following steps to disable one or more links:

1. Click **VSTP** > **Maintenance** > **Link Status**.
2. Select 1 - 20 links to disable.
   To select multiple links, press CTRL when selecting each connection. To select multiple contiguous links, click the first connection you want, then press SHIFT and select the last link you want. All the links in between are also selected.
3. Click **Disable**.
4. Click **OK** on the confirmation screen to disable the selected links. If any of the selected links no longer exist (they have been deleted by another user), an error message displays, but any selected links that do exist are disabled.

5.2.2 vSTP Maintenance Connection Status

The **VSTP** > **Maintenance** > **Connection Status** page allows you to view information about existing Connections, including the operational status of each Connection.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of Connections to display only the desired Connections.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Connection Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable Connections
- Disable Connections

vSTP Maintenance Connection Status Elements

The following describes fields on the Connection Status maintenance page:

Field	Description
Connection Name	Name of the Connection.
mp Server Host Name	Hostname of the MP server from which status is reported.
Admin State	A Connection's administrative state can be: • Enabled: the Connection is Enabled • Disabled: the Connection is Disabled • Unk: unknown; the state of the Connection is not available in the database

Field	Description
Operational Status	A Connection's administrative state can be: • Available: the Connection is available for routing • Degraded: the Connection is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Connection is unavailable. The Operational Reason field provides additional information on this status.
Operational Reason	Reason for the Operational Status.
Local Host Name	Name of the local host.
Remote Host Name	Name of the remote host.
Time of Last Update	Time stamp that shows the last time the status information was updated.
Status Known	The status can be: • True: The Connection status is available. • False: The Connection status is not available. The value depends on the Operational Status, mp Server Host Name, Time of Last Update, or Operational Reason.

Enabling Connections

Use the following steps to enable one or more Connections:

1. Click **VSTP** > **Maintenance** > **Connection Status**.
2. Select 1 - 20 Connections to enable.
   To select multiple Connections, press CTRL when selecting each connection. To select multiple contiguous Connections, click the first connection you want, then press SHIFT and select the last Connection you want. All the Connections in between are also selected.
3. Click **Enable**.
4. Click **OK** on the confirmation screen to enable the selected Connections. If any of the selected Connections no longer exist (they have been deleted by another user), an error message displays, but any selected Connections that do exist are enabled.

Disabling Connections

Use the following steps to disable one or more Connections:

1. Click **VSTP** > **Maintenance** > **Connection Status**.
2. Select 1 - 20 Connections to disable.
   To select multiple Connections, press CTRL when selecting each connection. To select multiple contiguous Connections, click the first connection you want, then press SHIFT and select the last Connection you want. All the Connections in between are also selected.
3. Click **Disable**.

4. Click **OK** on the confirmation screen to disable the selected Connections. If any of the selected Connections no longer exist (they have been deleted by another user), an error message displays, but any selected Connections that do exist are disabled.

5.2.3 vSTP Maintenance Remote Signaling Point Status

The **VSTP** > **Maintenance** > **Remote Signaling Point Status** page allows you to view information about existing RSPs, including the operational status of each RSP.

You can perform these tasks on an Active System OAM (SOAM):

- Filter the list of RSPs to display only the desired RSPs.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by RSP Name in ascending ASCII order.
- Click the + in any entry in the **Routes** field to view information about the routes associated with the RSP.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.

vSTP Maintenance RSP Status Elements

The following describes fields on the RSP Status maintenance page:

Field	Description
MP server	Name of the vSTP MP server that is currently reporting the status of the RSP.
RSP Name	Name of the RSP.
mp Server Host Name	Hostname of the MP server from which status is reported.
Operational Status	A RSP's administrative state can be: • Available: the RSP is available for routing • Degraded: the RSP is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the RSP is unavailable. The Operational Reason field provides additional information on this status.
Point Code	Unique address of the RSP.
Routes	RSP route. An RSP can have two routes.
Route Adjacent Status	The status of adjacent part. It can have these four status: • Down: The adjacent part to RSP is down. • UP: The adjacent part to RSP is up. • Restricted: The adjacent part to RSP is restricted.. • Unassigned: The adjacent part to RSP is not assigned to any other RSP.
Route Name	Name of the route.

Field	Description
Route Remote Status	The status of the non adjacent part. The route remote status can be: • Available: The non-adjacent part to RSP is available. • Unavailable: The non-adjacent part to RSP is unavailable. • Restricted: The non-adjacent part to RSP is restricted. • Unassigned: The non-adjacent part to RSP is not assigned to any other RSP.
SS7 Domain Type	Types of SS7 Domain. The values can be: • ANSI • ITUI • ITUN • ITUN24 • ITUI_S • ITUN_S
Status Known	Status can have the following values: • True: The RSP status is known. • False: The RSP status is unknown.
Last Updated	The congestion level of the Link Set. This is the lowest of the congestion levels of all the Links configured in the Link Set. The congestion level options are: • Normal • CL1 • CL2 • CL3

5.2.4 vSTP Maintenance Link Set Status

The **VSTP** > **Maintenance** > **Link Set Status** page allows you to view information about existing Linksets, including the operational status of each Linkset.

You can perform these tasks on an Active System OAM (SOAM):

- Filter the list of Linksets to display only the desired Linksets.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Linkset Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.

vSTP Maintenance Linkset Status Elements

The following describes fields on the Linkset status maintenance page:

Field	Description
Congestion Level	The congestion level of the Link Set. This is the lowest of the congestion levels of all the Links configured in the Link Set. The congestion level options can be : • Normal • CL1 • CL2 • CL3
MP server	Name of the vSTP MP server that is currently reporting the status of the Link Set.
Link Set Name	Name of the Linkset.
mp Server Host Name	Hostname of the MP server from which status is reported.
Operational Reason	Reason for the operational status.
Operational Status	A Linkset's administrative state can be: • Available: the Linkset is available for routing • Degraded: the Linkset is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Linkset is unavailable. The Operational Reason field provides additional information on this status.
Status Known	Status can be: • True: The Linkset status is known. • False: The Linkset status is unknown. The value depends on Operational Status, Congestion Level, Last Updated, Operational Reason values.
Last Updated	Time stamp which indicates the last time status information was updated.

5.2.5 vSTP Maintenance SCCP Application Status

The **VSTP** > **Maintenance** > **SCCP Application Status** page allows you to view information about existing SCCP Applications, including the operational status of each SCCP Application.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of SCCP Applications to display only the desired applications.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by SCCP Application Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable SCCP Applications.
- Disable SCCP Applications.

vSTP Maintenance SCCP Application Status Elements

The following describes fields on the SCCP Application Status maintenance page:

Field	Description
Admin State	A SCCP Application's administrative state can be: • Enabled: the SCCP Application is Enabled • Disabled: the SCCP Application is Disabled • Unk: unknown; the state of the SCCP Application is not available in the database
App Id	The unique ID of the application.
Operational State	A SCCP Application's administrative state can be: • Available: the SCCP Application is available for routing • Degraded: the SCCP Application is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the SCCP Application is unavailable. The Operational Reason field provides additional information on this status.
App Type	Type of Application. Options are: • EIR • ATINP • INPQ • SFAPP
Host Name	The name of vSTP MP server that is currently reporting the status of this application.
SSN	Sub System Number
Status Known	Status values can be: • True: The application status is known. • False: The application status is unknown. The value depends on Operation Status, Host Name, or Time of Last Update.
Time of Last Update	Time stamp that shows the last time the status information was updated.

Enabling SCCP Applications

Use the following steps to enable one or more SCCP Applications:

1. Click **VSTP** > **Maintenance** > **SCCP Application Status**.
2. Select 1 - 20 SCCP Applications to enable.
   To select multiple SCCP Applications, press CTRL when selecting each SCCP Application. To select multiple contiguous SCCP Applications, click the first SCCP Application you want, then press SHIFT and select the last SCCP Application you want. All the SCCP Applications in between are also selected.
3. Click **Enable**.

4. Click **OK** on the confirmation screen to enable the selected SCCP Applications. If any of the selected SCCP Applications no longer exist (they have been deleted by another user), an error message displays, but any selected SCCP Applications that do exist are enabled.

Disabling SCCP Applications

Use the following steps to disable one or more SCCP Applications:

1. Click **VSTP** > **Maintenance** > **SCCP Application Status**.
2. Select 1 - 20 SCCP Applications to disable.
   To select multiple SCCP Applications, press CTRL when selecting each SCCP Application. To select multiple contiguous SCCP Applications, click the first SCCP Application you want, then press SHIFT and select the last SCCP Application you want. All the SCCP Applications in between are also selected.
3. Click **Disable**.
4. Click **OK** on the confirmation screen to disable the selected SCCP Applications. If any of the selected SCCP Applications no longer exist (they have been deleted by another user), an error message displays, but any selected SCCP Applications that do exist are disabled.

5.2.6 MP Peer Status

The **VSTP** > **Maintenance** > **MP Peer Status** page allows you to view information about existing MP Peers, including the operational status of each MP and corresponding peers.

You can perform these tasks on an Active System OAM (SOAM):

- Filter the list of peers to display only the desired peers.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by peer Name in ascending ASCII order.
- Click the + in any entry in the **Routes** field to view information about the routes associated with the peer.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.

vSTP Maintenance MP peer Status Elements

The following describes fields on the peer Status maintenance page:

Field	Description
MP	Name of the vSTP MP server.
Peer MP	Name of the peer vSTP MP server.
Status	Operational status of the vSTP MP server.
CPL	Connection priority level of the vSTP MP server.
CPL Reason	Reason for CPL Setting.

5.3 IR21 Utility

The **IR21 Utility** page converts IR21 XML files to IR21 csv files.

Import the converted IR21(IR21NetworkElement.csv and IR21RoutingInfo.csv) csv files from **Diameter Common > Import** page. The page lists all the files under **File Management** option. The directory name containing IR21 xml files is **IR21XMLGUI**.

The **VSTP** > **IR21 Utility** pages allow you to perform the conversion as follows:

5.3.1 Conversion

Select the **VSTP**, and then **IR21 Utility**, and then **Conversion** page. The page displays the following details:

- **File Name**: Name of the IR21 file.
- **Line Count**: Number of lines in the file.
- **Time Stamp**: Timestamp when the file is uploaded for conversion.

Converting Files

Perform the following steps to convert files:

1. On the **Conversion** page, select the file(s) that needs to be converted.

   > **Note:**
   >
   > Click **Convert All Files** to convert all the files.

2. Click **Convert Selected Files**.
3. Click **OK** to confirm.
   Click **Cancel** to canel the conversion.

File Management

You can perform file management operations such as, viewing, uploading, downloading, or deleting files. On the **Conversion** page, click **File Management** and select the required operation:

- **Upload**: Click **Upload** to upload new files.
- **Download**: Select the file to be downloaded and click **Download**.
- **Delete**: Select the file to be deleted and click **Delete**.
- **View**: To view the content of a file, select the file and click **View**.
  Click **Save** to save the xml file in PDF format.

  Click **Back** to go back to the file management page.
- **Deploy ISO**: To deploy the iso image, select the file and click **Deploy ISO**.
- **Validate ISO**: To verify the iso, select the file and click **Validate ISO**.

6
Maintenance

The **VSTP** > **Maintenance** pages display status information for Links, RSPs, Connections, Linksets, and SCCP applications.

The **VSTP** > **Maintenance** pages allow you to view the following information and perform the following actions:

6.1 vSTP Maintenance Link Status

The **VSTP** > **Maintenance** > **Link Status** page allows you to view information about existing links, including the operational status of each link.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of links to display only the desired Connections.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Link Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable Links
- Disable Links

vSTP Maintenance Link Status Elements

The following describes fields on the Link Status maintenance page:

Field	Description
Link Name	Name of the link.
mp Server Host Name	Hostname of the MP server from which status is reported.
Admin State	A Link's administrative state can be: • Enabled: the Link is Enabled • Disabled: the Link is Disabled • Unk: unknown; the state of the Link is not available in the database
Operational Status	A Link's administrative state can be: • Available: the Link is available for routing • Degraded: the Link is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Link is unavailable. The Operational Reason field provides additional information on this status.
Operational Reason	Reason for the Operational Status.
Link Type	Link type.

Field	Description
Linkset Name	Name of the associated linkset.
Time of Last Update	Time stamp that shows the last time the status information was updated.
Status Known	The status can be: • True: The Link status is available. • False: The Link status is not available. The value depends on the Operational Status, mp Server Host Name, Time of Last Update, or Operational Reason.

Enabling Links

Use the following steps to enable one or more links:

1. Click **VSTP** > **Maintenance** > **Link Status**.
2. Select 1 - 20 links to enable.
   To select multiple links, press CTRL when selecting each connection. To select multiple contiguous links, click the first connection you want, then press SHIFT and select the last link you want. All the links in between are also selected.
3. Click **Enable**.
4. Click **OK** on the confirmation screen to enable the selected links. If any of the selected links no longer exist (they have been deleted by another user), an error message displays, but any selected links that do exist are enabled.

Disabling Links

Use the following steps to disable one or more links:

1. Click **VSTP** > **Maintenance** > **Link Status**.
2. Select 1 - 20 links to disable.
   To select multiple links, press CTRL when selecting each connection. To select multiple contiguous links, click the first connection you want, then press SHIFT and select the last link you want. All the links in between are also selected.
3. Click **Disable**.
4. Click **OK** on the confirmation screen to disable the selected links. If any of the selected links no longer exist (they have been deleted by another user), an error message displays, but any selected links that do exist are disabled.

6.2 vSTP Maintenance Connection Status

The **VSTP** > **Maintenance** > **Connection Status** page allows you to view information about existing Connections, including the operational status of each Connection.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of Connections to display only the desired Connections.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Connection Name in ascending ASCII order.

- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable Connections
- Disable Connections

vSTP Maintenance Connection Status Elements

The following describes fields on the Connection Status maintenance page:

Field	Description
Connection Name	Name of the Connection.
mp Server Host Name	Hostname of the MP server from which status is reported.
Admin State	A Connection's administrative state can be: • Enabled: the Connection is Enabled • Disabled: the Connection is Disabled • Unk: unknown; the state of the Connection is not available in the database
Operational Status	A Connection's administrative state can be: • Available: the Connection is available for routing • Degraded: the Connection is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Connection is unavailable. The Operational Reason field provides additional information on this status.
Operational Reason	Reason for the Operational Status.
Local Host Name	Name of the local host.
Remote Host Name	Name of the remote host.
Time of Last Update	Time stamp that shows the last time the status information was updated.
Status Known	The status can be: • True: The Connection status is available. • False: The Connection status is not available. The value depends on the Operational Status, mp Server Host Name, Time of Last Update, or Operational Reason.

Enabling Connections

Use the following steps to enable one or more Connections:

1. Click **VSTP** > **Maintenance** > **Connection Status**.
2. Select 1 - 20 Connections to enable.
   To select multiple Connections, press CTRL when selecting each connection. To select multiple contiguous Connections, click the first connection you want, then press SHIFT and select the last Connection you want. All the Connections in between are also selected.

3. Click **Enable**.
4. Click **OK** on the confirmation screen to enable the selected Connections. If any of the selected Connections no longer exist (they have been deleted by another user), an error message displays, but any selected Connections that do exist are enabled.

Disabling Connections

Use the following steps to disable one or more Connections:

1. Click **VSTP** > **Maintenance** > **Connection Status**.
2. Select 1 - 20 Connections to disable.
   To select multiple Connections, press CTRL when selecting each connection. To select multiple contiguous Connections, click the first connection you want, then press SHIFT and select the last Connection you want. All the Connections in between are also selected.
3. Click **Disable**.
4. Click **OK** on the confirmation screen to disable the selected Connections. If any of the selected Connections no longer exist (they have been deleted by another user), an error message displays, but any selected Connections that do exist are disabled.

6.3 vSTP Maintenance Remote Signaling Point Status

The **VSTP** > **Maintenance** > **Remote Signaling Point Status** page allows you to view information about existing RSPs, including the operational status of each RSP.

You can perform these tasks on an Active System OAM (SOAM):

- Filter the list of RSPs to display only the desired RSPs.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by RSP Name in ascending ASCII order.
- Click the + in any entry in the **Routes** field to view information about the routes associated with the RSP.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.

vSTP Maintenance RSP Status Elements

The following describes fields on the RSP Status maintenance page:

Field	Description
MP server	Name of the vSTP MP server that is currently reporting the status of the RSP.
RSP Name	Name of the RSP.
mp Server Host Name	Hostname of the MP server from which status is reported.

Field	Description
Operational Status	A RSP's administrative state can be: • Available: the RSP is available for routing • Degraded: the RSP is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the RSP is unavailable. The Operational Reason field provides additional information on this status.
Point Code	Unique address of the RSP.
Routes	RSP route. An RSP can have two routes.
Route Adjacent Status	The status of adjacent part. It can have these four status: • Down: The adjacent part to RSP is down. • UP: The adjacent part to RSP is up. • Restricted: The adjacent part to RSP is restricted.. • Unassigned: The adjacent part to RSP is not assigned to any other RSP.
Route Name	Name of the route.
Route Remote Status	The status of the non adjacent part. The route remote status can be: • Available: The non-adjacent part to RSP is available. • Unavailable: The non-adjacent part to RSP is unavailable. • Restricted: The non-adjacent part to RSP is restricted. • Unassigned: The non-adjacent part to RSP is not assigned to any other RSP.
SS7 Domain Type	Types of SS7 Domain. The values can be: • ANSI • ITUI • ITUN • ITUN24 • ITUI_S • ITUN_S
Status Known	Status can have the following values: • True: The RSP status is known. • False: The RSP status is unknown.
Last Updated	The congestion level of the Link Set. This is the lowest of the congestion levels of all the Links configured in the Link Set. The congestion level options are: • Normal • CL1 • CL2 • CL3

6.4 vSTP Maintenance Link Set Status

The **VSTP** > **Maintenance** > **Link Set Status** page allows you to view information about existing Linksets, including the operational status of each Linkset.

You can perform these tasks on an Active System OAM (SOAM):

- Filter the list of Linksets to display only the desired Linksets.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by Linkset Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.

vSTP Maintenance Linkset Status Elements

The following describes fields on the Linkset status maintenance page:

Field	Description
Congestion Level	The congestion level of the Link Set. This is the lowest of the congestion levels of all the Links configured in the Link Set. The congestion level options can be : • Normal • CL1 • CL2 • CL3
MP server	Name of the vSTP MP server that is currently reporting the status of the Link Set.
Link Set Name	Name of the Linkset.
mp Server Host Name	Hostname of the MP server from which status is reported.
Operational Reason	Reason for the operational status.
Operational Status	A Linkset's administrative state can be: • Available: the Linkset is available for routing • Degraded: the Linkset is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the Linkset is unavailable. The Operational Reason field provides additional information on this status.
Status Known	Status can be: • True: The Linkset status is known. • False: The Linkset status is unknown. The value depends on Operational Status, Congestion Level, Last Updated, Operational Reason values.
Last Updated	Time stamp which indicates the last time status information was updated.

6.5 vSTP Maintenance SCCP Application Status

The **VSTP** > **Maintenance** > **SCCP Application Status** page allows you to view information about existing SCCP Applications, including the operational status of each SCCP Application.

You can perform these tasks on an Active System OAM (SOAM).

- Filter the list of SCCP Applications to display only the desired applications.
- Sort the list by a column, in ascending or descending order, by clicking the column heading. The default order is by SCCP Application Name in ascending ASCII order.
- Prevent the page from automatically refreshing by clicking the **Pause updates** checkbox.
- Enable SCCP Applications.
- Disable SCCP Applications.

vSTP Maintenance SCCP Application Status Elements

The following describes fields on the SCCP Application Status maintenance page:

Field	Description
Admin State	A SCCP Application's administrative state can be: • Enabled: the SCCP Application is Enabled • Disabled: the SCCP Application is Disabled • Unk: unknown; the state of the SCCP Application is not available in the database
App Id	The unique ID of the application.
Operational State	A SCCP Application's administrative state can be: • Available: the SCCP Application is available for routing • Degraded: the SCCP Application is not unavailable but it is not operating as expected. The Operational Reason field provides additional information on this status. • Unavailable: the SCCP Application is unavailable. The Operational Reason field provides additional information on this status.
App Type	Type of Application. Options are: • EIR • ATINP • INPQ • SFAPP
Host Name	The name of vSTP MP server that is currently reporting the status of this application.
SSN	Sub System Number

Field	Description
Status Known	Status values can be: • True: The application status is known. • False: The application status is unknown. The value depends on Operation Status, Host Name, or Time of Last Update.
Time of Last Update	Time stamp that shows the last time the status information was updated.

Enabling SCCP Applications

Use the following steps to enable one or more SCCP Applications:

1. Click **VSTP** > **Maintenance** > **SCCP Application Status**.
2. Select 1 - 20 SCCP Applications to enable.
   To select multiple SCCP Applications, press CTRL when selecting each SCCP Application. To select multiple contiguous SCCP Applications, click the first SCCP Application you want, then press SHIFT and select the last SCCP Application you want. All the SCCP Applications in between are also selected.
3. Click **Enable**.
4. Click **OK** on the confirmation screen to enable the selected SCCP Applications.
   If any of the selected SCCP Applications no longer exist (they have been deleted by another user), an error message displays, but any selected SCCP Applications that do exist are enabled.

Disabling SCCP Applications

Use the following steps to disable one or more SCCP Applications:

1. Click **VSTP** > **Maintenance** > **SCCP Application Status**.
2. Select 1 - 20 SCCP Applications to disable.
   To select multiple SCCP Applications, press CTRL when selecting each SCCP Application. To select multiple contiguous SCCP Applications, click the first SCCP Application you want, then press SHIFT and select the last SCCP Application you want. All the SCCP Applications in between are also selected.
3. Click **Disable**.
4. Click **OK** on the confirmation screen to disable the selected SCCP Applications.
   If any of the selected SCCP Applications no longer exist (they have been deleted by another user), an error message displays, but any selected SCCP Applications that do exist are disabled.

7

Alarms, Errors, KPIs, and Measurements

This chapter describes the types of alarm, error, KPI, and measurements information that is available for vSTP.

7.1 vSTP Alarms and Events

The vSTP alarms and events are described in the *Alarms and KPIs Reference*, which can be accessed as described in the DSR *Getting Started* manual.

Active alarms and events and alarm and event history can be displayed on the **Alarms & Events**, and then **View Active** and **Alarms & Events**, and then **View History** pages.

7.2 vSTP Measurements

Measurements for vSTP are collected and reported in various measurement groups.

A measurement report and a measurement group can be associated with a one-to-one relationship. A measurements report can be generated with report criteria selected on the **Measurements**, and then **Reports** page.

The *Measurements Reference*, which can be accessed as described in the DSR *Getting Started* manual, explains the report selection criteria and describes each measurement in each measurement group.

7.3 vSTP Errors

Errors for vSTP are collected and reported in various error groups.

GTT Actions

Resource GTT Actions (/vstp/gttactions).

A GTT Action entry consists of an Action ID, an action, and action-specific data. The action specified in the entry determines the actions performed on the MSU during translation.

GTT Actions is added in DSR 8.2 as part of the GTT actions feature.

Table 7-1 GTT Actions Errors

Error Code Number	Description
001 - Missing Field Value	
002 - Invalid Syntax	CGPC must be in proper point code format.
003 - Field value must be unique	The GTT Action entry specified by the actid parameter cannot already exist in the database.

Table 7-1 (Cont.) GTT Actions Errors

Error Code Number	Description
071 - Operation failed. The entry no longer exists	The specified MAP set must already exist in the database or MRN table. or The specified Action ID must already exist in the database. or The specified GTT Action entry must already exist in the database.
50136 - MAPSET must be specified (only) if RI parameter is SSN	If the ri=gt parameter is specified, then the mapset parameter cannot be specified.
50137 - MRNSET must be specified (only) if RI parameter is GT	If the ri=ssn parameter is specified, then the mrnset parameter cannot be specified.
50141 - With FGTTLS feature in OFF state, MAP Set Id must not be specified	The Flexible GTT Load Sharing feature must be enabled before the mapset parameter can be specified.
50142 - With FGTTLS and IGTTLS feature in OFF state, MRN Set ID must not be specified	The Flexible GTT Load-Sharing feature must be enabled before the mrnset parameter can be specified.
50143 - RSP does not exist in the routing table	The value specified for the rsp parameter must already exist as a destination in the Route table.
50207 - RSP does not exist in specified MRNSET	If the Flexible GTT Load Sharing feature is enabled, the specified PC must already exist in the specified MRN set.
50208 - RSP/SSN does not exist in MAPSET	The specified rsp and ssn must already exist in the specified MAP set. or If the rsp, ri=ssn and ssn parameters are specified, then the RSP/SSN must be populated in the MAPSET table.

Table 7-1 (Cont.) GTT Actions Errors

Error Code Number	Description
50215 - Invalid parameter combination specified	• A value of disc, udts, tcaperr must be specified for the act parameter before a value of uimreqd can be specified for the on or off parameter. or • A value of dup or fwd must be specified for the act parameter before the rspName, cgpc, cgpcogmsg, domain, ssn, ri, mrnset, mapset parameter can be specified and before a value of useicmsg can be specified for the on or off parameter. • The act=tcaperr parameter must be specified before the atcaperr and itcaperr parameters can be specified. • The act=udts parameter must be specified before the udtserr parameter can be specified. • The act=fwd parameter must be specified before the defactid parameter can be specified. or • A value of fwd, dup must be specified for the act parameter before a value of useicmsg can be specified for the on or off parameter.
50216 - RSP and CGPC must be of same domain	The values specified for the RSP and CGPC parameters must have the same domain. or The rspName and CGPC parameters must have the same domain.
50217 - Maximum number of GTT Actions within this site has already been configured (max={2000})	The GTT Action table cannot contain more than 2000 entries.
50218 - CGPC/DOMAIN must be specified	If a value of dup or fwd is specified for the act parameter then the rspName parameter must be specified. If the ri=ssn parameter is specified, then the ssn parameter must be specified. If the value of the cgpcogmsg=provcgpc parameter is specified, then the cgpc and domain parameter must be specified.
50219 - GTT Action ID does not exist	The GTT Action ID specified by the defactid parameter must already exist.
50220 - The type of the action for DEFACTID shall be disc, udts, tcaperr	A value of disc, utds, or tcaperr must be specified for the defactid parameter.

Table 7-1 (Cont.) GTT Actions Errors

Error Code Number	Description
50221 - GTT Action entry is referenced	The value specified by the act parameter cannot be changed until the associated Action ID is referenced by an Action Set or by any forward action. or The Action ID specified by the actid parameter cannot be referenced by an Action Set or an action entry that is associated an action of fwd.
50222 - GTT Action entry is referenced and can only be changed from disc/udts/tcaperr to disc/udts/tcap.	The value can only be changed from disc/udts/tcaperr to disc/udts/tcaperr.
50223 - GTT Action ID must not be fallback	A value of fallback cannot be specified for the actid parameter.

GTT Action Sets

Resource GTT Action Sets (/vstp/gttactionsets).

Global Title Translation (GTT) Action Set consists of an Action Set name and a group of actions.

Table 7-2 GTT Action Sets Errors

Error Code Number	Description
001 - Missing Field Value	At least one Action ID should be provided in GTT Action Set.
50231 - GTT Action name already provisioned in GTT Action Set	The value specified by the actsn parameter cannot already exist in a GTT Action Set.
50232 - GTT Action ID does not exist	The Action ID specified by the actid1/actid2 parameter(s) must already exist in the GTT Action table.
50233 - Maximum number of GTT Action Set within this site has already been configured (max={20000}).	The GTT Action Set table cannot contain more than 20000 entries.
50234 - Invalid Combinations. ACTID1 should be DUP	If one action Id is provided, then it can be associated with an action of any type (dup, disc, udts, tcaperr, fwd) in GTT Action Set. If both action Ids are provided, then first action id should be associated with an action of 'dup', and second action id should be associated with an action of disc, udts, tcaperr, or fwd in GTT Action Set.
50235 - GTT Action IDs should be unique in a GTT Action Set	The actid1/actid2 parameters must each specify a unique GTT Action ID in the command.
50236 - GTT Action Set does not exist	The specified GTT Action Set name must already exist in the database.

Table 7-2 (Cont.) GTT Action Sets Errors

Error Code Number	Description
50236 - GTT Action ID does not exist	The Action ID specified by the actid1/actid2 parameter(s) must already exist in the GTT Action table.
50237 - GTT Action Set is referenced by translations	The GTT Action entry cannot be referred by any translation entry.
50334 - GTT Action DUP and FWD must have same domain	GTTASET: Dup and Fwd Actions must have same domain, implement error code as per Bug# 26809167.

GTT Selectors

Resource GTT Selectors (/vstp/gttselectors).

Global Title Translation (GTT) Selector is an entity assigned to a GTT Set.

Table 7-3 GTT Selectors Errors

Error Code Number	Description
001 - Missing Field Value	At least one GTT set name parameter must be specified. These parameters include: • gttsn or • cdgttsn and/or cggttsn
071 - Operation failed. The entry no longer exists	The linkset specified by the linksetName parameter must already exist. or The value specified for the gttsn parameter must match the name of an existing GTT set. or The GTT set specified by the gttsn parameter must already exist in the GTT Set table. or The GTT set specified by the cdgttsn parameter must already exist in the GTT Set table.

Table 7-3 (Cont.) GTT Selectors Errors

Error Code Number	Description
50106 - Translation Type, NAI(v) and NP(v) must be specified when GTI value is \'TtNumEncodingNature\'	If a value of 2 or 4 is specified for the gti(x) parameter, then the tt parameter must be specified. or If the gtii/gtin/gtin24/gtiis/gtins/ gtin16=4 parameter is specified, an np(v)/ nai(v) parameter combination must be specified. These parameters can be specified in any combination. or If the gtii/gtin/gtin24/gtiis/gtins/ gtin16=4 parameter is specified, an np(v)/ nai(v) parameter combination must be specified. These parameters can be specified in any combination: np/naiv, npv/nai, np/nai, or npv/naiv.
50107 - Translation Type must be specified when GTI value is \'TtOnly\'	If a value of 2 or 4 is specified for the gti(x) parameter, then the tt parameter must be specified.
50108 - NAI(v) or NP(v) must not be specified when GTI value is \'TtOnly\'	If the gti/gtia/gtii/gtin/gtin24/gtiis/gtins/ gtin16=2 parameter is specified, then the np/npv and nai/naiv parameters cannot be specified.
50109 - NAI(v), NP(v), or TT must not be specified when GTI value is \'NoGlobal\"	If the gti(x)=0 parameter is specified, then the tt, np/npv, and nai/naiv parameters cannot be specified. or If the gti(x)=0 parameter is specified, then the eaglegen, tt, np/npv, and nai/ naiv parameters cannot be specified.
50110 - NAI entries per TT-NP combination has reached allowed max of {max}	If the gti(x)=4 parameter is specified, then the GTT selector table cannot have more than 5 nai entries per tt/np combination.
50111 - NAI and NAI Value both cannot be specified	The nai and naiv parameters cannot be specified in the same command. or The nai and naiv parameters cannot be specified together in the same command.
50112 - NP and NP Value both cannot be specified	The np and npv parameters cannot be specified in the same command. or The np and npv parameters cannot be specified together in the same command.
50113 - CdPA GTT Set type must be cdgta	The GTT set specified by the gttsn parameter must have a set type of cdgta
50114 - GTT Selector domain does not match with the domain of the GTT set	The network domain of the specified GTT selector must match the domain of the GTT set that is specified by the cdgttsn and/or cggttsn parameter.

Table 7-3 (Cont.) GTT Selectors Errors

Error Code Number	Description
50165 - GTI and TT/NP/NAI/CGSSN/SELID/ LINKSET combination is not unique	An entry cannot already exist that matches the gti, tt, and np(v), and nai(v) and cgssn and selid and linkset parameter combination for the specified CdPA and/or CgPA selector.
50248 - MBR settypes cannot be referenced by GTT selectors	The MBR supported GTT set types (IMSI/ MSISDN) cannot be referenced by GTT selectors.
50249 - GTTSN and CDGTTSN/CGGTTSN/ LINKSETNAME/CGSSN/SELID are mutually exclusive	The gttsn and cdgttsn/cggttsn/linkset name/ cgssn/selid parameters cannot be specified together in the command.
50250 - CGSSN and CDGTTSN value both cannot be specified	The cgssn and cdgttsn parameters cannot be specified together in the command.
50251 - LinkSet domain must match the domain of GTT selector	The linkset domain must match the domain of the GTT selector.

GTT Addresses

Resource GTT Addresses (/vstp/globaltitleaddresses).

Global Title Translation (GTT) Global title address (GTA) information for applicable global title selectors required to specify a global title entry.

Table 7-4 GTT Addresses Errors

Error Code Number	Description
GTT Set Name: {ERR_ONT_002} - Invalid Syntax.	The gttsn parameter must be specified and must match an existing gttsn.
Routing Signaling Point: {ERR_ONT_002} - Invalid Syntax.	The pc parameter cannot be out of range.
50122 - Maximum Number of GTA have already been configured. (max={50000}).	The GTT table cannot be full in case a delete command causes a split requiring more entries to be added.
50122 - Maximum Number of GTA have already been configured. (max={270000}).	The GTA table cannot contain more than 270000 entries.
50122 - OPTSN GTT set type is not compatible with GTTSN set type	If the GTTSN set has a set type of cdgta or cdssn, then the OPTSN set cannot have a set type of opc. If the GTTSN set has a set type of opcode, then the OPTSN set cannot have a set type of opc. If the GTTSN set has a set type of MBR (imsi/ msisdn), then the OPTSN set type cannot have the same set type as GTTSN. If the OPTSN set has a set type of MBR (imsi/ vmsisdn), then the GTTSET must have a set type of MBR (imsi/msisdn) or opcode.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
50126 - GTA End Address must be greater than or equal to the value of the GTA Start Address	If the endAddress/emapaddr parameter is specified, then the value of the endAddress/ emapaddr parameter must be greater than or equal to the value of the startAddress/ smapaddr parameter.
50128 - Routing Indicator must be specified as \'GT\' when Translate Indicator is \'DPCNGT\'.	If the xlat=dpcngt parameter is specified, then the ri=gt parameter must be specified.
50129 - Sub System Number must be specified when Translate Indicator is \'DPCSSN\'	If the xlat=dpcssn parameter is specified, then the ssn parameter must be specified.
50134 - Start Address and End Address Range is overlaping with existing GTA - {gttsets}	The specified startAddress/ endAddress or smapaddr/emapaddr range must exist for the specified GTT set in the STP active database. While an exact match is not required, you cannot specify an overlap with another range. If the range overlaps, an error is generated that displays a list of overlapped global title addresses. An example follows that shows what happens when the user attempts to enter a global title address range (such as 8005550000 to 8005559999) that overlaps an existing range. The overlapping links must match. If they do not, the error message displays the list of overlapped global title addresses.
50135 - Translate Indicator must be \'DPCSSN\' when Sub System Number is specified	If the ssn parameter is specified, then the xlat=dpcssn parameter must be specified.
50143 - RSP does not exist in the routing table	The value specified for the pc parameter must exist as a destination in the Route table or reside in a cluster that exists as a destination in the Route table (for global routing).
50176 - Length of ENDADDRESS/ EMAPADDR must be equal to length of STARTADDRESS/SMAPADDR	If the endAddress/emapaddr parameter is specified, then the values of the startAddress/smapaddr and endAddress/ emapaddr parameters must be the same length.
50176 - Exceeding max GTA Lengths supported per GTT SET (max={16}).	Since the Support for 16 GTT Lengths in VGTT feature is always turned on, up to 16 GTA/SADDR lengths can exist per GTT set. or The Support for 16 GTT Lengths in VGTT feature, then up to 16 GTA/SADDR lengths can exist per GTT set.
50182 - Update of GTT Set is not allowed	gttsn (Gtt Set name) should not be edited.
50183 - Update of GTA Start Address is not allowed	gta (start gta) should not be edited.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
50204 - RSP does not exist in specified MAPSET	If a final GTT (the ri=ssn parameter is specified with the xlat=dpc parameter), then the PC (pc/pca/pci/pcn/pcn24/pcn16) must exist in the Remote Point Code/MAP table. or If a final GTT (the ri=ssn parameter is specified with the xlat=dpc parameter), then the PC must exist in the Remote Point Code/MAP table.
xxxxx - ACN parameter is allowed with ITU TCAP PKGTYPE	If the acn parameter is specified, then a value of bgn, ituabort, ituuni, any, end, or cnt must be specified for the pkgtype parameter.
xxxxx - Both FAMILY and OPCODE must be NONE if either is NONE	If the family and opcode parameters are specified in the command, then either both parameters must have a value of none or neither parameter can have a value of none.
xxxxx - CCGT must be NO when the RI is set to GT	If the ri=gt parameter is specified, then the ccgt=no parameter must be specified.
xxxxx - CDSSN param must be specified if GTTSN settype is CDSSN	If the GTT set specified by the gttsn parameter has a set type of cdssn (see the ent-gttset command), then the cdssn parameter must be specified. This parameter cannot be specified for GTT sets with other set types.
xxxxx - CGPCx parm must be specified if GTTSN is type of CGPC	If the GTTSN set type has a value of cgpc, the cgpc/cgpca/cgpci/cgpcn/cgpcn24 parameter must be specified. This parameter cannot be specified for other set types. or If the GTTSN set type has a value of cgpc, the cgpc parameter must be specified. This parameter cannot be specified for other set types.
xxxxx - CGSSN cannot be specified with OPTSN/OPCSN/CGSELID	If the cgssn parameter is specified, then the optsn, opcsn, and cgselid parameters cannot be specified. or If the cgssn parameter is specified, then the optsn and cgselid parameters cannot be specified.
xxxxx - CGSSN/CDSSN range cannot overlap an existing range	The range specified by the cdssn/ecdssn and cgssn/ecgssn parameters cannot overlap a currently existing range for the specified GTT set.
xxxxx - CGSSN parm must be specified if GTTSN is type of CGSSN	If the GTTSN set type has a value of cgssn, the cgssn parameter must be specified. The cgssn parameter cannot be specified for GTTSN of other types.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
xxxxx - DEFMAPVR is supported by MBR GTT settypes	The defmapvr parameter can be specified in the GTA command for the ITU opcode entry if the GTT set specified by the optsn parameter is of MBR type (IMSI/MSISDN).
xxxxx - End value must be greater than or equal to a starting value	The value specified for the ecgssn or ecdssn parameter must be greater than the value specified for the cgssn or cdssn parameter.
xxxxx - FAMILY parameter is allowed with ANSI TCAP PKGTYPE	If the family parameter is specified, then a value of ansiuni, qwp, qwop, resp, cwp, cwop, ansiabort, or any must be specified for the pkgtype parameter.
xxxxx - GTA End Address must be greater than or equal to the value of the GTA Start Address	If the endAddress/emapaddr parameter is specified, then the value of the endAddress/ emapaddr parameter must be greater than or equal to the value of the startAddress/ smapaddr parameter.
xxxxx - GTA parm must be specified if GTTSN is type of CDGTA/CGGTA	The GTA must be specified if the GTTSN set type has a value of cdgta or cggta. The GTA cannot be specified for other set types.
xxxxx - GTT Action Set does not exist	The specified GTT Action Set must already exist in the database.
xxxxx - GTTSET MBR Settypes Support ITU BGN/CNT/END Pkgtype	If the GTT set specified by the optsn parameter is of MBR type (IMSI/ MSISDN) in the GTA command for the ITU opcode entry, then the package type specified via the pkgtype parameter must be ITU BGN/CNT/END.
xxxxx - GTT Set specified by OPTSN/OPCSN does not exist	The GTT set specified by the optsn and opcsn (cgcnvsn is not supported by VSTP) parameter must match an existing GTT set.
xxxxx - GTTSN set name must not be same as OPTSN set name	The same value cannot be specified for the gttsn and optsn parameters.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
xxxxx - Invalid parameter combination specified	If the cgssn parameter is specified, then the ecdssn parameter cannot be specified. If the cdssn parameter is specified, then the ecgssn parameter cannot be specified. or If the xlat=none parameter is specified, then the ri, pc/pca/pci/pcn/pcn24/pcn16, force, ssn and ccgt parameters cannot be specified. or The specified GTT set must have a set type of opcode (see the ent-gttset command) before the opcode/acn/pkgtype or opcode/family/pkgtype parameters can be specified. The specified GTT set must have a set type of cdssn, cgssn, cdgta/cgta, opc, or cgpc before the cdssn, cgssn, gta, opc, or cgpc parameter, respectively, can be specified. or The acn and family parameters cannot be specified together in the command. or If the opc parameter is specified, then the startAddress/endAddress, (e)cgssn, (e)cdssn, and opcode parameters cannot be specified.
xxxxx - OPCODE param must be specified if GTTSN settype is OPCODE	If the GTT set specified by the gttsn parameter has a set type of opcode (see the ent-gttset command), then the opcode/acn/pkgtype or opcode/family/pkgtype parameter must be specified. These parameters cannot be specified for GTT sets of any other set types.
xxxxx - OPCODE, PKGTYPE, ACN/FAMILY must be specified together	The opcode, pkgtype, and family parameters must be specified together for ANSI TCAP translations. The opcode, pkgtype, and acn parameters must be specified together for ITU TCAP translations.
xxxxx - OPCSN is valid with cdgta/cdssn/opcode GTTSN type	The GTT set specified by the gttsn parameter must have a set type of cdgta, opcode, or cdssn (see the ent-gttset command) before the opcsn parameter can be specified.
xxxxx - OPCSN set domain must be the same as GTTSN set domain	The OPC set name domain must be the same as the GTTSN set domain. If the GTT set domain is ANSI, then the OPC set name domain must be ANSI. If the GTT set domain is ITU, then the OPC set name domain must be ITU.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
xxxxx - OPCx parm must be specified if GTTSN is type of OPC	The opc parameter must be specified if the GTTSN set type has a value of opc. These parameters cannot be specified for other set types.
xxxxx - OPTSN and CGSELID/CDSELID are mutually exclusive	The cdselid, cgselid, and optsn parameters cannot be specified together in the command. If the GTT set has a set type of cdgta, cdssn, or opcode, then the opcsn parameter can be specified with one of the above parameters.
xxxxx - OPTSN GTT set type is not compatible with GTTSN set type.	If the GTTSN set has a set type of cdgta or cdssn, then the OPTSN set cannot have a set type of opc. If the GTTSN set has a set type of opcode, then the OPTSN set cannot have a set type of opc. If the GTTSN set has a set type of MBR (imsi/msisdn), then the OPTSN set type cannot have the same set type as GTTSN. If the OPTSN set has a set type of MBR (imsi/vmsisdn), then the GTTSET must have a set type of MBR (imsi/msisdn) or opcode.
xxxxx - PKGTYPE abort requires ACN/FAMILY/OPCODE value none	If the pkgtype=ituabort parameter is specified, then a value of none must be specified for the acn and opcode parameters.
xxxxx - Point code out of range	The cgpc, opc parameters must have a valid value within the range for each subfield.
xxxxx - RI must be SSN when CCGT is YES	If the ccgt=yes parameter is specified, then the ri=ssn parameter must be specified.
xxxxx - Set type of GTT Set Name doesn't match	The GTT set name specified by the opcsn parameter must have a set type of opc (see the ent-gttset command).
xxxxx - SMAPADDR must be specified for MBR GTT settypes	The smapaddr parameter must be specified if the GTT set specified by the gttsn parameter is of MBR type (IMSI/MSISDN).
xxxxx - STARTADDRESS/CGPC/OPC/CG-CDSSN/OPCODE/DPC/SMAPADDR are mutually xclusve	The cgpc, cgssn, gta, opc, cdssn, opcode, and smapaddr parameters cannot be specified together in the command.
xxxxx - STARTADDRESS/CGPC/OPC/CGSSN/CDSSN/OPCODE/DPC/SMAPADDR must be specified	The startAddress, cgpc, opc, cgssn, cdssn, opcode/acn/pkgtype, opcode/family/pkgtype or smapaddr parameter must be specified.
xxxxx - Translation entry already exists	The translation entry specified by the cgpc, opcode, opc parameters cannot already exist.

Table 7-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
SQL error: Database Operation Failed	Failure while reading GTT Action Set Table. or The GTT Set table is corrupt or cannot be found. or The GTA table is corrupt or cannot be found. or The Route table is corrupt or cannot be found. or The MRN table is corrupt or cannot be found. or The MAP table is corrupt or cannot be found.

GTT Sets

Resource GTT Sets (/vstp/gttsets).

A GTT set consists of a GTT set name, the domain of the point codes used in the translation. After the GTT set is provisioned, you can enter subsequent GTT Selectors and GTAs. It is a collection of GTAs which are searched during GTT routing.

Table 7-5 GTT Sets Errors

Error Code Number	Description
003 - Field value must be unique	The gttsn parameter must be specified and must not match an existing gttsn.
071 - Operation Failed, the entry no longer exists.	The gttsn parameter must be specified and must match an existing GTT set. or The value specified for the gttsn parameter must match the name of an existing GTT Set.
50098 - Maximum number of GTT Set within this site have already been configured (max={2000})	The GTT Set table cannot contain more than 2000 entries.
50100 - Delete Failed. Selected GTT Set is assoicated with GTAs	The GTT set cannot be deleted if it is referenced in the GTTSEL or GTA tables.
50101 - Delete Failed. Selected GTT Set is associated with GTT Selectors	The GTT set cannot be deleted if it is referenced by npsn.
50238 - GTT settype and NPSN settype should be of MBR settypes	The GTT set type of the GTT set entry and the set type of associated NPSN parameter should be of MBR (IMSI/MSISDN) set types.
50239 - NPSN SETTYPE should be different from GTT SETTYPE	The GTT set type of the GTT set entry referred to by the NPSN parameter should be different from the GTT set type referred to by the GTTSN parameter.
50240 - NPSN not configured under GTTSET	The value specified for the NPSN parameter must be an existing GTT set of MBR (IMSI/MSISDN) set types.

Table 7-5 (Cont.) GTT Sets Errors

Error Code Number	Description
50241 - GTTSET and NPSN set domain mismatch	The GTTSET domain and associated NPSN set domain must match.
50242 - GTT Set does not exist	The specified GTT Set name must already exist in the database.
50243 - GTT Set already referenced in GTTSELECTOR/GTA/GTTSET. Domain/Type cannot be changed	If GTT Set is referenced in GTT Selector or GTA or in NPSN parameter of GTT Set, then user is not allowed to update domain and settype. In this case, only npsn parameter can be changed.
50244 - GTT Set already referenced in GTTSET as NPSN	
xxxxx - GTTSN and NPSN must not form Circular Entries	The GTT set specified by the gttsn parameter must not be associated with the GTT set referred by the NPSN parameter.
SQL error: Database Operation Failed	The GTT Set table must be accessible.

Link Sets

Resource GTT Link Sets (/vstp/linksets).

A Link Set is a logical element representing link attributes assigned to a link and a far end-point assigned to a Route.

Table 7-6 Link Sets Errors

Error Code Number	Description
AS Notification: {ERR_ONT_002}	The ipsg=yes and adapter=m3ua parameters must be specified before the asnotif parameter can be specified.
Link TPS: {ERR_ONT_002}	The value specified for the slktps/ rsvdslktps and maxslktps parameters must be within the allowed range. slktps/rsvdslktps maxslktps
Link Name: {ERR_ONT_003}	The specified linkset name cannot already exist in the database.
50068 - Maximum number of Link Set within this site have already been configured (max={max})	The maximum number of linksets that can be defined in the system is 1024.
50072 - Delete Failed: This Link Set is associated with Link	The linkset can be removed only if all links associated with the linkset have been removed.
50073 - Delete Failed: This Link Set is associated with Route	If the linkset is referenced by the historic routeset of any destination, then this command cannot be entered.

Table 7-6 (Cont.) Link Sets Errors

Error Code Number	Description
50075 - Point code already in use in Local Signaling Point={name}	The specified adjacent point code cannot be the same as the self-ID destination point code of the STP. or The adjacent point code cannot match the site point code.
50086 - ITU Transfer Restricted can only be configued for ITUN linksets	The itutfr parameter is valid only for ITU linksets.
50093 - Link Set type cannot be updated when current Link Set is referenced by any Link	If the IPSG linkset contains links, then the adapter parameter cannot be specified.
50161 - Remote Signaling Point must be unique for Link Sets	The specified adjacent point code cannot be assigned to any other linkset. or The value of the apc/apca/apci/apcn/ apcn24/apcn16 or sapc/sapca/sapci/sapcn/ sapcn24 parameter cannot be assigned to more than one linkset. or The apc/apca/apci/apcn/apcn24 or sapc/ sapca/sapci/sapcn/sapcn24 parameter can be defined only once per linkset.
50214 - Routing context can only be configured for M3UA linksets	The ipsg=yes and the adapter=m3ua parameters must be specified before the rcontext parameter can be specified.
50215 - Could not locate adapter type	The adapter type specified must be either m3ua or m2pa.
50246 - Could not locate adapter type	The adapter type specified must be either m3ua or m2pa.
50247 - Linkset referenced by GTT selector table	If the linkset is referenced by the GTT selector table, then this command cannot be entered.
HTTP/1.1 404 Not Found Item does not exist	The specified linkset must be in the database.
LinkSet: {ERR_OPR_FAILED_NO_ENTRY}	The linkset name must be in the database.

SCCP Options

Resource SCCP Options (/vstp/sccpoptions).

SCCP Options are those configuration values that govern the overall SCCP functionality.

Table 7-7 SCCP Options Errors

Error Code Number	Description
50177 - Transaction Based GTT Load Sharing Feature not enabled	The Transaction-based GTT Loadsharing feature must be enabled before the tgtt0, tgtt1, tgttudtkey, or tgttxudkey parameters can be specified.