Oracle® Communications Diameter Signaling Router

Virtual Signaling Transfer Point User Guide

Release 9.2.0.0.0
G24662-01
September 2025

ORACLE

Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User Guide, Release 9.2.0.0.0

G24662-01

Contents

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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.

What's New in This Guide

This section introduces the documentation updates for Release 9.2.0.0.0.

Release 9.2.0.0.0 - G24662-01, September 2025

- Updated the "Admin State" parameter in the vSTP Maintenance Link Status Elements.
- Updated the "Group Code" parameter description in the Table 5-3.
- Updated the "Group Code" parameter description in the Table 5-4.
- Added a note about IR21.xml files in the IR21 Utility section.
- Added XList Status field in the Maintenance section.
- Added the parameter "Full RSP Point Code" in the Table 5-15.
- Added the parameter "Actname" in the Table 5-20.
- Added Gserv Data in the Configurations section.
- Added "Admin State" parameter in the vSTP Maintenance RSP Status Elements.
- Updated Interaction section to provide information about group code.
- Added a note in the Tracing and Troubleshooting section about validating the "traceoam" process status post SOAM server upgrade.
- Updated the code for the following topics in the MMI Managed Objects for Duplicate Point Code section:
  - localsignalingpoints - Display, Update
  - remotesignalingpoints - Insert, Update, Delete
  - networkappearances - Insert
- Updated Dependencies to provide information about conversion between ITU-I and ITU-N or ANS.
- Added the following parameters in the vSTP Maintenance Linkset Status Elements:
  - Enable
  - Disable
- Added the following parameter in the Table 5-13:
  - Full RSP Point Code
  - Cluster X-List Expire Timer
  - ATI GTT Set Name
- Added the following parameters in the Table 5-4:
  - Exception List Exclusion Indicator
  - Nested Cluster Allowed Indicator
  - Enable
  - Disable
- Added the following parameters in the Table 5-38:
  - XList Expiry Timer Duration

  - XList Cluster Threshold
  - CNCF
- Added the following parameters in the Table 5-22:
  - Enable Intermediate GTT Act
  - sriPrepaid
- Added the following features in the vSTP Features section:
  - Cluster Routing Support
    - Feature Configuration Cluster Routing Support
      - GUI Configuration Cluster Routing Support
      - MMI Managed Objects for Cluster Routing
      - Alarms/Events and Measurements Cluster Routing Support
  - Nested Cluster Routing
    - Feature Configuration Nested Cluster Routing
      - GUI Configuration Nested Cluster Routing
      - MMI Managed Objects for Nested Cluster Routing
  - Network Routing
- Added vSTP Gateway Screening and following sections:
  - MTP3 Screening
  - SCCP Screening
- Added the following feature in the vSTP Features section:
  - Calling Name Conversion Facility (CNCF)
    - Feature Configuration CNCF
      - GUI Configuration CNCF
      - MMI Managed Objects CNCF
      - Alarms/Events and Measurements CNCF
    - Troubleshooting
    - Dependencies

Acronyms

Following are the list of acronyms:

Table Acronyms

Short Form	Description
MTP3	Message Transfer Point
OPC	Originating Point Code
VSTP	Virtual Signaling Transfer Point
SCCP	Signaling Connection Control Part
MEAL	Measurement Event Alarm Logging
CGPA	Calling Party Address
CDPA	Called Party Address
GTT	Global title Translation
GTA	Global Title Address
FLOBR	Flexible Origin Based Routing

1

Introduction

This document provides information about the role of Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point (vSTP) in signaling and how to configure and use the vSTP functionality and services.

1.1 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
vSTP Features

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

2.1 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.

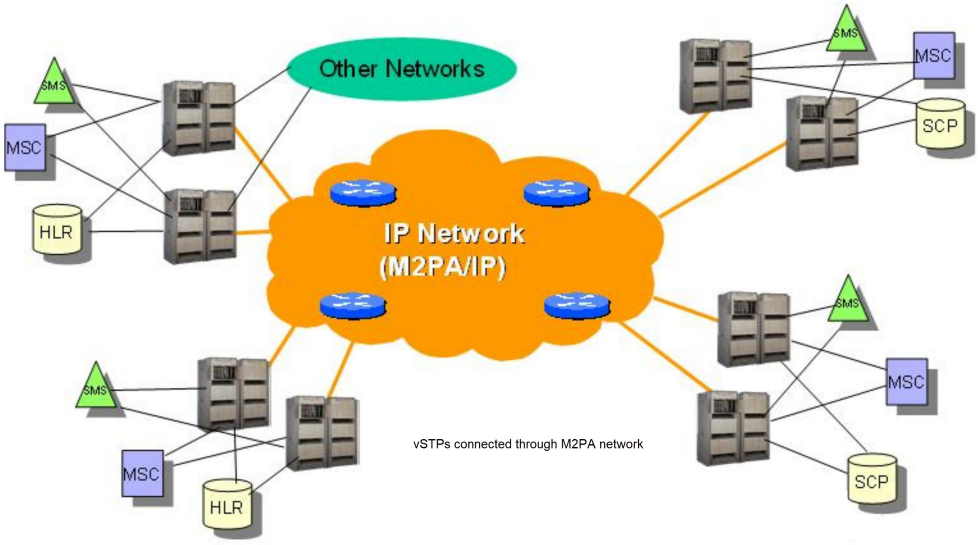
> **Note**
>
> As a Signaling Gateway, vSTP should always be configured as M3UA Server (SG role).

2.2 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



2.3 Global Title Translation

The Global Title Translation (GTT) feature is designed for the Signaling Connection Control Part (SCCP) of the SS7 protocol. For detailed information about this feature, refer to *vSTP SS7 Security User's Guide*.

2.4 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.

2.4.1 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.

2.4.2 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.

2.5 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 2-1 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 2-1 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 2-2 shows how the states of the RC group are determined.

Table 2-2 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 2-3, 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 2-3 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 2-2.
- Available RC group weight – The sum of all entity available weights in the RC group.

Table 2-4 shows an example of Weighted GTT Load Sharing applied to a load shared MAP or MRN group.

Table 2-4 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

Table 2-4 (Cont.) Load Shared Group with Weighted GTT Load Sharing Example

Entity	RC	Weight	RC Group Weight	In-Service Threshold	Required RC Group Weight	Entity Status
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 2-2.
- 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 2-5 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 2-5 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.

2.6 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.

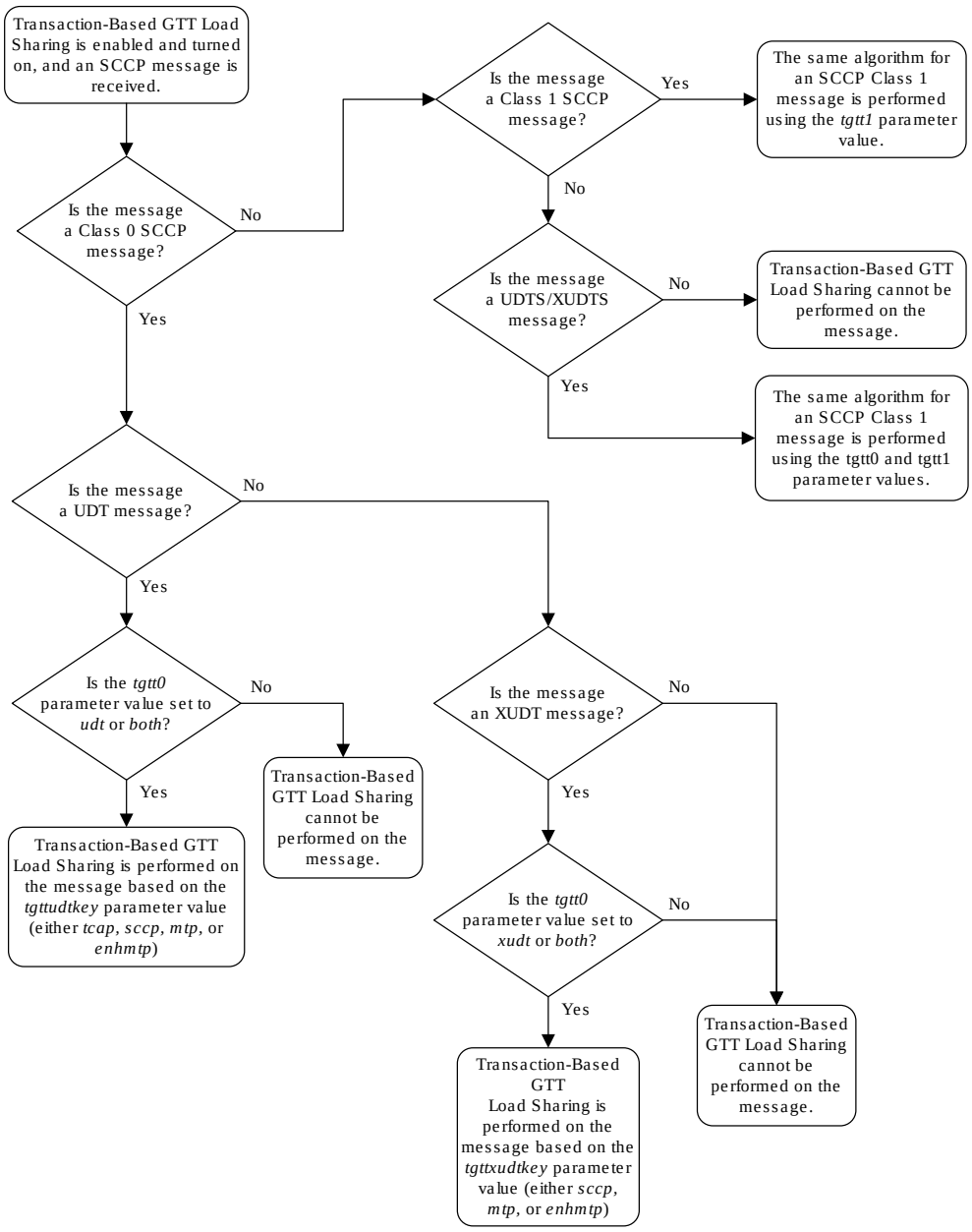
- MTP parameters - the first 3 bytes of the incoming OPC and 1 byte of the SLS.
- SCCP parameters - the last 4 bytes of the global title address field of the called party address.
- TCAP parameter - the TCAP Transaction ID in the messages.
- Enhanced MTP parameter - a combination of the SLS and the incoming 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 2-2 describes how the Transaction-Based GTT Load Sharing SCCP options are used.

Figure 2-2 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.

2.7 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).

For detailed information about this feature, refer to *vSTP SS7 Security User's Guide*.

2.8 M3UA Client Support

Note

- vSTP does not support full M3UA Client (ASP) functionality. M3UA Client configuration can only be used in specific scenarios for STP to STP links.
- vSTP as M3UA client does not support initiation of `ASP_DOWN` or any other ASPSM and ASPTM messages which are not mentioned in **Message Flow for ASP - M3UA Client** figure.
- vSTP as M3UA client does not support re-initiation of M3UA association by sending ASPUP on receiving `ASP_DOWN_ACK` from remote SG, though it updates the internal state to DOWN.
- As per specifications , DUNA(Destination Unavailable)/DAVA (Destination Available)/SCON (Signaling Congested) messages are initiated by SG in ASP-SG communication, but vSTP as M3UA client(ASP) still sends DUNA/DAVA/SCON messages to remote SG.
- vSTP as M3UA client should not be used as End points.

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:

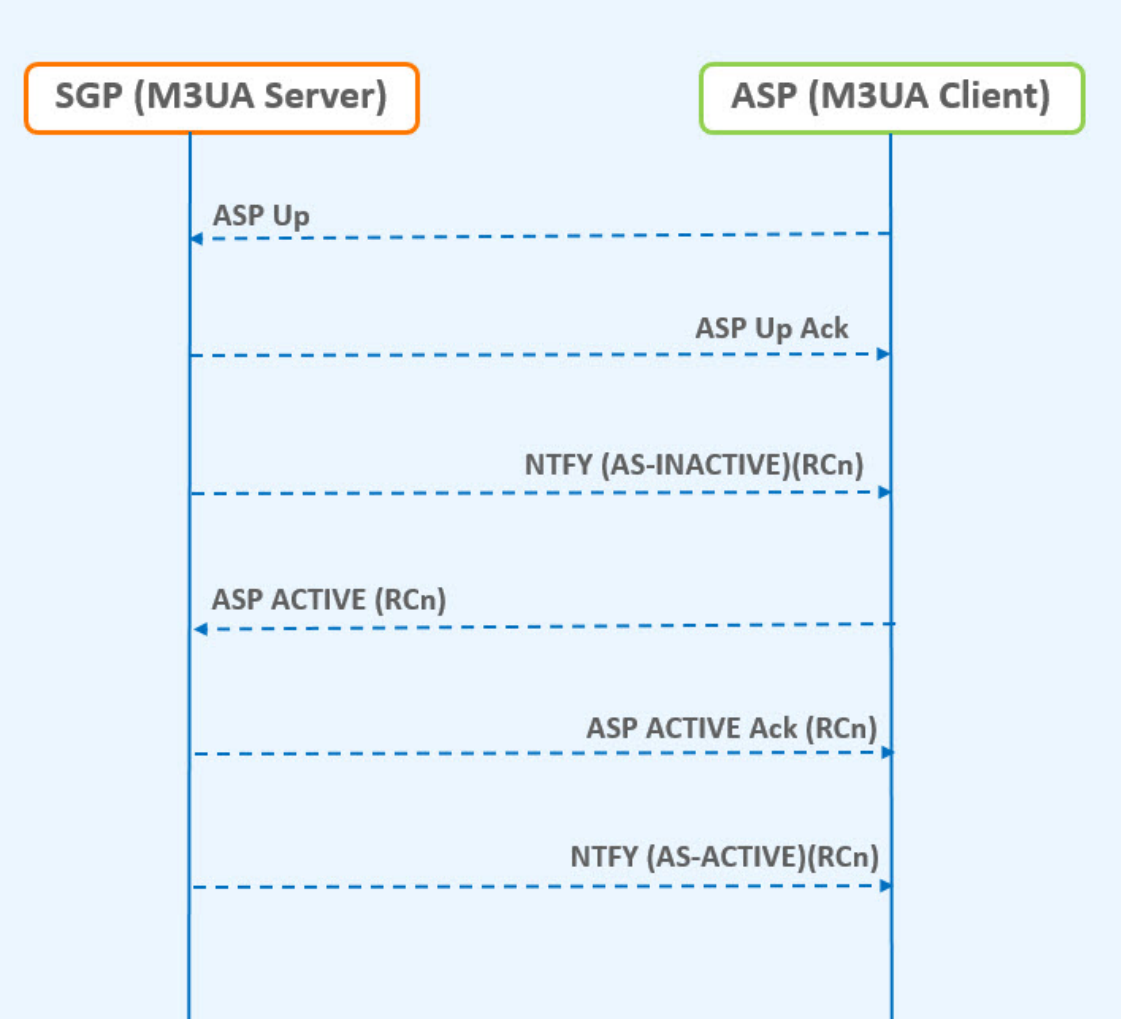
- Initiation of SCTP connection to send INIT message to the server.
- Initiation of ASP state maintenance messages such as, ASP-UP, ASP-Active etc.
- Receiving and processing of SS7 Signaling Network Management messages such as, DAVA, DUNA, DUPU, DRST, DAUD and SCON.
- Receiving and processing of M3UA 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 2-3 Message Flow for ASP - M3UA Client



2.8.1 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.

2.8.1.1 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 2-6 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.

2.8.1.2 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.

2.8.2 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.

2.8.3 Dependencies

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

2.9 Time Division Multiplexing

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

2.9.1 Feature Overview

The TDM support functionality includes the following components

- **TDM Hardware:** The hardware involves PCIe card with physical TDM connectivity supporting Virtual IO. This card contains built-in processor to process the MTP2 layer on hardware itself.
- **MTP Network Interworking Function (NIF):** §An additional (MTP Network Interworking Function - NIF) layer will be added to existing VSTP MP so that the MTP3 Layer can communicate with the MTP2 layer running on the TDM PCIe Card.
- **MTP2 Adapter:** §The MTP2 Adapter (NIF) layer on VSTP MP shall communicate with MTP2 layer using Virtual-IO calls.
- **Host machine:** §The Host machine shall allow PCI Pass-through Access to the vSTP MP virtual machines.

2.9.2 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

The TDM card supports either E1 or T1 mode at a time. The mode must be defined during driver configuration. It also supports, either HSL or LSL configuration at a time, and it needs to be defined during configuration.

> **Note**
>
> In case of ADAX card, the MTP2 Adapter layer uses the libraries and APIs provided by ADAX to communicate with ADAX HDC3 Card.

2.9.3 vSTP TDM Support Components

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

PCIe Card installed on Host Sever(s).

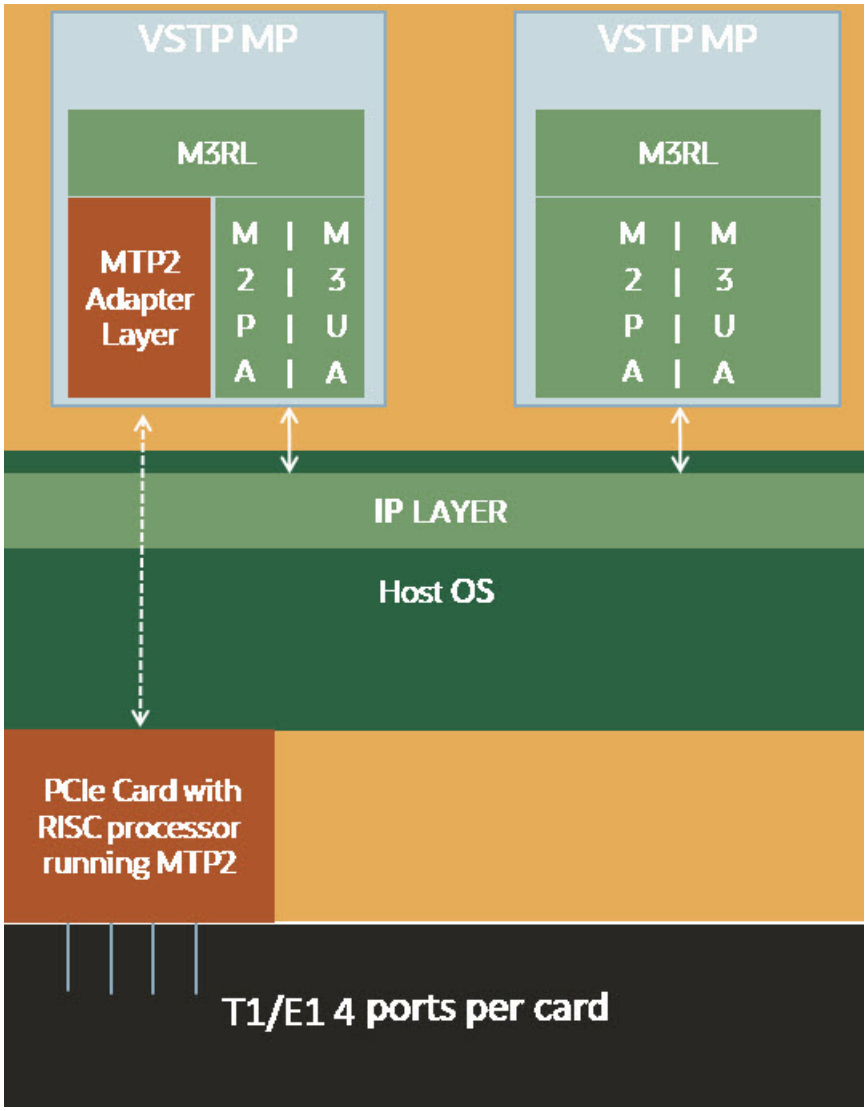
VSTP MP(s) supporting TDM are co-located with TDM card(s) on same host.

MTP2 Adapter layer on VSTP MP communicates with MTP2 Layer running on the PCIe 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 2-4 vSTP TDM Support Components



2.9.4 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.

2.9.4.1 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:

Table 2-7 TDM Interface Mapping (eLynx card)

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

Table 2-8 TDM Interface Mapping (ADAX card)

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

2.9.4.2 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.

2.9.4.3 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.

2.9.5 TDM Functionalities

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

2.9.5.1 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.

2.9.5.2 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.

2.9.5.3 MTP2 Link Congestion

MTP2 Link congestion is derived from the utilization of link transmission buffers maintained at MTP2 adaption layer and unacknowledged messages buffered at 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 2-9 Congestion Threshold Values

Congestion Level	Threshold Level	Onset Threshold	Clear Threshold
3	Critical	95	90
2	Major	85	80

Table 2-9 (Cont.) Congestion Threshold Values

Congestion Level	Threshold Level	Onset Threshold	Clear Threshold
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.

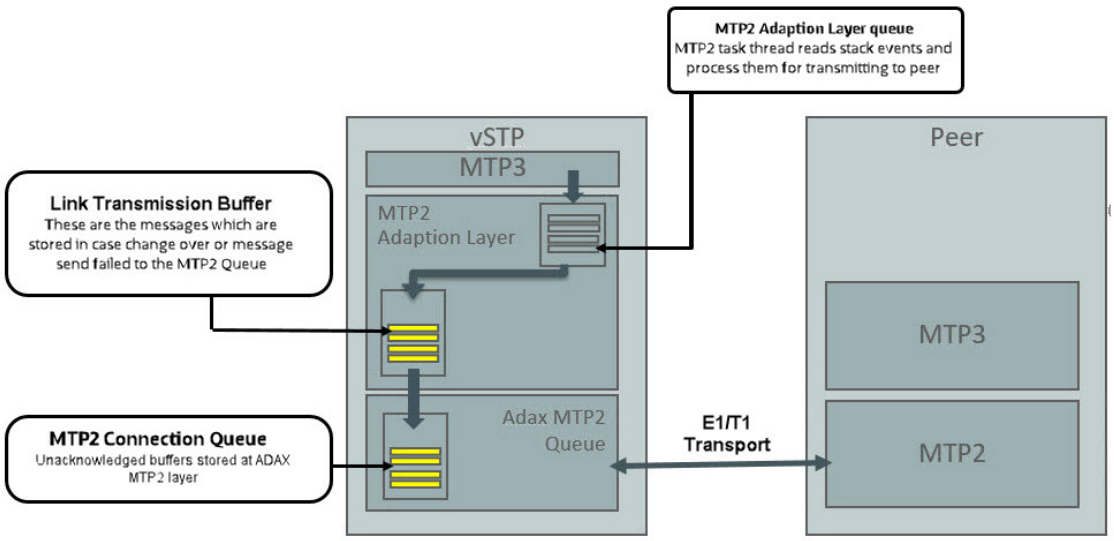
(Link TPS * 2) base is used for the base calculation of the congestion detection.

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 2-5 MTP2 Link Congestion Detection



2.9.5.4 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.

2.9.6 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.

2.9.6.1 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 2-10 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

MTP2 Interface Mapping (eLynx Card)

This MO configures the interface channel for eLynx Card. This channel is specified while configuring the MTP2 link.

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

```
{
            "boardType": "MTP2_BOARD_TYPE_ELYNX",
            "channelName": “elynx1",
            "ecm": "LINK_ECM_BASIC",
            "encodingScheme": "ENCODE_NONE",
            "framing": "FRAMING_SF",
            "hostName": “velynx-so1mp1",
            "linkTiming": "LINK_TIME_NONE",
```

```
            "linkType": "T1_hsl",
            "ll": 133,
            "minSuRate": 1000,
            "port": 4,
            "speed": "Hsl_1536k"
}
```

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

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

Example Output:

```
{
          "boardType": "MTP2_BOARD_TYPE_ELYNX",
            "channelName": “elynx1",
            "ecm": "LINK_ECM_BASIC",
            "encodingScheme": "ENCODE_NONE",
            "framing": "FRAMING_SF",
            "hostName": “velynx-so1mp1",
            "linkTiming": "LINK_TIME_NONE",
            "linkType": "T1_hsl",
            "ll": 133,
            "minSuRate": 1000,
            "port": 4,
            "speed": "Hsl_1536k"
}
```

MTP2 Interface Mapping (ADAX Card)

This MO configures the interface channel for ADAX Card. This channel is specified while configuring the MTP2 link.

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

```
{
    "boardType": "MTP2_BOARD_TYPE_ADAX",
    "channelName": "chan149",
    "hostName": “vadax-so1mp1",
    "linkType": "E1",
    "port": 3,
    "sequenceLength": "7_BIT ",
    "speed": "Lsl_64k",
    "timeSlot": 20
}
```

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

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

Example Output:

```
{
    "boardType": "MTP2_BOARD_TYPE_ADAX",
    "channelName": "chan149",
    "hostName": “vadax-so1mp1",
    "linkType": "E1",
    "port": 3,
    "sequenceLength": "7_BIT ",
    "speed": "Lsl_64k",
    "timeSlot": 20
}
```

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
}
```


2.9.6.2 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

Alarm/ Event ID	Name
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.

2.9.7 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

> **Note**
>
> The vSTP MP VM and the Adax HDC3 card must be co-located on same host machine.

2.9.8 Dependencies

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

Points to Consider

The following points must be considered while configuring eLynx Card:

- The eLynx card support only E1 traffic.
- eLynx is supported when installed in Oracle X8-2 and X8-2L servers.
- A maximum of 4 eLynx cards per server are supported.
- PCI slots 5 and 6 are not supported for eLynx on the Oracle X8-2L servers.
- Only 1 eLynx card per Message Processor (MP) is supported.
- The eLynx card is rated to process a maximum of 10K messages per second. If the ingress message rate crosses the 10K per second limit, the eLynx card may go into local congestion. This causes all the links on the eLynx card to go out of service until the congestion condition abates. Once the congestion condition is cleared, the eLynx card starts the link alignment process again.
  If the congestion condition persists for too long, the eLynx card can be impacted severely. some links may not recover automatically. If this happens, then the eLynx card needs to be reset or reloaded to recover.

The following points must be considered while configuring ADAX Card:

- After each upgrade ADAX Configurations has to be installed afresh.

- The J1 and ATM interfaces are not supported.
- Single ADAX HDC3 card cannot be accessed from Multiple VSTP MP VMs.
- The ADAX HDC3 driver and required components are not packaged with Standard DSR ISO. These components and RPMs have to be installed separately.

2.10 Scalability

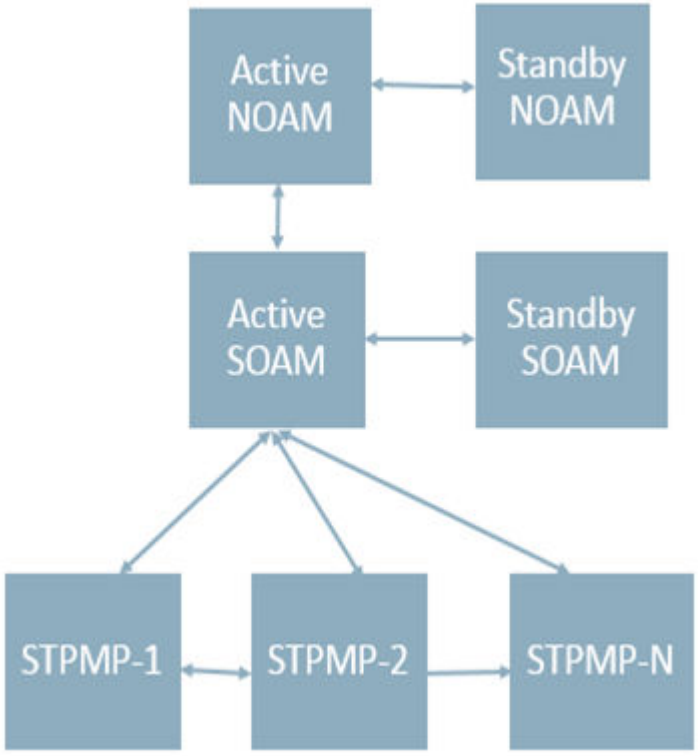
vSTP supports 10K MPS SS7 traffic capacity at the system level. This allows vSTP to support redundancy and diversity at the signaling interfaces. That is, more than one active STP-MP server can support signaling interfaces pointing toward the same remote signaling point.

Topology

vSTP supports two topologies.

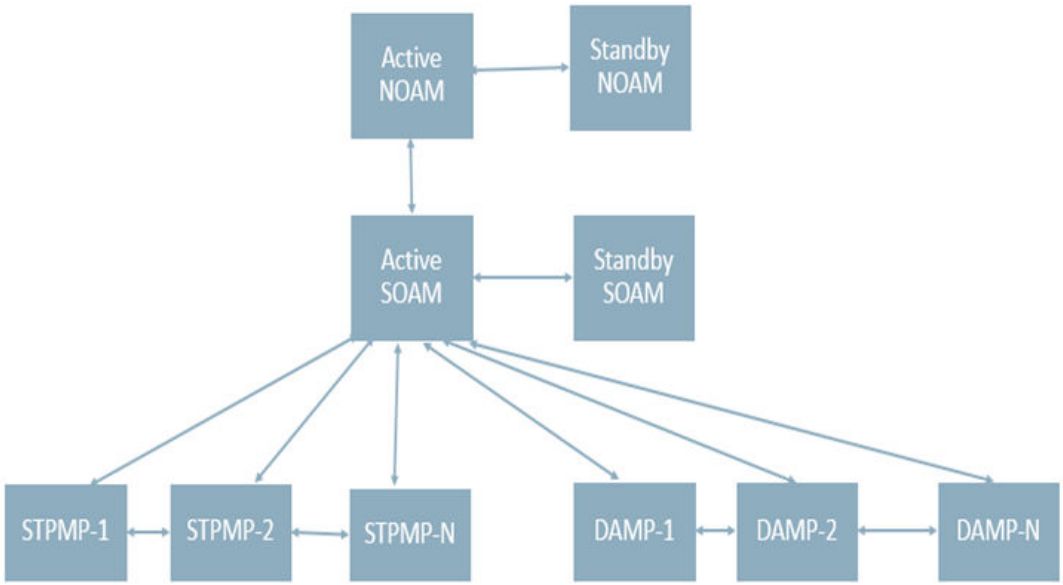
- **Only STP-MP servers in a site**

Figure 2-6 Only STP-MP Site



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

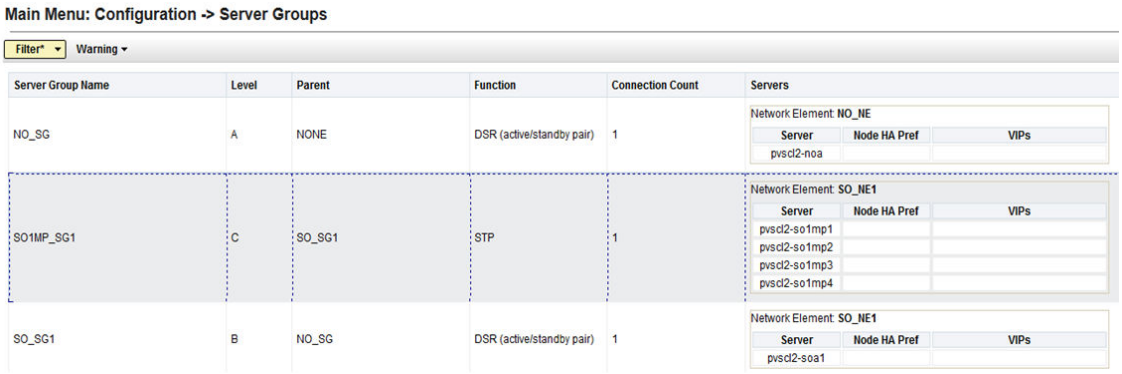
Figure 2-7 STP-MP and DA-MP in a Site



Server Group Configuration

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

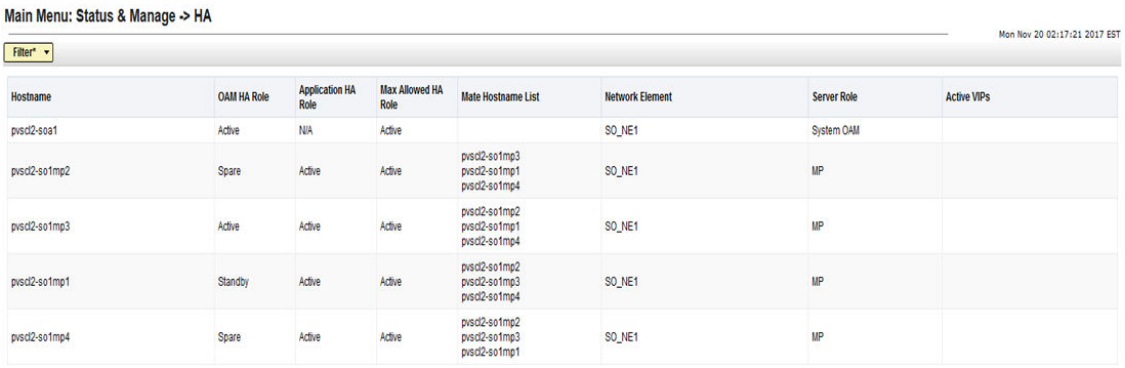
Figure 2-8 Multiple STP Servers in a Server Group



HA Status

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

Figure 2-9 HA Role for STP Servers



2.11 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.

2.12 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

2.12.1 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.

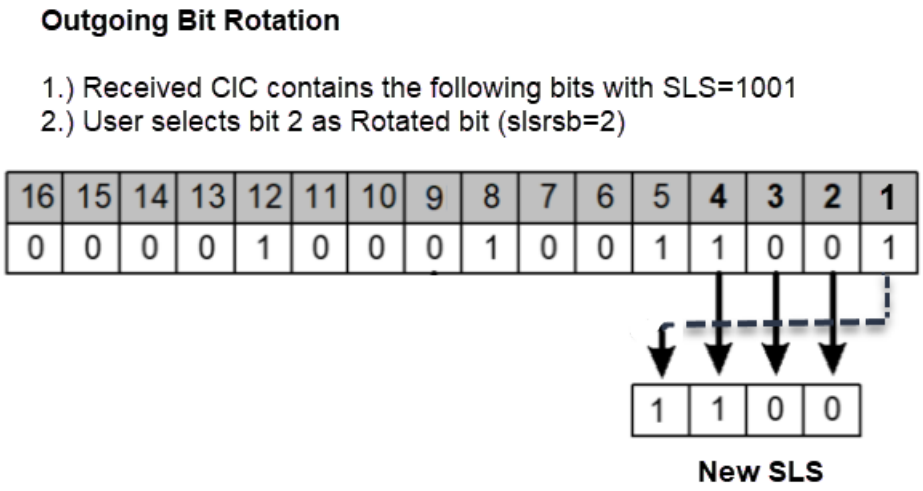
  For example, SLS = SLS = 0110 becomes Rotated SLS = 0011
- If bit position 1 is selected (`slsrsb` =**1**) for the outgoing linkset, then no rotation is performed since bit 1 is the existing LSB. Bit **1** is the default value.

  For example, SLS = 0110 remains 0110 only.

Outgoing Bit Rotation Example:

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

Figure 2-10 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.

2.12.2 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.

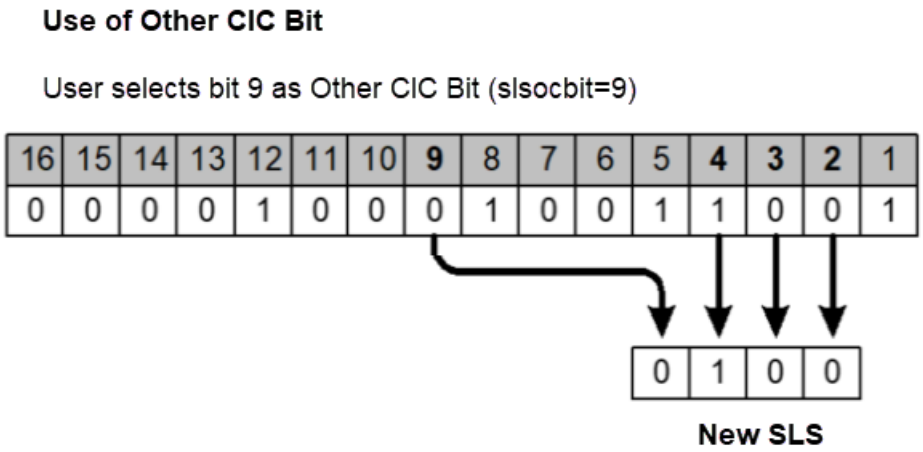
This option can be used as a solution to the problem of vSTP not sharing load between all links within a linkset. It is applicable to ITU ISUP messages.

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 2-11 Example: SLS Use of Other CIC Bit



2.12.3 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 2-11 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 2-12 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.

Table 2-12 (Cont.) Rules applied for Incoming Bit Rotation of ANSI

Rule	asls8	rsls8	islsbr	CNV	Incoming SLS Bits Rotation (islsbr)
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.
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

Incoming ANSI SLS	RSLS8 on incoming linkset	Chosen LSB	Rotated SLS	Applied Rule from Rules applied for Incoming Bit Rotation of ANSI
10010	true	8	**01**100101 **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

2.12.4 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 2-13 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 .

Table 2-13 (Cont.) Rules applied for Random SLS for ITU

System-wide randsls (in m3rloptions)	randsls on outgoing linkset	Random SLS
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 2-14 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.
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.

2.12.5 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.

2.12.6 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

2.12.6.1 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 2-12 ANSI 5-bit to ANSI 8-bit SLS Conversion

Calculation of ANSI 5-bit to ANSI 8-Conversion

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

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)

2.12.6.2 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.

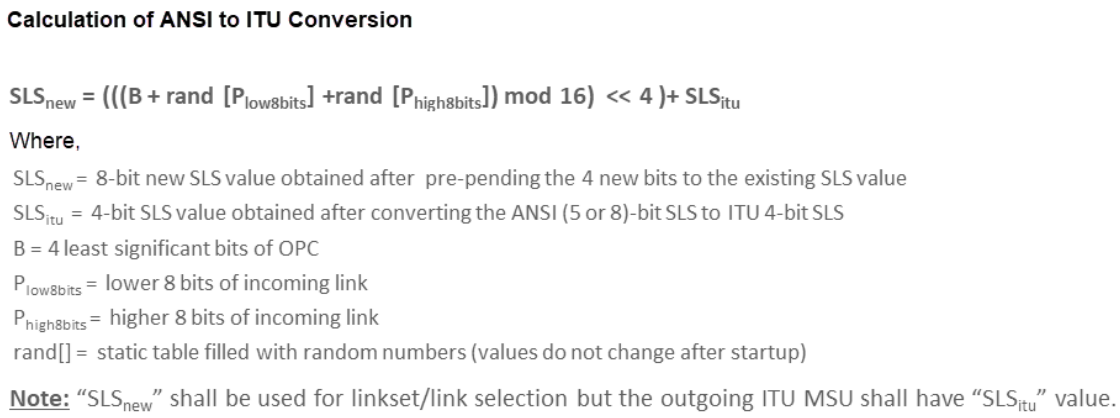
2.12.6.3 ANSI to ITU SLS Conversion

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 2-13 ANSI to ITU SLS Conversion



2.12.6.4 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 2-15 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
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

Table 2-15 (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	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 2-16 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

Table 2-16 (Cont.) 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
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.

2.12.7 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.

2.12.7.1 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 2-17 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
```

2.12.7.2 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.

2.12.7.3 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.

2.12.8 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.

2.12.9 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.

2.13 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

2.13.1 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.

2.13.1.1 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.

> **Note**
>
> vSTP discards the Reassembly procedure if the length of the first segmented MSU is lesser than the configured length. vSTP discards all segments irrespective of the value of the option `alwMsgDuringRsmblyErr` and generates XUDTS for the first segment in case the `return on Error` option is set in the message.

2.13.2 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.

2.13.3 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.

2.13.3.1 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 2-18 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
}
```

2.13.3.2 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.

2.13.3.3 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.

2.13.4 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.

2.13.5 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.

2.14 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/International or Spare destinations into groups. These groups are based on the country. When the user enters an ITU National/International 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.

2.14.1 ITU Point Code Support Functionality

When an ITU-N/ITU-I 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/ITU-I 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.

2.14.1.1 Operations for MTP3 and SCCP Management Messages

When vSTP receives a network management message concerning an ITU-National/ International 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/ International 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.

2.14.1.2 Interaction

ITU-National or Spare MSUs received on ITU-International linksets are assigned a group code of "aa".

ITU-International or spare MSUs received on ITU-National 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/ITU-I destination and group code can have it’s own ITU-N/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.

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

2.14.2 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.

2.14.2.1 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 2-19 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“
}
$ Cat lsp1.json
{ "ss7DomainType": "Itui",
"configurationLevel": "0",
"pcType": "Spc",
"mtpPointCode": "1-001-1",
"name": "lsp111s1",
"groupCode":"ab“
}
```

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
}

{
"data": [
{
"configurationLevel": "382",
"groupCode": “ab",
"mtpPointCode": "1-001-1",
"name": "lsp111s1",
"pcType": "Spc",
"ss7DomainType": "Itui"
```

```
},
],
"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"
}

$ Cat rsp1.json
{"configurationLevel": "0",
"name": "rsp111",
"ss7DomainType": "Itui",
"mtpPointCode": "5-001-1",
"enableBroadcastException": true,
"groupCode": "ab"
}
```

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
}

{
"data": [
{
"configurationLevel": "382",
"enableBroadcastException": true,
"groupCode": “ab",
"mtpPointCode": "5-001-1",
"name": "rsp111",
"nprst": "Off",
"rcause": "None",
"splitiam": "None",
"ss7DomainType": "Itui"
}
],
"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"
}

$ Cat na.json
{
"name": "Na5",
"na": 11,
"naType": "Itui",
```

```
"groupCode": "ad"
}
```

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
}

{
"data": [
{
"groupCode": "ad",
"na": 11,
"naType": "Itui",
"name": "Na5"
}
],
"links": {},
"messages": [],
"status": true
}
```

2.14.2.2 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.

2.14.2.3 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.

2.14.3 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.

2.14.4 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-International/ ITUN-Spare/ITUI-Spare Destinations.
- The ITU-National/International 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.
- If conversion between ITU-I and ITU-N or ANSI is used, then only one ITU-I group can send traffic to a specific ANSI or ITU-N node.

2.15 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.

For detailed information about this feature, refer to *vSTP SS7 Security User's Guide*.

2.16 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.

2.16.1 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.

2.16.2 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.

2.16.3 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.

2.16.3.1 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 2-20 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"
}
```


2.16.3.2 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.

2.16.3.3 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.

2.16.3.4 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.

2.16.4 Troubleshooting

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.

2.16.5 Dependencies

The AINPQ/INPQ functionality for vSTP has no dependency on any other vSTP operation.

2.17 Multiple Routes Support

vSTP provides support for multiple routes to a destination of ANSI/ITU-I/ITU-N/ITU-N24 domain and allows load sharing between 2 routes of same cost.

The Multiple Routes feature allows up to 6 routes to a single destination or exception route. However, load sharing is allowed between only 2 routes having same cost.

2.17.1 Feature Overview

A route is a path to a destination. For example, RSP.Routeset is a collection of routes to a destination. With multiple Routes support, vSTP allows up to 6 routes to be established to a single destination or exception route. However, it continues to allow load sharing between only 2 routes. The remaining routes are used for backup.

The Multiple Route support feature considerations:

- The feature allows vSTP to allow load sharing between only 2 routes with same Route Cost, where Route Cost is the cost assigned to a route.
- Only one route can be associated to a linkset to a single destination.
- vSTP can have multiple cost groups or individual cost route for a destination.
- With no network or link failures, routing starts on the normal cost routes. In case of link and network failures, routing switches to a higher cost routes or the route without any traffic loss.

Where, Normal Cost Route is the route with minimum route cost to a destination. and Higher Cost Routs is the route with the cost more than the minimum route cost to a destination.

vSTP provides four different options for route set:

1. Three Combined Routes
   Where, Combined Routing is having more than one routes with same cost to a destination (vSTP allows only two routes of same route cost).
2. Two combined routes and two individual routes with different costs
3. One combined route and four individual routes with different costs
4. Six individual routes with different cost

In case of combined routing the traffic will loadshare between two equal cost active routes.

Note

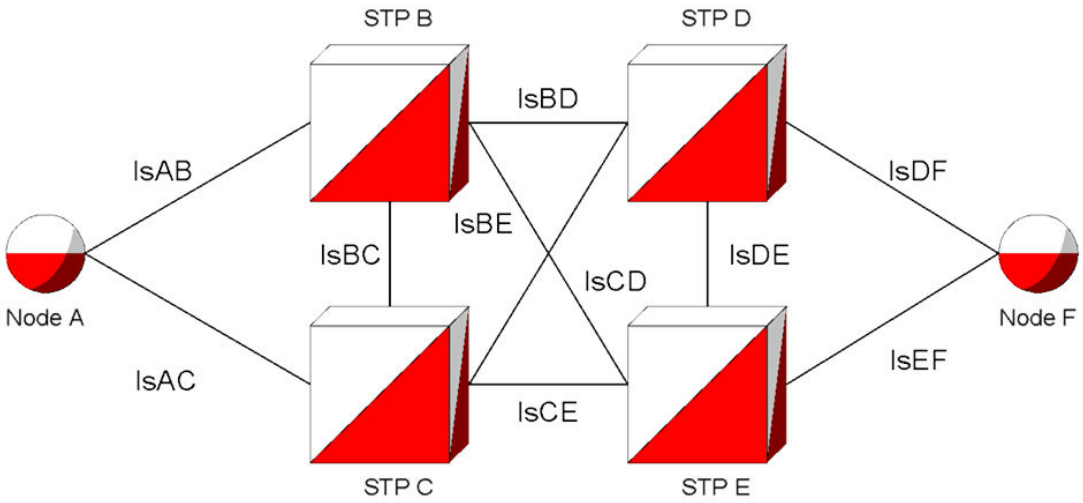
- vSTP broadcasts TFP messages, if all the routes to a destination goes down.
- Route to any destination will be restricted if associated linkset is restricted.
- vSTP broadcasts TFR, if higher cost route to a destination becomes restricted.
- vSTP broadcasts TFA, if any configured route to a destination becomes available.

2.17.1.1 Feature Description

The following example of Combined Linkset Networking describes the multiple routes support functionality:

Combined Linkset Networking

The following figure shows an example of combined linkset networking:



Node A has a route to **Node F** through a combined linkset where both `lsAB` and `lsAC` have the same relative cost for their respective routes, making up a cost group.

Thus, the following conditions holds true:

- The traffic sent from Node A over Linksets lsAB and lsAC will be distributed equally between both linksets.
- The status of the routeset of **Node A** for which the destination is **Node F**, follows the rules shown in the following table:

Table 2-21 Route set Status

lsAB Route Status	lsAC Route Status	RSP status	Linksets with Traffic
Allowed	Allowed	Allowed	lsAB & lsAC
Restricted	Allowed	Allowed	lsAC
Allowed	Restricted	Allowed	lsAB
Restricted	Restricted	Restricted	lsAB & lsAC
Allowed	Prohibited	Allowed	lsAB
Restricted	Prohibited	Restricted	lsAB
Prohibited	Restricted	Restricted	lsAC
Prohibited	Allowed	Allowed	lsAC
Prohibited	Prohibited	Prohibited	None

2.17.2 Feature Configuration

This section provides procedures to perform the configurations for Multiple Routes functionality.

Multiple Routes support 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.

2.17.2.1 MMI Managed Objects for Multiple Routes Support

MMI information associated with Multiple Routes 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 Multiple Routes support:

Table 2-22 Multiple Routes support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
routes	Insert, Update, Delete
remotesignalingpoints	Insert, Update, Delete

routes - Insert, Update, Delete

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

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

```
}
cat route
{
 "configurationLevel": "141",
 "linksetName": "test6",
 "name": "ROUTE7",
 "remoteSignalingPointName": "RSPITUI1201",
 "routeCost": 12
 }
```

Sample Output:

```
{
"data": [
{
"configurationLevel": "141",
"linksetName": "test6",
"name": "ROUTE7",
"remoteSignalingPointName": "RSPITUI1201",
"routeCost": 12
},
 ],
 "links": {},
 "messages": [],
 "status": true
}
```

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

```
/vstp/routes -v PUT -r /tmp/route
{
 "data": true,
 "links": {},
 "messages": [],
 "status": true
}
cat route
{
 "configurationLevel": "141",
 "linksetName": "test6",
 "name": "ROUTE7",
 "remoteSignalingPointName": "RSPITUI1201",
 "routeCost": 22
 }
```

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

```
/vstp/routes/<routename> -v DELETE
```

remotesignalingpoints - Display

Execute the following command on Active SOAM to display the status:

```
/vstp/remotesignalingpoints/RSP3/status
```

Sample Output:


```
{
    "data": [
        {
            "groupCode": "aa",
            "mpServerHostname": "MRA-so1mp1",
            "name": "RSP3",
            "operationalStatus": "Unavailable",
            "pointCode": "3-005-3",
            "routes": [
            {
                    "adjacentPC": "RSP6",
                    "linksetName": "LS6",
                    "routeAdjacentStatus": "Down",
                                          "routeCost": 45,
                     "routeName": "Route2_RSP6",
                    "routeRemoteStatus": "Available",
                    "routeStatus": "Unavailable"
            }
            ],
            "ss7DomainType": "Itui",
            "statusKnown": true,
            "timeOfLastUpdate": "2020-05-14T19:00:43-04:00"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```


2.17.2.2 GUI Configuration

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

Select **Routes** and configure the parameters.

For more details related to these parameters, see Routes.

2.17.2.3 Alarms and Measurements

There are no alarms, events, or measurements specific to the multiple routes support functionality. However, the existing vSTP alarms and measurements are pegged during the multiple routes operations.

2.17.3 Troubleshooting

While using the Multiple Routes Support functionality, if routes are not available for non-adjacent node, then check the route configuration.

2.17.4 Dependencies

The Multiple Routes Support functionality for vSTP has no dependency on any other vSTP operation.

The following points must be considers for multiple routes support:

- This feature does not support n-way load sharing.
- Only two routes can have same route cost.

2.18 Multiple Linksets Support

vSTP provides support for establishing multiple linksets to Adjacent Point Code (APC).

This functionality hepls operators to host more than one linksets to single node. It also enables provisioning of additional links between two nodes beyond the number of links permitted by the protocol. This feature does not require adjacent node to support multiple point codes using Multiple Point Code support.

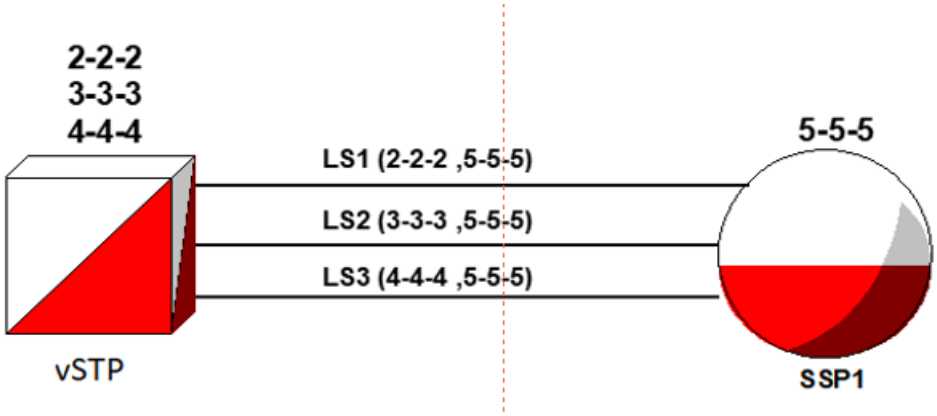
2.18.1 Feature Overview

The Multiple Linksets Support feature allows multiple linksets to be established between the vSTP and an adjacent node regardless of whether that node supports the multiple point code or not. The feature supports multiple Linksets to be established with single adjacent point code (APC). For more than one adjacent point code, the MLS feature requires vSTP to support the MPC feature.

Example:

The following figure illustrates a vSTP with 3 linksets assigned to the same APC, where each linkset uses a different TPC/SPC of the vSTP:

Figure 2-14 Multiple Linksets Support



2.18.1.1 Multiple Linksets Support Feature Description

The MLS feature allows up to 6 linksets to be created to a single APC. Only 2 routes can be assigned the same cost for loadsharing,

The MTP and GT routed traffic cannot be load shared beyond on all provisionable routes with the MLS feature.

2.18.1.2 Message Specific Handling

The following points describe the message handling with Multiple Linkset Support:

- **Signaling Link Test Messages (SLTM/SLTA)**
  vSTP validates that the OPC and DPC of the message matches with the RSP and LSP respectively provisioned in the Linkset on which message received.

  Even if DPC matches with any other provisioned TPC/SPC, the message is rejected.

  This check is enforced to detect provisioning errors which interferes with network management.
- **Transfer Prohibited/Restricted/Allowed Messages**
  On reception of TFx message, vSTP performs the concerned procedures for the point codes received in TFx message. For example, in Figure 2-14, if point code 5-5-5 sends a TFP message on LS1 to the vSTP concerning a point code X, then vSTP performs transfer prohibited procedures for SPC 2-2-2, DPC 5-5-5, and concerned point code “X”.

  vSTP does not initiate transfer prohibited procedure on LS2 and LS3 until, it receives a TFP for point code associated with these linksets.
- **Management Inhibit Messages (LIN/LIA/LUN/LUA/LID/LFU/LLT/LRT)**
  vSTP validates that the OPC and DPC of the message matches with the RSP and LSP respectively provisioned in the Linkset on which message received. Even if, the DPC matches with any other provisioned TPC/SPC, the message is rejected.
- **ChangeOver Messages (CBD/CBA/COO/COA/XCO/XCA/ECO/ECA)**
  vSTP validates that the OPC and DPC of the message matches with the RSP and LSP respectively provisioned in the Linkset on which message received. Even if, the DPC matches with any other provisioned TPC/SPC, the message is rejected.
- **Route Set Test Messages(RST/RSR)**
  vSTP validates that the OPC and DPC of the message matches with the RSP and LSP respectively provisioned in the Linkset on which message received. Even if, the DPC matches with any other provisioned TPC/SPC, the message is rejected.

2.18.2 Feature Configuration

This section provides procedures to perform the configurations for Multiple Linksets functionality.

Multiple Linksets support 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.

2.18.2.1 MMI Managed Objects for Multiple Linksets Support

MMI information associated with Multiple Linksets 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 Multiple Linksets support:

Table 2-23 Multiple Linksets support Managed Objects and Supported Operations

Managed Object Name	Supported Operations
linksets	Insert, Update, Delete
localsignalingpoints	Insert, Update, Delete
remotesignalingpoints	Insert, Update, Delete

linksets - Insert, Update, Delete

Consider the following points wjile configuring linksets objects:

- Ensure that LSP is provisioned in VstpLocalSP and RSP is provisioned in VstpRemoteSP Table.
- Ensure that the linkset maintains the unique key pair of LSP and RSP.
- Maximum 6 Linksets are allowed to be provisioned with same RSP.

Execute the following command to display the content:

```
mmiclient.py /vstp/linksets
```

Sample Output:


```
/vstp/linksets
       {
          "data": [
              {
            "asls8": false,
            "cgGtmod": false,
            "configurationLevel": "4162",
            "enableBroadcastException": false,
            "gttmode": "Fcd",
            "islsrsb": 1,
            "ituTransferRestricted": false,
            "l2TimerSetName": "Default",
            "l3TimerSetName": "Default",
            "linkTransactionsPerSecond": 100,
            "localSignalingPointName": "Itui_SPC6",
            "name": "MP1_Eagle_LS6",
            "randsls": "Off",
            "remoteSignalingPointName": "Eagle",
            "rsls8": false,
            "slsci": false,
            "slsrsb": 1,
            "type": "M2pa"
         }
           ],
           "links": {},
           "messages": [],
```

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

To insert data, create a file with following content:

```
$ cat linkset.txt
{
            "configurationLevel": "0",
            "enableBroadcastException": false,
            "gttmode": "Fcd",
            "ituTransferRestricted": false,
            "linkTransactionsPerSecond": 100,
            "localSignalingPointName": "Itui_SPC2",
            "name": "SO2_SO3_LS",
            "remoteSignalingPointName": "RspItui_TPC",
            "type": "M2pa"
      }
```

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

```
/vstp/linksets -v POST -r /<Absolute path>/linkset.txt
```

Sample Output:

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

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

```
/vstp/linksets/<linksetname> -v DELETE
```

2.18.2.2 GUI Configuration

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

Select the **Link Sets**, **Remote Signalling Point**, and **Local Signalling Point** options to configure the respective parameters.

For more details related to these parameters, see GUI Configurations.

2.18.2.3 Alarms and Measurements

There are no alarms, events, or measurements specific to the multiple linksets support functionality. However, the existing vSTP alarms and measurements are pegged during the multiple linksets operations.

2.18.3 Troubleshooting

In case, the links are not available for multiple linksets, verify whether the APC of linkset configured on remote node and LSP of linkset configured on vSTP node are same. Also, verify if the route is configured for the APC using same linkset on vSTP and remote node.

2.18.4 Dependencies

The Multiple Linksets Support functionality for vSTP has no dependency on any other vSTP operation.

The following points must be considers for multiple linksets support:

- This feature does not support n-way load sharing.
- Only two linksets can be configured as combined route.

2.19 Accounting Measurement Support

vSTP supports Accounting Measurement for different combinations to track the send/received MSUs on any linkset of vSTP. Users can enable any of the accounting measurement combinations as per their requirements. This feature allows users to perform the following:

- Generating CSV report for any combination for any given time period.
- To check pegging for any record or entry using the `pegstat -W` command on vSTP MP.

2.19.1 Feature Description

The Accounting Measurement feature allows users to keep track of MSUs sent or received on any linkset of vSTP for different combinations. These combinations are described in Accounting Measurement Combinations

2.19.1.1 Accounting Measurement Combinations

The Accounting Measurement combinations are described in the following table:

Table 2-24 Accounting Measurement Combination

Serial No	Measurement Description	Measurement Name	Measurement Sub	Group Peg Condition
1	Number of Rx messages per Linkset and OPC	VstpRxOpcLnksetMsu	Opc Linkset	Service Indicator >= 3
2	Number of Tx messages per Linkset and OPC	VstpTxOpcLnksetMsu	Opc Linkset	Service Indicator >= 3
3	Number of Rx msg octets per Linkset and OPC	VstpRxOpcLnksetMsuOctets	Opc Linkset	Service Indicator >= 3
4	Number of Tx msg octets per Linkset and OPC	VstpTxOpcLnksetMsuOctets	Opc Linkset	Service Indicator >= 3

Table 2-24 (Cont.) Accounting Measurement Combination

Serial No	Measurement Description	Measurement Name	Measurement Sub	Group Peg Condition
5	Number of Rx messages per Linkset and DPC	VstpRxDpcLnksetMsu	Dpc Linkset	Service Indicator >= 3
6	Number of Tx messages per Linkset and DPC	VstpTxDpcLnksetMsu	Dpc Linkset	Service Indicator >= 3
7	Number of Rx msg octets per Linkset and DPC	VstpRxDpcLnksetMsuOctets	Dpc Linkset	Service Indicator >= 3
8	Number of Tx msg octets per Linkset and DPC	VstpTxDpcLnksetMsuOctets	Dpc Linkset	Service Indicator >= 3
9	Number of Rx messages per OPC and DPC	VstpRxOpcDpcMsu	Opc Dpc	Service Indicator >= 3
10	Number of Tx messages per OPC and DPC	VstpTxOpcDpcMsu	Opc Dpc	Service Indicator >= 3
11	Number of Rx msg octets per OPC and DPC	VstpRxOpcDpcMsuOctets	Opc Dpc	Service Indicator >= 3
12	Number of Tx msg octets per OPC and DPC	VstpTxOpcDpcMsuOctets	Opc Dpc	Service Indicator >= 3
13	Number of Rx messages from OPC and SCCP Called party	VstpRxOpcSccpCdpa	Opc Sccp Called Party	GTA should be present in called party
14	Number of Tx messages from DPC and SCCP Called party	VstpTxDpcSccpCdpa	Dpc Sccp Called Party	GTA should be present in called party
15	Number of Rx messages from OPC and SCCP Calling party	VstpRxOpcSccpCgpa	Opc Sccp Calling Party	GTA should be present in called party
16	Number of Tx messages from DPC and SCCP Calling party	VstpTxDpcSccpCgpa	Dpc Sccp Calling Party	GTA should be present in called party
17	Number of Rx message per OPC, SI and NI	VstpRxOpcSiNiMsu	Opc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
18	Number of Tx message per OPC, SI and NI	VstpTxOpcSiNiMsu	Opc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.

Table 2-24 (Cont.) Accounting Measurement Combination

Serial No	Measurement Description	Measurement Name	Measurement Sub	Group Peg Condition
19	Number of Rx message octets per OPC, SI and NI	VstpRxOpcSiNiMsuOctets	Opc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
20	Number of Tx message octets per OPC, SI and NI	VstpTxOpcSiNiMsuOctets	Opc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
21	Number of Rx message per DPC, SI and NI	VstpRxDpcSiNiMsu	Dpc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
22	Number of Tx message per DPC, SI and NI	VstpTxDpcSiNiMsu	Dpc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
23	Number of Rx message octets per DPC, SI and NI	VstpRxDpcSiNiMsuOctets	Dpc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
24	Number of Tx message octets per DPC, SI and NI	VstpTxDpcSiNiMsuOctets	Dpc SI NI	For all valid value of Service Indicator. For valid value of Network Indicator.
25	Number of Rx message per LS and SI	VstpRxLinksetSI	Linkset SI	For all valid value of Service Indicator.
26	Number of Tx message per LS and SI	VstpTxLinksetSI	Linkset SI	For all valid value of Service Indicator.
27	Number of Rx message octets per SI and LS	VstpRxLinksetSIOctets	Linkset SI	For all valid value of Service Indicator.
28	Number of Tx message octets per SI and LS	VstpTxLinksetSIOctets	Linkset SI	For all valid value of Service Indicator.
29	Number of Rx message per DPC, OPC and NI	VstpRxOpcDpcNi	Opc Dpc Ni	For valid value of Network Indicator.
30	Number of Tx message per DPC, OPC and NI	VstpTxOpcDpcNi	Opc Dpc Ni	For valid value of Network Indicator.
31	Number of Rx message octets per DPC, OPC and NI	VstpRxOpcDpcNiOctets	Opc Dpc Ni	For valid value of Network Indicator.

Table 2-24 (Cont.) Accounting Measurement Combination

Serial No	Measurement Description	Measurement Name	Measurement Sub	Group Peg Condition
32	Number of Tx message octets per DPC, OPC and NI	VstpTxOpcDpcNiOctets	Opc Dpc Ni	For valid value of Network Indicator.
33	Number of times particular GTT rule is executed for given linkset	VstpRxGTTRulePerLinkset	GTTRule Linkset	GTT Rule should be applied successfully.
34	Number of msu octets used in msg that particular GTT rule is executed for given linkset	VstpRxGTTRulePerLinksetOctets	GTTRule Linkset	GTT Rule should be applied successfully.
35	Number of GTTs performed, result is a DPC of an interconnecting network.	VstpTxGTTPerfDpc	GTT on Interconnect	
36	Number of GTTs performed on messages received from an inter-connecting network, no translation table for the translation type.	VstpRxGTTNoTranslationTableTT	GTT on Interconnect	
37	Number of GTTs performed on messages received from an inter-connecting network	VstpRxGTTPerfLinkSet	GTT on Interconnect	
38	Number of GTTs unable to perform on messages received from an inter-connecting network, no translation for this address.	VstpRxGTTFailNoTranslation	GTT on Interconnect	

All the combinations given in above table have the VSTP Accounting Measurement group: The VSTP Accounting Measurement Report will contain different measurement sub-reports for different combinations. All the measurements in Accounting Measurement feature will be arrayed.

2.19.2 Feature Configuration

This section provides procedures to perform the configurations for Accounting Measurement functionality.

Accounting Measurement support 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.

2.19.2.1 MMI Managed Objects for Accounting Measurement Support

MMI information associated with Accounting Measurement 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 Accounting Measurement support:

Table 2-25 Accounting Measurement support Managed Objects and Supported Operations

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

1)Accounting Measurement feature for any particular combination will be enabled only if combination specific field in VstpAccMeasOptions MO will be set as Yes.

accountingmeasurementoptions - Insert, Update, Delete

> **Note**
>
> - The Accounting Measurement feature for any combination is enabled only if value of the **AccountingMeasurementFeature** field in VstpAccMeasOptions MO is set as **Yes**.
> - The Accounting Measurement feature for any combination is enabled only the value of the combination specific field in VstpAccMeasOptions MO is set as **Yes**.

Execute the following command to display the content:

```
/vstp/accountingmeasurementoptions
```

Sample Output:

```
{
"data": [
{
"accountingMeasFeature": "No",
"dpcCdpaAccMeasOption": "No",
"dpcCgpaAccMeasOption": "No",
"dpcLinksetAccMeasOption": "No",
"dpcSiNiAccMeasOption": "No",
"gttOnInterConnectingNw": "No",
"linksetSiAccMeasOption": "No",
"opcCdpaAccMeasOption": "No",
```

```
"opcCgpaAccMeasOption": "No",
"opcDpcAccMeasOption": "No",
"opcDpcNiAccMeasOption": "No",
"opcLinksetAccMeasOption": "No",
"opcSiNiAccMeasOption": "No"
}
],
"links": {},
"messages": [],
"status": true
}
```


To update data, create a file with following content:


```
{
"accountingMeasFeature": "Yes",
"dpcCdpaAccMeasOption": "Yes",
"dpcCgpaAccMeasOption": "Yes",
"dpcLinksetAccMeasOption": "No",
"dpcSiNiAccMeasOption": "No",
"gttOnInterConnectingNw": "No",
"linksetSiAccMeasOption": "Yes",
"opcCdpaAccMeasOption": "No",
"opcCgpaAccMeasOption": "Yes",
"opcDpcAccMeasOption": "No",
"opcDpcNiAccMeasOption": "No",
"opcLinksetAccMeasOption": "No",
"opcSiNiAccMeasOption": "Yes"
}
```


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

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

Sample Output:


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


linksets - Insert, Update, Delete

> **Note**
>
> Accounting Measurement feature for any linkset is enabled only if the **linksetAccMeasOption** in linksets MO is set as **Yes**.

Execute the following command to display the content:

```
/vstp/linksets
```

Sample Output:

```
"data": [
{
"cgGtmod": false,
"configurationLevel": "135",
"enableBroadcastException": false,
"gttmode": "Fcd",
"ituTransferRestricted": false,
"linkTransactionsPerSecond": 100,
"localSignalingPointName": "LSP1“,
"name": "Linkset1",
"remoteSignalingPointName": "RSP1",
“linksetAccMeasOption”: “On”,
"type": "M2pa"
}
],
"links": {},
"messages": [],
"status": true
}
```

To update data, create a file with following content:

```
{
"cgGtmod": false,
"configurationLevel": "135",
"enableBroadcastException": false,
"gttmode": "Fcd",
"ituTransferRestricted": false,
"linkTransactionsPerSecond": 100,
"localSignalingPointName": "LSP1",
"name": "Linkset1",
"remoteSignalingPointName": "RSP1",
“linksetAccMeasOption”: “On”,
"type": "M2pa"
}
```

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

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

Sample Output:

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

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

2.19.2.2 Alarms and Measurements

There are no alarms or events specific to the Accounting Measurement functionality. However, the existing vSTP alarms are generated during the Accounting Measurement operations.

Measurements

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

Measurement ID	Measurement Name
22070	VstpRxLnksetOpcMsu
22071	VstpTxLnksetOpcMsu
22072	VstpRxLnksetOpcMsuOctets
22073	VstpTxLnksetOpcMsuOctets
22074	VstpRxLnksetDpcMsu
22075	VstpTxLnksetDpcMsu
22076	VstpRxLnksetDpcMsuOctets
22077	VstpTxLnksetDpcMsuOctets
22078	VstpRxOpcDpcMsu
22079	VstpTxOpcDpcMsu
22080	VstpRxOpcDpcMsuOctets
22081	VstpTxOpcDpcMsuOctets
22082	VstpRxOpcSccpCdpa
22083	VstpTxDpcSccpCdpa
22084	VstpRxOpcSccpCgpa
22085	VstpTxDpcSccpCgpa
22086	VstpRxOpcSiNiMsu
22087	VstpTxOpcSiNiMsu
22088	VstpRxOpcSiNiMsuOctets
22089	VstpTxOpcSiNiMsuOctets
22090	VstpRxDpcSiNiMsu
22091	VstpTxDpcSiNiMsu
22092	VstpRxDpcSiNiMsuOctets
22093	VstpTxDpcSiNiMsuOctets
22094	VstpRxLinksetSI
22095	VstpTxLinksetSI
22096	VstpRxLinksetSIOctets
22097	VstpTxLinksetSIOctets
22098	VstpRxOpcDpcNi
22099	VstpTxOpcDpcNi
22100	VstpRxOpcDpcNiOctets
22101	VstpTxOpcDpcNiOctets
22102	VstpRxGTTRulePerLinkset
22103	VstpRxGTTRulePerLinksetOctets

Measurement ID	Measurement Name
22104	VstpTxGTTPerfDpc
22105	VstpRxGTTNoTranslationTableTT
22106	VstpRxGTTPerfLinkSet
22107	VstpRxGTTFailNoTranslation

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

2.19.3 Troubleshooting

The troubleshooting steps for Accounting Measurement feature are:

- If pegs are missed for any combination, verify that the **linksetAccMeasOption** field in Linkset MO is set as **On** for incoming linkset (for all Rx related combinations) and outgoing linkset (for all Tx related combinations).
- If records are not getting added, check if the number of records in the report has reached the limit 100000.

> **Note**
>
> Only 100000 records can be added in one report.

2.19.4 Dependencies

The Accounting Measurement functionality for vSTP has no dependency on any other vSTP operation.

The following points must be considers for accounting measurement support:

- Whenever a new entry or record is created for any combination of Accounting Measurement feature, initially some of the MSUs corresponding to that entry may get missed in pegging.
- This feature does not support deletion of entries or records.

2.20 vSTP Reserved and Maximum link TPS

vSTP enables you to set the Reserved (Resv) and Maximum (Max) link Transaction Per Second (TPS).

- **Reserved link TPS**: The minimum reserved bandwidth in TPS for a link.
- **Maximum link TPS**: The maximum limit for the TPS used by the link, if the TPS is available on MP.

This feature overcomes the limitation of single link TPS parameter that limits the capacity of all links, assuming all of them have maximum traffic at the same time.

The sum of all Reserved link TPS for all links configured on MP can not pass Max MP capacity, but sum of MAX TPS for all links configured on MP can be more than MAX MP capacity.

2.20.1 Feature Description

The following points describes the work flow of the Resv and Max link TPS:

- The Resv Link TPS is the reserved bandwidth of specific link and it is the guaranteed bandwidth for each Link in a Linkset.
- The sum of the Reserved TPS values for all the links does not exceed the MP capacity.
- The Max Link TPS is the maximum TPS that can be utilized by Link if bandwidth is available on the MP.
- The Max link TPS value must be greater than the Resv link TPS. And the value is smaller than 10 K TPS for a link.
- The Resv link TPS and Max link TPS cannot have same values.
- A link is never allowed to exceed the Max link TPS to avoid the risk of entering congestion.
- The Max Link TPS is the maximum limit of a link. However, it is not always true.
- Traffic up to Reserved TPS is expected. It may go up to Max link TPS based on the available bandwidth. However, it is not always true.
- Any unused MP capacity available, is shared among all the remaining links.
- For MTP2 , Resv link TPS value and Max link TPS parameter value must be same.
- vSTP enforces TPS distribution up to Resv link TPS value for the in-service links.
- An MP is never allowed to exceed the Max MP TPS to avoid risk of entering congestion

2.20.2 Feature Configurations

This section provides procedures to perform the vSTP Resv and Max Link TPS functionality.

The Resv and Max Link TPS 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.

2.20.2.1 MMI Managed Objects for Resv and Max Link TPS Support

MMI information associated with Resv and Max Link TPS 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 Resv and Max Link TPS support:

Managed Object Name	Supported Actions
linksets	Insert, Update, Delete

linksets - Insert, Update, Delete

Execute the following command to display the content::

```
/vstp/linksets
```

Sample Output:

```
/vstp/linksets
       {
        "asls8": false,
        "cgGtmod": false,
        "cgpnblSet": "None",
        "configurationLevel": "3404",
        "enableBroadcastException": false,
        "gnameset": "SetA",
        "gttmode": "Sysdflt",
        "islsrsb": 1,
        "ituTransferRestricted": false,
        "l2TimerSetName": "Default",
        "l3TimerSetName": "Default",
        "linksetAccMeasOption": "No",
        "localSignalingPointName": "LspAnsi_TPC1",
        "maximumLinkTransactionsPerSecond": 9000,
        "name": "LSANSIM2PA",
        "randsls": "Off",
        "remoteSignalingPointName": "RspAnsi_TPC",
        "reservedLinkTransactionsPerSecond": 4500,
        "rsls8": false,
        "securityLogging": "Off",
        "slsci": false,
        "smsProxy": "Off",
        "type": "M2pa"
},
```

2.20.2.2 GUI Configurations for Resv and Max Link TPS Support

The Resv and Max Link TPS functionality can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

The following parameters on the **Link Sets** option page are used to perform the configurations:

- `Reserved Link Transactions Per Second`
- `Maximum Link Transactions Per Second`

For more information, see GUI Configuration in *Oracle Communications vSTP User's Guide*.

2.20.2.3 Resv and Max Link TPS Alarms and Measurements

Alarms and Events

The following table lists the alarms or events specific to the Resv and Max Link TPS functionality for vSTP:

Event ID	Event Name
70357	Ingress max Mp MSU TPS Crossed
70358	Egress max Mp MSU TPS Crossed

For more details related to measurements, refer to *Diameter Signaling Router Alarms and KPIs Reference*.

Measurements

The following table lists the measurements specific to the Resv and Max Link TPS functionality for vSTP:

Measurement ID	Measurement Name
21586	VstpRxMpMSU
21589	VstpTxMpMSU

For more details related to measurements, refer to *Diameter Signaling Router Measurement Reference*.

2.20.3 Troubleshooting

In case of the error scenarios, the measurements specific to Resv and Max Link TPS feature are pegged. For information related to Resv and Max Link TPS measurements, see Resv and Max Link TPS Alarms and Measurements.

2.20.4 Dependencies

The Resv and Max Link TPS feature for vSTP has no dependency on any other vSTP operation.

> **Note**
>
> In general scenarios, the configured max link TPS value should be double of the RESV Link TPS value. Achieving the Max Link TPS depends on the cloud infrastructure, such as CPU availability traffic latency or buffer memory.

2.21 Support for CAP/INAP Parameter Filtering

vSTP supports the GTT translations based on CDPN, BCD CDPN, and SK+BCSM with the CAP/INAP filtering feature . It provides the following Opcodes to support CAP/INAP filtering:

- Initial DP
- IDPSMS
- IDPGPRS

2.21.1 Feature Description

The CAP/INAP based filtering enables vSTP to route INAP based opcode messages based on their CAP components.

vSTP uses the `SKBCSM` and `MSISDN` GTT set types to achieve this functionality. The `SKBCSM` set type remains linked with the `OPCODE` set type or any of the existing `MBR` set types, such as `IMSI` or `MSISDN`.

The CAP/INAP based filtering is supported only for the following TCAP package types:

- BEGIN
- CONTINUE
- END

Therefore, the OPTSN (Optional Set Name) with one of the MBR set types are allowed to be provisioned only for TOBR GTA entries that have PKGTYPE as BEGIN, CONTINUE, or END.

The INAP/CAP messages are identified using unique the ACN.

When an INAP MSU is processed by the TOBR GTT translation with the OPTSN as SKBCSM or MSISDN, vSTP decodes the CAP portion, extracts the CDPN, BCD CDPN digits, or SKBCSM digits from the MSU and use as a key to search the translation from the GTA table.

2.21.1.1 CDPN and BCD CDPN Based Filtering

For CDPN or BCD CDPN based filtering, the GTT set type must be set as MSISDN and it must be linked with the OPTSN of an INAP based OPCODE/MBR set type GTA entry.

Once the MSU is processed, filtering is done for CDPAGTA followed by the filtering for OPCODE, and then if OPTSN is set as MSISDN and the message contains CDPN or BCD CDPN portion, digits are decoded and are looked up in Global Title Addresses table, where message is translated and sent to the configured Point Code (RSP).

If MSU contains both CDPN and BCD CDPN portion, then BCD CDPN gets more priority and translation takes place only for those digits. The MSISDN decoding is supported for the following INAP messages:

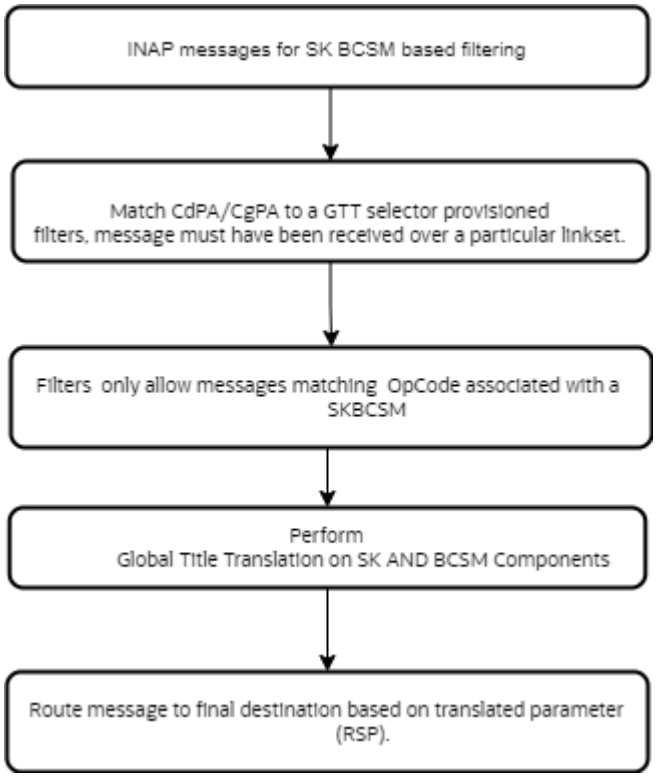
- IDP
- IDPSMS
- IDPGPRS

> **Note**
>
> In case of an MSU that contains both CDPN and BCD CDPN portion, translation is performed only on BCD CDPN digits. If BCD CDPN is not present in GTA table, translation gets failed irrespective of the availability of the CDPN digits translation entry in the table.

Call Flow

The following diagram shows a call flow for OPCODE MSISDN based filtering:

Figure 2-15 Call Flow for Opcode-Msisdn Based Filtering



2.21.1.2 SK+BCSM Based Filtering

vSTP supports the SK+BCSM based filtering. The GTT set type is set as SKBCSM and it is linked with the OPTSN of an INAP based OPCODE/MBR set type GTA entry.

Once the MSU is processed, filtering is done for CDPAGTA followed by the filtering for OPCODE, and then if OPTSN is set as SKBCSM and the message contains SK and BCSM portion, digits are decoded and are looked up in Global Title Addresses table, where message is translated and sent to the configured Point Code (RSP).

For allowing any SK+BCSM entry, '*' can be used as an wildcard entry for both SK and BCSM.

The SK+BCSM decoding is supported for the following INAP messages:

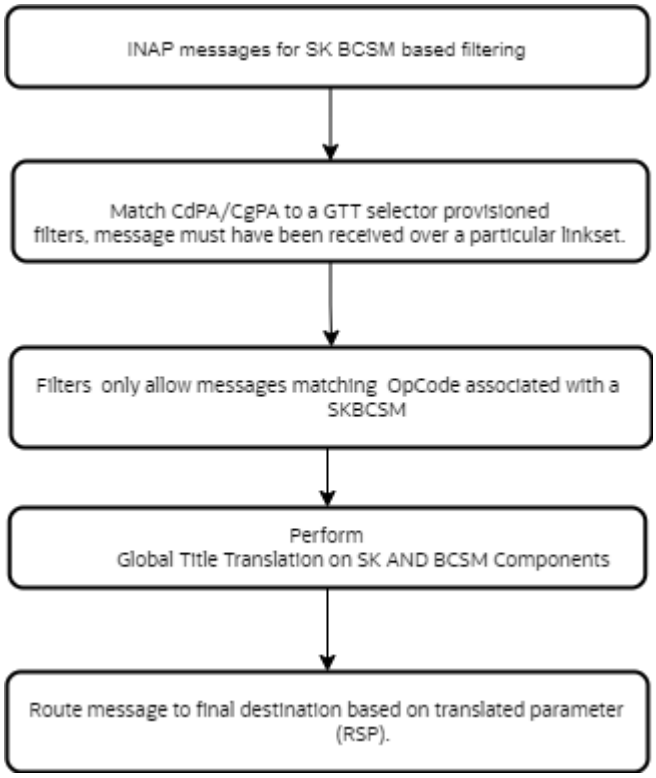
- IDP
- IDPSMS
- IDPGPRS

where, SK is Service Key component and BCSM for IDP, IDPSMS, and IDPGPRS are eventTypeBCSM, EventTypeSMS, and GPRSEventType components respectively.

Call Flow

The following diagram shows a call flow for SK BCSM based filtering:

Figure 2-16 Call Flow for SK BCSM Based Filtering



2.21.2 Feature Configurations

This section provides procedures to perform the CAP/INAP based filtering functionality.

The CAP/INAP based filtering 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.

2.21.2.1 GUI Configurations for CAP/INAP Based Filtering

The CAP/INAP Based Filtering can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

- The following parameter on the **GTT Sets** page are used to perform the configurations:
  - `Gtt Set Type`
- The following parameter on the **Global Title Addresses** page are used to perform the configurations:
  - SK
  - `BCSM`

For more information, see GUI Configuration in *Oracle Communications vSTP User's Guide*.

2.21.2.2 MMI Managed Objects for CAP/INAP Filtering

MMI information associated with vSTP generated CAP/INAP Filtering can be configured 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 CAP/INAP Filtering:

Managed Object Name	Supported Actions
GTT Sets	GET, PUT, POST, DELETE
Global Title Addresses	GET, PUT, POST, DELETE

gttsets - Insert

To insert:

Create a file with following content to set value for the `gttSetType` parameter. File name could be anything, for example option name can be used as filename:

```
{
            "domain": “Itu",
            "gttSetType": “Skbcsm",
            "name": "set1"
      }
```

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

```
/vstp/gttsets –v POST –r <filename>.json
```

Execute the following command to display the content:

```
vstp/gttsets
{
            "configurationLevel": "1",
            "domain": “Itu",
            "gttSetType": “Skbcsm",
            "name": "set1"
}
```

globaltitleaddresses - Insert

To insert:

Create a file with following content to set value for the `bcsm` and `sk` parameter. File name could be anything, for example option name can be used as filename:

```
{
            "bcsm": "ab“,
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "fallback": "Sysdflt",
            "gttSetName": "skbcsm",
            "routingIndicator": “Gt",
            "rspName": "rsp1",
            "sk": "04c1b1“,
```

```
            "translateIndicator": "Dpc“
        }
```

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

```
/vstp/globaltitleaddresses –v POST –r <filename>.json
```

Execute the following command to display the content:

```
vstp/globaltitleaddresses
{
            "bcsm": "ab“,
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "configurationLevel": "402",
            "fallback": "Sysdflt",
            "gttSetName": "skbcsm",
            "routingIndicator": “Gt",
            "rspName": "rsp1",
            "sk": "04c1b1“,
            "translateIndicator": "Dpc",
            "uniqueIdentifier": "e9f9edc0-1018-4169-a181-564ff616b4be"
        }
```

2.21.2.3 CAP/INAP Filtering Alarms and Measurements

There are no alarms, events, and measurements specific to the CAP/INAP Filtering functionality in vSTP.

2.21.3 Troubleshooting

In case of the error scenarios, the vSTP measurements are pegged. For information related to UDTS Routing measurements, see Measurement Reference document..

2.21.4 Dependencies

The CAP/INAP Filtering functionality for vSTP has no dependency on any other vSTP operation.

2.22 vSTP Generated UDTS Routing

A UDTS service message is an SCCP connectionless message. It is utilized when a UNITDATA (UDT) message is undeliverable and the message originator has requested a delivery report. A UDTS message is only sent if the option field in the received UDT was set to return an error.

vSTP supports the routing of vSTP generated UDTS messages, based on Originating Point Code (OPC) of the incoming SCCP request or message. This provides an additional capability to the existing vSTP functionality wherein UDTS response messages generated by vSTP can be routed to originator, based on OPC of incoming UDT Message.

2.22.1 Feature Configurations

This section provides procedures to perform the vSTP generated UDTS Routing functionality.

The UDTS Routing 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.

2.22.1.1 GUI Configurations for UDTS Routing Support

The UDTS Routing functionality can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

The following parameter on the **SCCP Options** page are used to perform the configurations:

- `Send UDTS on Opc`

For more information, see GUI Configuration in *Oracle Communications vSTP User's Guide*.

2.22.1.2 MMI Managed Objects for UDTS Routing Support

MMI information associated with vSTP generated UDTS Routing 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 UDTS Routing support:

Managed Object Name	Supported Actions
sccpoptions	Update

sccpoptions - Update

To update:

Create a file with following content to set value for the `sendVstpgenUdtsOnOpc` parameter. File name could be anything, for example option name can be used as filename:

```
{
"sendVstpgenUdtsOnOpc": "On"
}
```

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

```
/vstp/sccpoptions –v PUT –r sccp.json
```

Execute the following command to display the content:

```
vstp/sccpoptions
{
        "allowedFirstSegLen": 0,
        "alwMsgDuringRsmblyErr": false,
```

```
    "class1seq": "Disabled",
    "dfltfallback": false,
    "dfltgttmode": "Cd",
    "isSegXUDTfeatureEnable": false,
    "mtprgtt": "Off",
    "mtprgttfallback": "Mtproute",
    "reassemblyTimerDurationAnsi": 5000,
    "reassemblyTimerDurationItu": 10000,
    "segmentedMSULength": 200,
    "sendVstpgenUdtsOnOpc": "Off",
    "smsDelivery": "Off",
    "smsOrigination": "Off",
    "smsTermination": "Off",
    "tcapErrorDiscard": "Off",
    "tgtt0": "None",
    "tgtt1": "None",
    "tgttudtkey": "Mtp",
    "tgttxudtkey": "Mtp",
    "travelVelocity": 700
}
```


2.22.1.3 UDTS Routing Alarms and Measurements

Alarms and Events

There are no alarms and events specific to the UDTS Routing functionality in vSTP.

Measurements

The following table lists the measurements specific to the UDTS Routing functionality for vSTP:

Measurement ID	Measurement Name
	VstpGenUdtsOnOpcTx

For more details related to measurements, refer to *Diameter Signaling Router Measurement Reference*.

2.22.2 Troubleshooting

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

2.22.3 Dependencies

The UDTS Routing feature for vSTP has no dependency on any other vSTP operation.

Consider the following points while using the UDTS Routing:

- The feature is applicable only for route on GT (CdPA) UDTS messages only.
- The feature is applicable only for vSTP generated UDTS messages.
- The feature is applicable when routing or GTT translation fails to route on GT (CdPA) vSTP Generated UDTS messages.

2.23 vSTP XUDT UDT Conversion Feature

In the network world, certain nodes package messages in XUDT format to facilitate segmentation of long SCCP messages into multiple parts, even if the data is not segmented and there are no further messages in the sequence. When these XUDT messages passes from another networks the receiving network may not be able to support the XUDT format. Therefore the XUDT(S) messages are required to be converted to UDT(S) messages.

vSTP supports the conversion of XUDT (S) messages to UDT (S) format and vice versa for both MTP3 and SCCP routed SCCP messages.

The feature allows the conversion of the following messages:

- A UDT(S) message to an XUDT(S) message
- An XUDT(S) message to a UDT(S) message

The XUDT(S) to UDT(S) conversion and vice versa is applicable to segmented and non-segmented UDT(S) and XUDT(S) messages. It is supported for messages destined for both ITU and ANSI domains. The feature is applied to both MTP3 routed SCCP messages and SCCP routed SCCP messages. q XUDT<->UDT Conversion feature shall be applied to SCMG Messages too.

2.23.1 UDT(S) to XUDT(S) Conversion

When converting a UDT(S) message to an XUDT(S) message, the changes shown in the following table are made to the message:

Table 2-26 Parameter Values after UDT to XUDT or UDTS to XUDTS Conversion

UDT to XUDT Conversion		**UDTS to XUDTS Conversion**	
Parameter	**Value after UDT to XUDT Conversion**	**Parameter**	**Value after UDTS to XUDTS Conversion**
Message Type	XUDT (0x11)	Message Type	XUDTS (0x12)
Protocol Class	Same as the pre-converted message.	Return Cause	Same as the pre-converted message.
Hop Counter	15, which is the maximum value.	Hop Counter	15, which is the maximum value.
Pointer to Called Party Address (CDPA)	Incremented from the pre-converted UDT message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Called Party Address (CDPA)	Incremented from the pre-converted UDTS message value by the size of the Pointer to Optional Parameters value (1 byte).
Pointer to Calling Party Address (CGPA)	Incremented from the pre-converted UDT message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Calling Party Address (CGPA)	Incremented from the pre-converted UDTS message value by the size of the Pointer to Optional Parameters value (1 byte).

Table 2-26 (Cont.) Parameter Values after UDT to XUDT or UDTS to XUDTS Conversion

UDT to XUDT Conversion		UDTS to XUDTS Conversion	
Parameter	**Value after UDT to XUDT Conversion**	**Parameter**	**Value after UDTS to XUDTS Conversion**
Pointer to Data	Incremented from the pre-converted UDT message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Data	Incremented from the pre-converted UDTS message value by the size of the Pointer to Optional Parameters value (1 byte).
Pointer to Optional Parameters	0, since no optional parameters are present in a converted XUDT message.	Pointer to Optional Parameters	0, since no optional parameters are present in a converted XUDTS message.
Called Party Address (CDPA) Parameter	Same as the pre-converted message.	Called Party Address (CDPA) Parameter	Same as the pre-converted message.
Calling Party Address (CGPA) Parameter	Same as the pre-converted message.	Calling Party Address (CGPA) Parameter	Same as the pre-converted message.
Data	Same as the pre-converted message.	Data	Same as the pre-converted message.

2.23.2 XUDT(S) to UDT(S) conversion

When converting an XUDT(S) message to a UDT(S) message, the changes shown in the following table are made to the message:

XUDT to UDT Conversion		XUDTS to UDTS Conversion	
Parameter	**Value after XUDT to UDT Conversion**	**Parameter**	**Value after XUDTS to UDTS Conversion**
Message Type	UDT (0x09)	Message Type	UDTS (0x0a)
Protocol Class	Same as the pre-converted message.	Return Cause	Same as the pre-converted message.
Hop Counter	Dropped from the converted message.	Hop Counter	Dropped from the converted message.
Pointer to Called Party Address (CDPA)	Decremented from the pre-converted (XUDT) message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Called Party Address (CDPA)	Decremented from the pre-converted (XUDTS) message value by the size of the Pointer to Optional Parameters value (1 byte).
Pointer to Calling Party Address (CGPA)	Decremented from the pre-converted (XUDT) message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Calling Party Address (CGPA)	Decremented from the pre-converted (XUDTS) message value by the size of the Pointer to Optional Parameters value (1 byte).

XUDT to UDT Conversion		XUDTS to UDTS Conversion	
Parameter	**Value after XUDT to UDT Conversion**	**Parameter**	**Value after XUDTS to UDTS Conversion**
Pointer to Data	Decremented from the pre-converted (XUDT) message value by the size of the Pointer to Optional Parameters value (1 byte).	Pointer to Data	Decremented from the pre-converted (XUDTS) message value by the size of the Pointer to Optional Parameters value (1 byte).
Pointer to Optional Parameters	Dropped from the converted message.	Pointer to Optional Parameters	Dropped from the converted message.
Called Party Address (CDPA) Parameter	Same as the pre-converted message.	Called Party Address (CDPA) Parameter	Same as the pre-converted message.
Calling Party Address (CGPA) Parameter	Same as the pre-converted message.	Calling Party Address (CGPA) Parameter	Same as the pre-converted message.
Data	Same as the pre-converted message.	Data	Same as the pre-converted message.
Segmentation – applies only to a segmented ANSI/ITU XUDT message.	Dropped from the converted message.	Segmentation – applies to a segmented ANSI/ITU XUDTS message.	Dropped from the converted message.
Importance – applies only to an ITU XUDT message.	Dropped from the converted message.	Importance – applies only to an ITU XUDTS message.	Dropped from the converted message.
INS – applies only to an ANSI XUDT message.	Dropped from the converted message.	INS – applies only to an ANSI XUDTS message.	Dropped from the converted message.
MTI – applies only to an ANSI XUDT message.	Dropped from the converted message.	MTI – applies only to an ANSI XUDTS message.	Dropped from the converted message.
End of Optional Parameters	Dropped from the converted message.	End of Optional Parameters	Dropped from the converted message.

2.23.3 Feature Configurations

This section provides procedures to perform the XUDT UDT Conversion functionality.

The XUDT UDT Conversion 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.

2.23.3.1 GUI Configurations for XUDT UDT Conversion

The XUDT UDT Conversion can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

- The following parameter on the **Remote Signaling Point** page used to perform the configurations:
  - `SCCP Message Conversion`: Indicates the type of conversion allowed for respective remote Signaling Point.
- The following parameter on the **GTT Set** page are used to perform the configurations:
  - `Allow Segmented XUDT`: The parameter decides if the segmented XUDT message for TOBR processing must be allowed or not.

For more information, see GUI Configurations.

2.23.3.2 MMI Managed Objects for XUDT UDT Conversion

MMI information associated with vSTP generated XUDT UDT Conversion can be configured 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 XUDT UDT Conversion:

Managed Object Name	Supported Actions
GTT Sets	GET, PUT, POST, DELETE
Remote Signaling Points	GET, PUT, POST, DELETE

gttsets

The `alwsegxudt` parameter in gttsets of type OPCODE indicates if TOBR processing must be allowed on Segmented XUDT(S) message or not. The parameter supports the following values:

- **NO**: Specifies that no segmented XUDT message for TOBR processing must be allowed.
- **YES**: Allows segmented XUDT message for TOBR processing.

> **Note**
>
> - The `alwsegxudt` parameter is configurable only when GTTSET type is **OPCODE**.
> - The XUDT only decodes messages with maximum of two byte TCAP lengths. Therefore, TOBR is not applicable on Segmented XUDT messages if the TCAP message length takes more than 2 bytes.
> - The ANSI TCAP segmented messages are not supported, although there are no restriction on the provisioning of SXUDT parameter in with ANSI opcode GTTSet type.
> - This is applicable for first segment only.

POST

Create a file with following content to set value for the `alwsegxudt` parameter. File name could be anything, for example option name can be used as filename:

```
{
            "alwsegxudt": "No",
            "checkmulcomp": "No",
            "domain": "Itu",
            "gttSetType": "Opcode",
            "name": "test1"
        }
```

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

```
/vstp/gttsets –v POST –r <filename>.json
```

Execute the following command to display the content:

```
vstp/gttsets
{
            "configurationLevel": "1",
            "domain": “Itu",
            "gttSetType": “Skbcsm",
            "name": "set1"
}
```

Sample Output:

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

GET

Execute the following command to display the content:

```
/vstp/gttsets
```

Sample Output:

```
{
    "data": [
        {
            "alwsegxudt": "No",
            "checkmulcomp": "No",
            "domain": "Itu",
            "gttSetType": "Opcode",
            "name": "test1"
        }
],
    "links": {},
    "messages": [],
    "status": true
}
```

remotesignalingpoints

The `udtxudtcnv` parameter remotesignalingpoints MO indicates the type of conversion allowed for respective Remote Signaling Point (RSP). The parameter supports the following values:

- **NOCONV**: Specifies that no conversion must be performed for the destination.

- **UDTTOXUDT**: Specifies that UDT(S) messages must be converted to XUDT(S) messages.
- **XUDTTOUDT**: Specifies the following:
  - Non-Segmented XUDT(S) messages must be converted to UDT(S) messages.
  - Segmented XUDT(S) messages must not be converted to UDT(S) messages.
- **SXUDTTOUDT**: Specifies that both Segmented XUDT(S) and non-segmented XUDT messages must be converted to UDT(S) messages.

POST

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

```
{
            "enableBroadcastException": true,
            "mtpPointCode": “1-2-1",
            "name": "RSP1",
            "nprst": "Off",
            "rcause": "None",
            "udtxudtcnv": "SXUDTTOUDT",
            "splitiam": "None",
            "ss7DomainType": "Ansi“
}
```

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

```
/vstp/remotesignalingpoints –v POST –r <filename>.json
```

Sample Output:

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

GET

Execute the following command to display the content:

```
/vstp/remotesignalingpoints
```

Sample Output:

```
{
    "data": [
        {
            "configurationLevel": "5",
            "enableBroadcastException": true,
            "mtpPointCode": "001-002-001",
            "name": "RSP1",
```

```
            "nprst": "Off",
            "rcause": "None",
            "udtxudtcnv": "SXUDTTOUDT",
            "splitiam": "None",
            "ss7DomainType": "Ansi"
        }
 ],
    "links": {},
    "messages": [],
    "status": true
}
```


2.23.3.3 XUDT UDT Conversion Alarms and Measurements

Alarms/Events

The following table lists the event specific to the XUDT UDT Conversion functionality for vSTP:

Table 2-27 Alarms/Events

Alarm/Event ID	Name
70291	vstpXudtUdtConversionFailed

For more details related to alarms and events, refer to *DSR Alarms and KPI Guide*.

Measuremet

The following table lists the measurements specific to the XUDT UDT Conversion functionality for vSTP:

Table 2-28 Measurements

Measurements ID	Measurements Name
22302	VstpM3rlXudtRx
22304	VstpXudtUdtSucc
22303	VstpM3rlUdtRx
22305	VstpUdtXudtSucc

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

2.23.4 Troubleshooting

In case of the error scenarios, the vSTP measurements are pegged. For information related to XUDT UDT Conversion measurements, see XUDT UDT Conversion Alarms and Measurements.

2.23.5 Dependencies

The XUDT UDT Conversion functionality for vSTP has no dependency on any other vSTP operation.

The following points must be considered for XUDT UDT Conversion:

- While performing the XUDT(S) to UDT(S) conversion, the `Segmentation` parameter (if present in XUDT(S) messages) is not encoded in the converted UDT(S) messages.
- While performing UDT(S) to XUDT(S) conversion, if the SCCP portion of the pre converted message is longer than 270 bytes in length and conversion results in the addition of the `Hop Counter` (1 byte) and `Pointer to Optional Parameters` (1 byte) fields causing the size of the SCCP portion to increase beyond a length of 272 bytes, then segmentation is performed.

2.24 Support for M2PA Busy Link

vSTP supports the M2PA busy link functionality based on the local received window accumulation size.

This functionality provides the capability to send busy links over M2PA link to the peer nodes when SCTP receives the window accumulation size that exceeds predefined thresholds depending upon Reserved TPS, MAXTPS , T7 value, and current receive window size. The functionality also allows to enable SCTP bundling per connection at vSTP.

The Link busy start threshold is calculated considering t7 timer value and receive queue size.

2.24.1 Feature Configurations

This section provides procedures to perform the M2PA Busy Link functionality.

The M2PA Busy Link 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.

2.24.1.1 MMI Managed Objects for M2PA Busy Link

MMI information associated with vSTP generated M2PA Busy Link can be configured 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 M2PA Busy Link functionality:

Managed Object Name	Supported Actions
m3rloptions	GET, PUT, POST, DELETE
connectionconfigurationsets	GET, PUT, POST, DELETE

m3rloptions

The `m2paSctpRxBusyLink` parameter in m3rloptions indicates if the M2PA busy link feature must be enabled or not. The parameter supports the following values:

- **On**: Specifies that the feature is enabled.
- **Off**: Specifies that the feature is not enabled.

POST

Create a file with following content to set value for the `m2paSctpRxBusyLink` parameter. File name could be anything, for example option name can be used as filename:

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

```
/vstp/m3rloptions –v POST –r <filename>.json
```

Execute the following command to display the content:

```
{
        "cnvAInat": 1,
        "cnvCgda": false,
        "cnvCgdi": false,
        "cnvCgdn": false,
        "cnvCgdn24": false,
        "cnvClgItu": "Off",
        "gtCnvDflt": false,
        "islsbrEnabled": false,
        "m2paSctpRxbusyLink": "Off",
        "performanceMeasurement": "Off",
        "randsls": "Off",
        "slsRotation": true,
        "slscnv": "Off",
        "slsocbEnabled": false,
        "slsreplace": false,
        "sparePCSupportEnabled": true
    },
```

Sample Output:

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

GET

Execute the following command to display the content:

```
/vstp/m3rloptions
```

Sample Output:

```
{
    "data": {
        "cnvAInat": 1,
        "cnvCgda": false,
        "cnvCgdi": false,
        "cnvCgdn": false,
        "cnvCgdn24": false,
        "cnvClgItu": "Off",
        "gtCnvDflt": false,
        "islsbrEnabled": false,
        "m2paSctpRxbusyLink": "On",
```

```
        "performanceMeasurement": "Off”,
        "randsls": "Off",
        "slsRotation": true,
        "slscnv": "Off",
        "slsocbEnabled": false,
        "slsreplace": false,
        "sparePCSupportEnabled": true
    },
    "links": {
        "update": {
            "action": "PUT",
            "description": "Update this item.",
            "href": "/mmi/dsr/v4.3/vstp/m3rloptions/",
            "type": "status"
        }
    },
    "messages": [],
    "status": true
}
```

connectionconfigurationsets

The `sctpBundlingEnabled` parameter in connectionconfigurationsets MO enables or disables the SCTP bundling. The parameter supports the following values: Yes/No

POST

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

```
{
            "name": "ConnCfgSet1",
            "sctpBundlingEnabled": "Yes",
            "sctpFragmentationEnabled": true,
            "sctpHeartbeatInterval": 1000,
            "sctpMaximumBurst": 4,
            "sctpMaximumSegmentSize": 0,
            "sctpNumberInboundStreams": 2,
            "sctpNumberOutboundStreams": 2,
            "sctpOrderedDelivery": true,
            "sctpRetransmissionAssociationFailure": 10,
            "sctpRetransmissionInitFailure": 8,
            "sctpRetransmissionInitTimeout": 120,
            "sctpRetransmissionMaximumTimeout": 800,
            "sctpRetransmissionMaximumTimeoutInit": 120,
            "sctpRetransmissionMinimumTimeout": 120,
            "sctpRetransmissionPathFailure": 5,
            "sctpSackDelay": 60,
            "sctpSocketReceiveSize": 1000000,
            "sctpSocketSendSize": 1000000
        }
```

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

```
/vstp/connectionconfigurationsets/ -v POST -r <filename>.json
```

Sample Output:

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

GET

Execute the following command to display the content:

```
/vstp/connectionconfigurationsets
```

Sample Output:

```
{
    "data": [
        {
            "configurationLevel": "204",
            "name": "ConnCfgSet1",
            "sctpBundlingEnabled": "Yes",
            "sctpFragmentationEnabled": true,
            "sctpHeartbeatInterval": 1000,
            "sctpMaximumBurst": 4,
            "sctpMaximumSegmentSize": 0,
            "sctpNumberInboundStreams": 2,
            "sctpNumberOutboundStreams": 2,
            "sctpOrderedDelivery": true,
            "sctpRetransmissionAssociationFailure": 10,
            “sctpRetransmissionInitFailure": 8,
            "sctpRetransmissionInitTimeout": 120,
            "sctpRetransmissionMaximumTimeout": 800,
            "sctpRetransmissionMaximumTimeoutInit": 120,
            "sctpRetransmissionMinimumTimeout": 120,
            "sctpRetransmissionPathFailure": 5,
            "sctpSackDelay": 60,
            "sctpSocketReceiveSize": 1000000,
            "sctpSocketSendSize": 1000000
        },
 ],
    "links": {},
    "messages": [],
    "status": true
}
```

2.24.1.2 GUI Configurations for M2PA Busy Link

The M2PA Busy Link can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

- The following parameter on the **Connection Configuration Sets** page used to perform the configurations:

  - `SCTP Bundling Enabled`: This parameter is used for enabling or disabling SCTP Bundling.
- The following parameter on the **M3rl Options** page are used to perform the configurations:
  - `M2PA Rx Busy Link`: This parameter is used for enabling/disabling M2PA Busy Link Indication on SCTP Feature.

For more information, see GUI Configurations.

2.24.1.3 M2PA Busy Link Alarms and Measurements

Alarms/Events

The following table lists the event specific to the M2PA Busy Link functionality for vSTP:

Table 2-29 Alarms/Events

Alarm/Event ID	Name
70201	linkOpStateChanged

For more details related to alarms and events, refer to *DSR Alarms and KPI Guide*.

Measuremet

The following table lists the measurements specific to the M2PA Busy Link functionality for vSTP:

Table 2-30 Measurements

Measurements ID	Measurements Name
21180	VstpRxSctpChunk
21176	VstpRxOccupanyAvg
21177	VstpRxOccupanyPeak

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

2.24.2 Troubleshooting

In case of the error scenarios, the vSTP measurements are pegged. For information related to M2PA Busy Link measurements, see M2PA Busy Link Alarms and Measurements.

2.24.3 Dependencies

The M2PA Busy Link functionality for vSTP has no dependency on any other vSTP operation.

2.25 Support for TPDA Based Filtering of MOFSM Message

vSTP supports the GTT translation based on SMS-Submit TP – Destination Address (TPDA) parameter available in the MAP portion of the MO_FSM messages. The feature provides the capability to accept or reject MO_FSM messages on the basis of TPDA present in the MAP portion of the message during GTT translation.

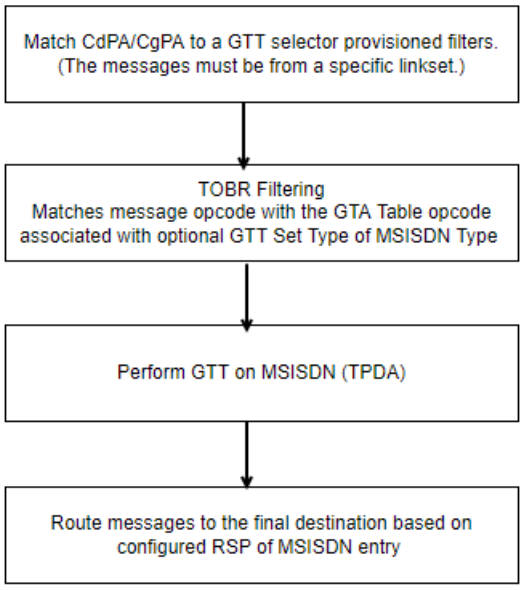
The TPDA parameter is configured as **Start Map Address** or **End Map Address** with MSISDN MBR GTT Set Type in the GTA table. The feature supports the **TP-MTI** as both **SMS-Submit** and **SMS-Command** for filtering.

> **Note**
>
> MO_FSM packets with Map Versions 1, 2, and 3 are supported for TPDA filtering.

Call Flow for Opcode-Msisdn (TPDA)

The following diagram shows a call flow for TPDA based filtering for MOSMS messages:

Figure 2-17 Call Flow of TPDA Based Filtering



2.25.1 Feature Configurations

This section provides procedures to perform the TPDA Based Filtering functionality.

The TPDA Based Filtering 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.

2.25.1.1 MMI Managed Objects for TPDA Based Filtering

MMI information associated with vSTP generated TPDA Based Filtering can be configured 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 TPDA Based Filtering functionality:

Managed Object Name	Supported Actions
gttsets	GET, PUT, POST, DELETE
globaltitleaddresses	GET, PUT, POST, DELETE

gttsets

The `gttSetType` parameter for TPDA must be set to MSISDN.

GET

Execute the following command to display the content:

```
/vstp/gttsets
```

Sample Output:

```
{
            "domain": “Itu",
            "gttSetType": “Msisdn",
            "name": "set1"
      }
```

globaltitleaddresses

The `emapaddr` and `smapaddr` parameters in globaltitleaddresses MO configures the a GTA with GTT Set having “Msisdn” gttSetType.

POST

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

```
{
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "emapaddr": "11223344",
            "fallback": "Sysdflt",
            "gttSetName": “set1",
            "routingIndicator": “Gt",
            "rspName": "rsp1",
            "smapaddr": "11223344",
            "translateIndicator": "Dpc“
        }
```

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

```
/vstp/globaltitleaddresses/ -v POST -r <filename>.json
```

Sample Output:

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

GET

Execute the following command to display the content:

```
/vstp/globaltitleaddresses
```

Sample Output:

```
{
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "configurationLevel": "402",
            "emapaddr": "11223344",
            "fallback": "Sysdflt",
            "gttSetName": "set1",
            "routingIndicator": “Gt",
            "rspName": "rsp1",
            "smapaddr": "11223344",
            "translateIndicator": "Dpc",
            "uniqueIdentifier": "e9f9edc0-1018-4169-a181-564ff616b4be"
        }
```

2.25.1.2 GUI Configurations for TPDA Based Filtering

The TPDA Based Filtering can be configured from Active System OAM (SOAM). Select **VSTP** , and then **Configuration** page.

- The following parameter on the **GTT Sets** page used to perform the configurations:
  - `GTT Set Type`: This parameter is used setting the GTT Type. It must be set as **Msisdn** for TPDA Filtering.
- The following parameter on the **Global Title Addresses** page are used to perform the configurations:
  - `MAP End Address`: Start Address. This parameter specifies the beginning of a range of MAP digits.
  - `Start Map Address`: Start Address (similar to startAddress). This parameter specifies the beginning of a range of MAP digits

For more information, see GUI Configurations.

2.25.2 Troubleshooting

The following measurements are pegged in case of successful and failed GTTs respectively:

- VstpSccpGTTPERFD
- VstpCdpaGTTFail

For more information, see *Diameter Signaling Router Measurement Reference Guide*.

2.25.3 Dependencies

The TPDA Based Filtering functionality for vSTP has no dependency on any other vSTP operation.

2.26 Tracing and Troubleshooting

This chapter provides the brief description for Tracing and Troubleshooting. This feature helps to troubleshoot and understand the life cycle of ingress Message at VSTP.

The vSTP Tracing feature adds to vSTP capabilities by allowing the life cycle of any ingress message at vSTP to be tracked and traced using message parameters.

The integration of troubleshooting capabilities into vSTP provides a high value proposition for customers to be able to troubleshoot issues that might be identified with the MTP3 or SCCP traffic transmitted to the vSTP.

The troubleshooting capabilities can supplement other network monitoring functions provided by the network support centers to quickly help and point the root cause of signaling issues.

> **Note**
>
> Post upgrade of SOAM server, verify if the "traceoam" process is running (use the "pl" command to verify). If it is not running, run the following commands in sequence:
>
> ```
> cd /usr/TKLC/vstp/prod/maint/loaders/upgrade
>
> ./load.vstp.upgrade.9.2.0+DSS6200
> ```

2.26.1 Tracing and Troubleshooting Feature Description

Following are the feature description for Tracing and Troubleshooting:

- Enables the user to create, enable, and disable tracing filters based on MTP3 and SCCP parameters to capture messages required for troubleshooting service issues.
- The vSTP tracing filters will generate PCAPNG file which captures the detailed information about the lifecycle of ingress message.
- The PCAPNG file, can be downloaded from file management of active SOAM over CLI as well as GUI status and manage file.
- The user can configure the repetition count of vSTP tracing filter to be tracked in PCAPNG file along with the duration up to which the vSTP tracing filter will remain active.
- Each repetition count will track the traced lifecycle of one ingress message.
- Each trace of PCAPNG file name starts with trace Id of the configured vSTP tracing filter and rotates from index 0 to 9.

- At vSTP, each ingress packet is either routed, discarded, or processed (similar to SSNM messages). As a result, the Trace `Pcap` file will capture the entire lifecycle of the message, from ingress to egress, ingress to discard or ingress to processed, based on the selected vSTP Tracing Filter.
- At vSTP the packet captured in PCAPNG file will have annotations corresponding to the actions, modifications, or operations performed.
- The `Traceoam` process at active SOAM will create PCAPNG files based on the traced packets received from vSTP MPs.

2.26.2 Feature Configuration Tracing and Troubleshooting

This chapter provides information about configuring trace filter parameters using new managed object `VstpTraceFilterParams`

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

The TRACEID (integer value) is auto generated by GUI, the user has to configure minimum one filter parameter. The Database lookup will be performed and TraceID with exact match entry to be used for the processing.

Parameters

The parameters given in table are used to perform the configurations for `TraceFilterParams`:

Table 2-31 Parameters

Name	Range	Description
OPC	Valid characters are integers, plus (+), and minus (-) sign. Maximum allowed length is 11.	Originating point code
DPC	Valid characters are integers, plus (+), and minus (-) sign. Maximum allowed length is 11.	Destination point code
SI	0 to 5	Service indicator
CDSSN	2 to 255	CdPA subsystem number
CGSSN	2 to 255	CgPA subsystem number.
CDPC	Valid characters are integers, plus (+), and minus (-) sign. Maximum allowed length is 11.	Called party point code
CGPC	Valid characters are integers, plus (+), and minus (-) sign. Maximum allowed length is 11.	Called party point code
CDRI	None, SSN, GT	Called Party Routing indicator.
CGRI	None, SSN, GT	Called Party Routing indicator.
CDTT	0 to 255	Called party translation type
CGTT	0 to 255	Calling party translation type
CDNAI	Subscriber, Reserved, National, International, and Spare.	Called Party Nature of Address indicator
CDNP	E164, Generic, X121, F69, E210, E212, E214, and Private.	Called Party Numbering Plan
CGNAI	Subscriber, Reserved, National, International, and Spare.	Called Party Nature of Address indicator.
CGNP	E164, Generic, X121, F69, E210, E212, E214 and Private	Calling Party Numbering Plan

Table 2-31 (Cont.) Parameters

Name	Range	Description
CDPA Address	a-f,A-F,0-9,*; Maximum Length = 21	Called party address
CGPA Address	a-f,A-F,0-9,*; Maximum Length = 21	Called party address
CDNPV	0 to 15	Called numbering plan
CDNAIV	0 to 127	Calling nature of Address indicator
Trace ID	0 to 100	Trace Identifier
Trace Enabled	No, Yes	Trace Enabled
Rep	1 to 5000	Rep
Duration	1 to 60 (in minutes)	Duration
Msg Type	UDT, XUDT, UDTS, XUDTS	Message Type
Domain	None, ANSI, ITUI, ITUN, ITUN24, ITUI_S, ITUN_S	Domain
Birth Time	Date or Time	Birth Time
Link set	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.	Link Set Name

2.26.2.1 GUI Configurations Tracing and Troubleshooting

The trace filter parameters conversion can be configured from Active System OAM (SOAM). Select **VSTP** --> **Configuration** page.

For parameters, see Feature Configuration for tracing and Troubleshooting.

2.26.2.2 MMI Managed Objects for Trace Filter Params

The conversion can be configured from Active System OAM (SOAM).

MMI information associated with vSTP generated Trace Filter Params can be configured from DSR SOAM **Main Menu** and **MMI API** Guide. From the **MMI API** guide, use the application navigation to locate specific vSTP managed object information.

Navigate to MMI API Guide, from the **Main Menu**, and click **MMI API guide**.

With `TraceFilterParams`, a user can apply filter on traces through filter parameters. All configuration of `TraceFilterParams` is done at the SOAM.

Table 2-32 MOs and Operations supported

MO Name	Operations Supported	URI
Trace Filter Params	POST/PUT/DELETE/GET	/vstp/tracefilterparams

Post

Following are the steps to post `Tracefilterparams`:

1. Create a file with the following parameters:

```
{
            "cdnaiv": 100,
            "cdpa_address": "123abc",
            "cdtt": 40,
            "cgnp": "Private",
            "domain": "Itui",
            "duration": 25,
            "opc": "2-2-2",
            "rep": 20,
            "traceEnabled": "No"
        }
```

2. Run the following command on active SOAM to post `TraceFilterParams`:

```
mmiclient.py /vstp/tracefilterparams -v POST –r /<Absolute Path>/<File
Name>
```

Example output for Insert :

```
/vstp/tracefilterparams -v POST -r /home/admusr/<filename>.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Get

Run the following command on Active SOAM to Get the TraceFilterParams:

```
/vstp/tracefilterparams
```

Example output for Get:

```
{
            "birthTime": "2024-03-28T02:27:55-04:00",
            "cdnaiv": 100,
            "cdpa_address": "123abc",
            "cdtt": 40,
            "cgnp": "Private",
            "domain": "Itui",
            "duration": 25,
            "opc": "2-002-2",
            "rep": 20,
            "traceEnabled": "No",
            "traceId": 1
        }
    ],
    "links": {},
```

```
    "messages": [],
    "status": true
```

Update

Following are the steps to update `Tracefilterparams`:

1. Create a file with the following parameters:

```
{
            "duration": 40,
            "rep": 501,
            "traceEnabled": "No",
            "traceId": 1
 }
```

2. Run the following command on active SOAM to update `TraceFilterParams`:

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

Example output for update:

```
/vstp/tracefilterparams -v PUT -r /home/admusr/<filename>.json
{
    "data": true,
    "links": {},
    "messages": [],
    "status": true
}
```

Delete

Run the following command on active SOAM to delete MTP screening rule:

```
/vstp/tracefilterparams/<Trace ID> -v DELETE
```

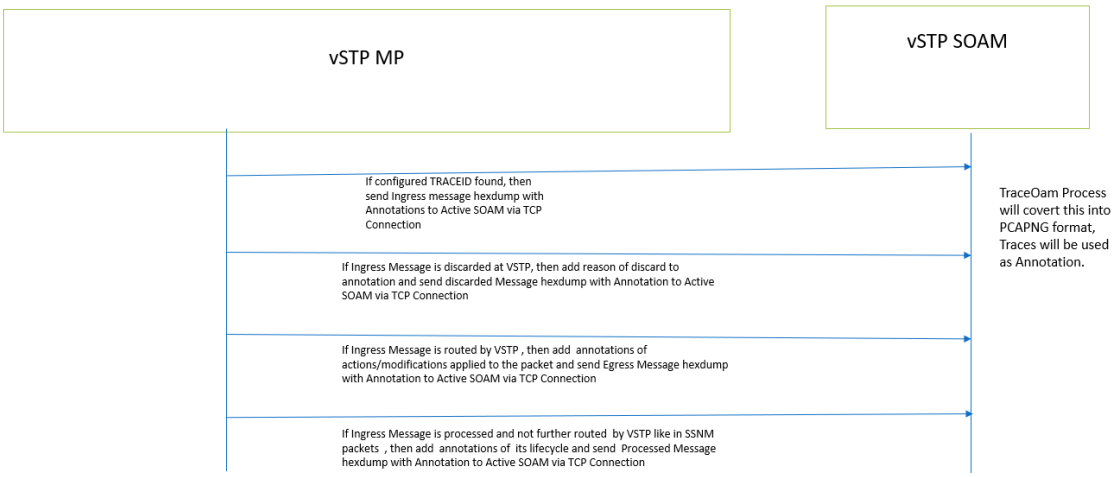
2.26.2.3 Virtual Internet Protocol (VIP)

To use vSTP Troubleshooting feature, a remote server needs to be configured , this can be performed by configuring Virtual Internet Protocol (VIP) Address.

Virtual Internet Protocol is required to establish connection between `Traceoam` process at active SOAM and VSTP MP.

TCP Protocol is used to communicate with vSTP MP and `TraceOam` process at Active SOAM. `TraceOam` process is a server process, listens at VIP address responsible for creating PCAPNG file from Tracing Data received from vSTP MP.

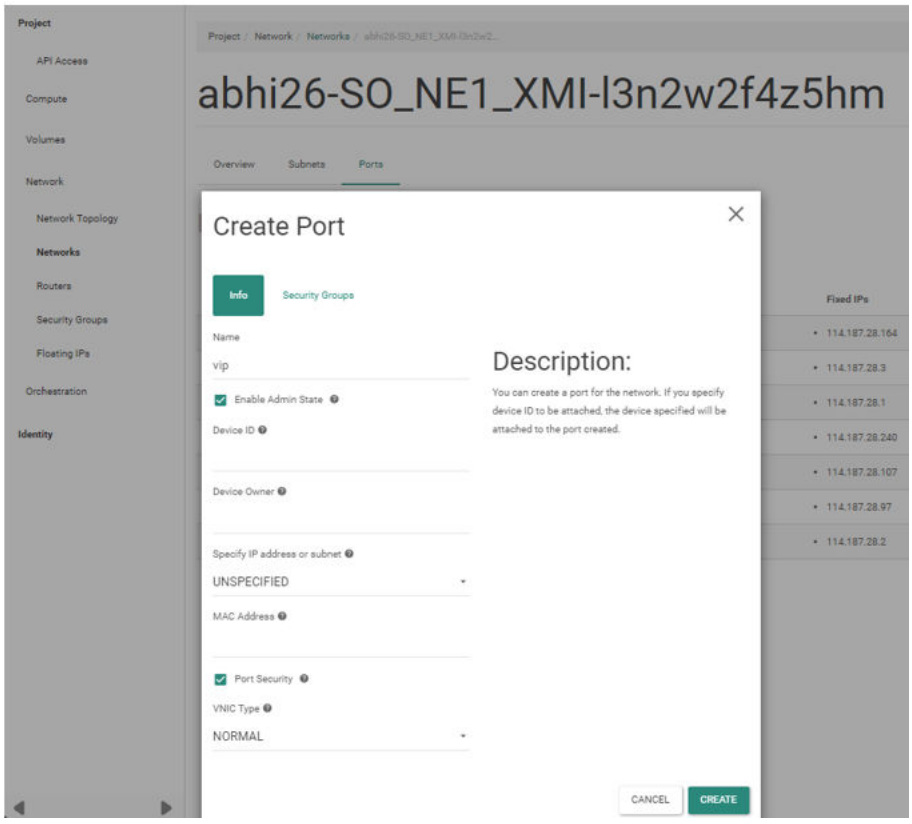
Figure 2-18 Architecture Design



Following are the steps to configure Virtual Internet Protocol address on SOAM and NOAM:

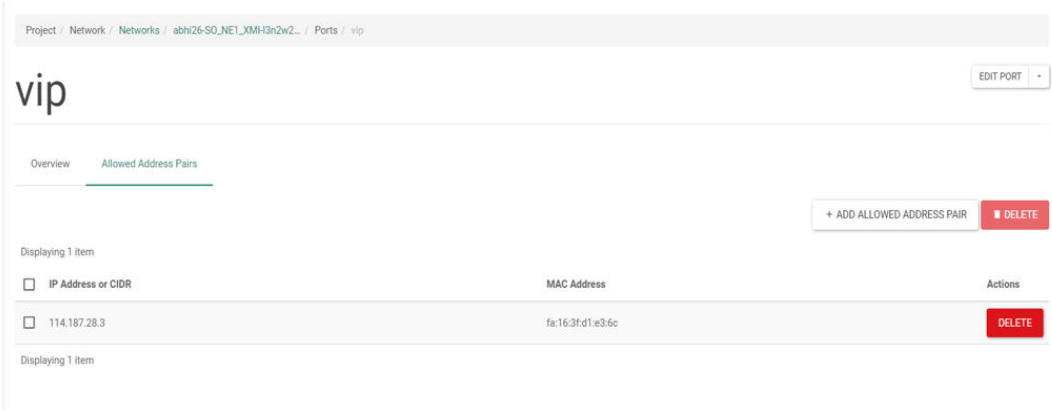
1. From the **Main Menu** of **OpenStack** cloud, click **Network** for the network page to open.
2. Select SO_NE1_XMI network for your stack.
3. Click **Create Port** and provide the name for the VIP port.

Figure 2-19 Creating Port



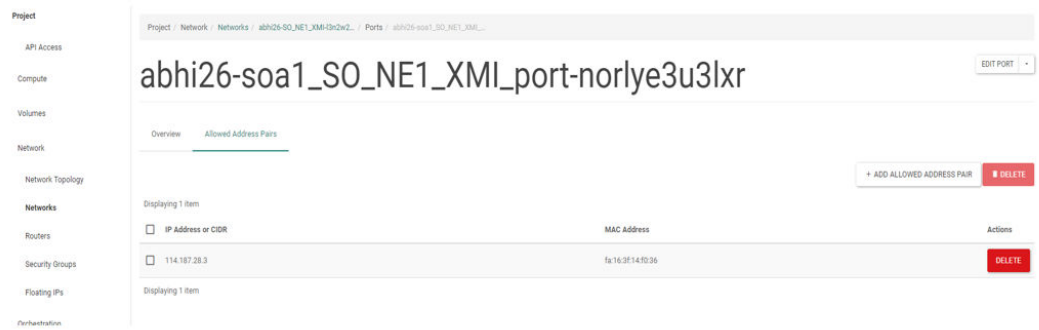
4. Click the newly added **VIP** port and then, navigate to **Allowed Address Pairs**.
5. Add your allocated VIP address.

Figure 2-20 VIP Port



6. Navigate to your active **SOAM** as illustrated in the following image soa1 is active. Click soa1_SO_NE1_XMI.
7. Click **Allowed Address Pairs**.
8. Add the IP address allocated previously.

Figure 2-21 Port



9. Log in to active NOAM and **Add** VIP address for Site server group.
Following image is an example of allocating VIP address:

Figure 2-22 Server Groups 1

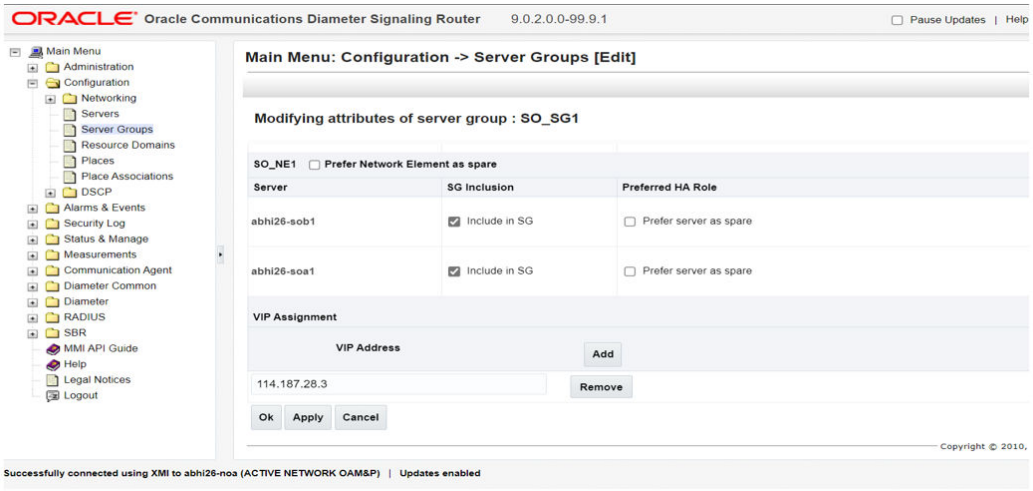
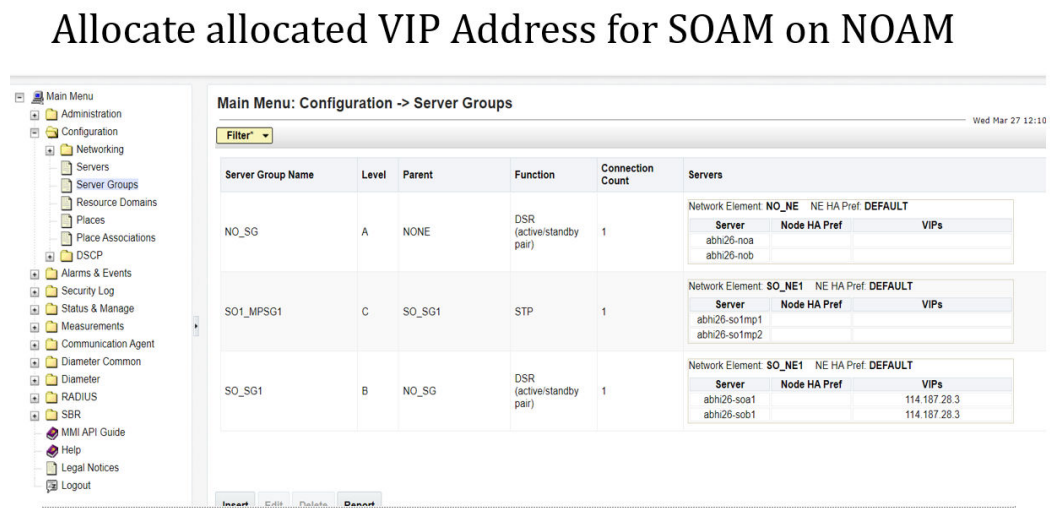


Figure 2-23 Server Groups 2



2.26.2.4 Alarms/Events and Measurements for vSTP Tracing and Troubleshooting

The following table lists the Alarms and Events for vSTP Tracing and Troubleshooting:

Table 2-33 Alarms

Alarm ID	Name	
70481	vSTP Tracing Stack Event Queue Utilization	
70482	vSTP Trace Oam Event Queue Utilization	

Table 2-34 Events

Event ID	Event Name
70478	failedToCreatePcapngFile
70479	tracingLayerCongestion
70480	traceIdDisabled

For more information, see *DSR Measurement Reference Guide*.

Table 2-35 Measurements

Measurement ID	Measurement Name
22321	VstpIngressTraced
22322	VSTP Tracing Performance
22323	VstpDiscardTraced
22324	VstpProcessedSsnmTraced
22325	VstpIngressTracedPerTi
22326	VstpEgressTracedPerTi
22327	VstpDiscardTracedPerTi
22328	VstpNumMsgLoggedPerTi
22329	VstpProcessedSsnmTracedPerTi
22330	VstpTracingStackQueuePeak
22331	VstpTracingStackQueueAvg
22332	VstpTracingStackQueueFull
22333	VstpIngressNotFilteredCpuExceed
22334	VstpTracingDiscardCpuExceed
22338	VstpTraceOamStackQueuePeak
22339	VstpTraceOamStackQueueAvg
22340	VstpTraceOamStackQueueFull
22341	VstpNumTraceSendSoamFail
22342	TraceoamNumRecvdPerTi
22343	TraceoamNumDiscardedPerTi

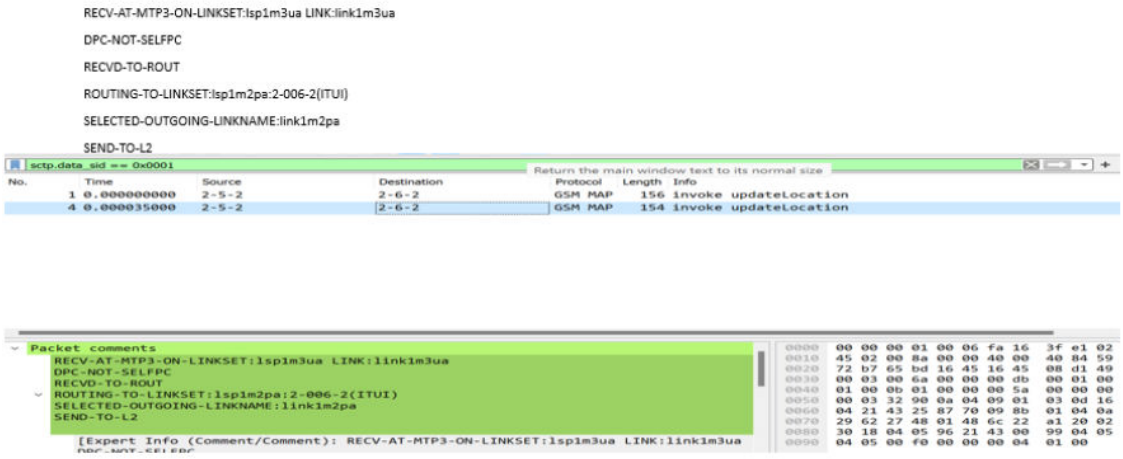
2.26.3 Troubleshooting Examples for Tracing and Troubleshooting

Annotations for any Ingress MTP3 Message.

Figure 2-24 Ingress MTP3 Message

Annotations for Egress MTP3 Routed Message

Figure 2-25 Egress MTP3 Routed Message



Annotations for Egress SCCP Routed Message

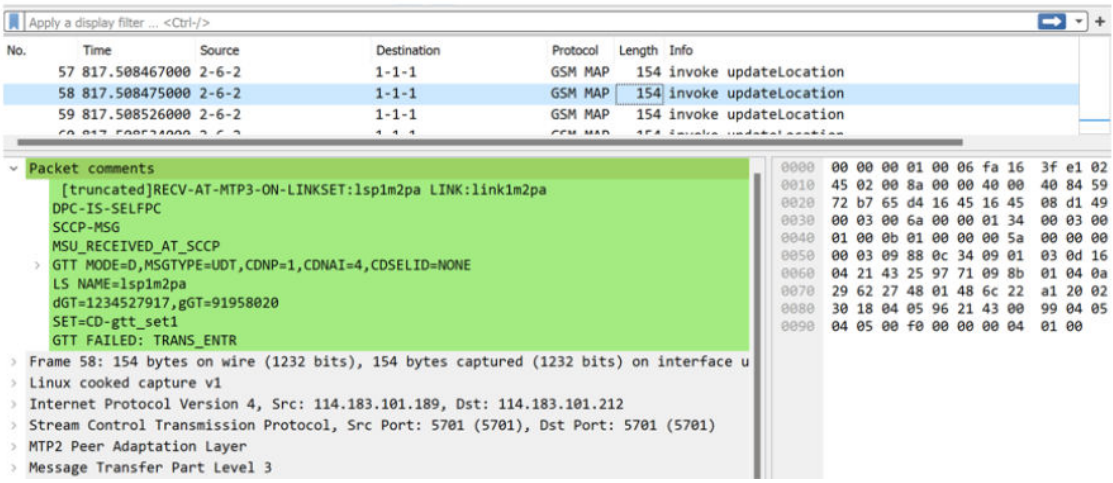
```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SCCP-MSG
MSU_RECEIVED_AT_SCCP
GTT MODE=D,MSGTYPE=UDT,CDNP=1,CDNAI=4,CDSELID=NONE
LS NAME=lsp1m2pa
dGT=1234527907,gGT=91958020
SET=CD-GTT_SET1
xlatPC=2-005-2, GTMODID=-, CGPCACT=DFLT, ACTSN=-
SCCP -MSU Encoded:GTT perfd
GTT complete
RECVD-TO-ROUT
ROUTING-TO-LINKSET:lsp1m3ua:2-005-2(ITUI)
SELECTED-OUTGOING-LINKNAME:link1m3ua
SEND-TO-L2
```

Annotations for SCCP Routed Message, No Translation Found, Send UDTs On OPC option is OFF.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SCCP-MSG
MSU_RECEIVED_AT_SCCP
GTT MODE=D,MSGTYPE=UDT,CDNP=1,CDNAI=4,CDSELID=NONE
LS NAME=lsp1m2pa
dGT=1234527917,gGT=91958020
SET=CD-gtt_set1
GTT FAILED: TRANS_ENTRY_NOT_FOUND
SCRC ERROR REASON:No translation found
SCRC_ERR_NO_TRANS_FOUND
DISCARDING PACKET
```

Annotations for SCCP Routed Message, No Translation Found, Send UDTs On OPC option is OFF – Contd.

Figure 2-26 SCCP Routed Message



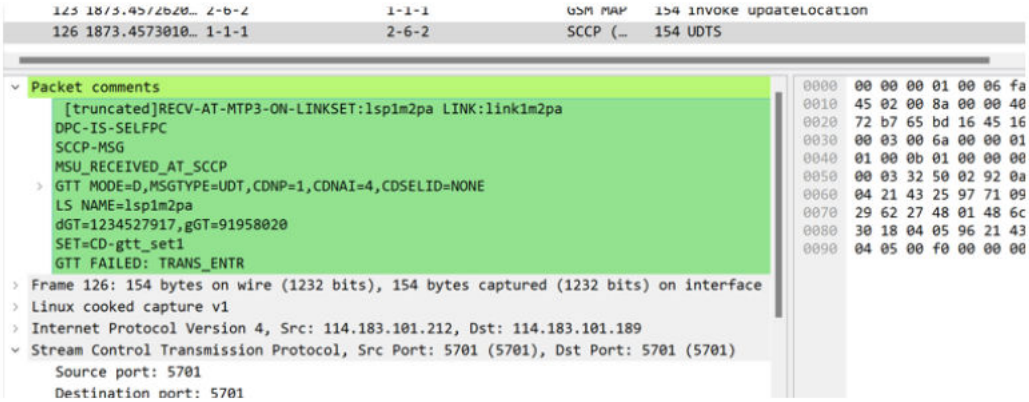
Annotations for SCCP Routed Message, No Translation Found, Send UDTs On OPC option is ON.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SCCP-MSG
MSU_RECEIVED_AT_SCCP
GTT MODE=D,MSGTYPE=UDT,CDNP=1,CDNAI=4,CDSELID=NONE
LS NAME=lsp1m2pa
dGT=1234527917,gGT=91958020
SET=CD-gtt_set1
GTT FAILED: TRANS_ENTRY_NOT_FOUND
SCRC ERROR REASON:No translation found
SCRC_ERR_NO_TRANS_FOUND
SCRC_UDTS_SENT
RECVD-TO-ROUT
```

```
ROUTING-TO-LINKSET:lsp1m2pa:2-006-2(ITUI)
SELECTED-OUTGOING-LINKNAME:link1m2pa
SEND-TO-L2
```

Annotations for SCCP Routed Message, No Translation Found, Send UDTs On OPC option is ON- Contd.

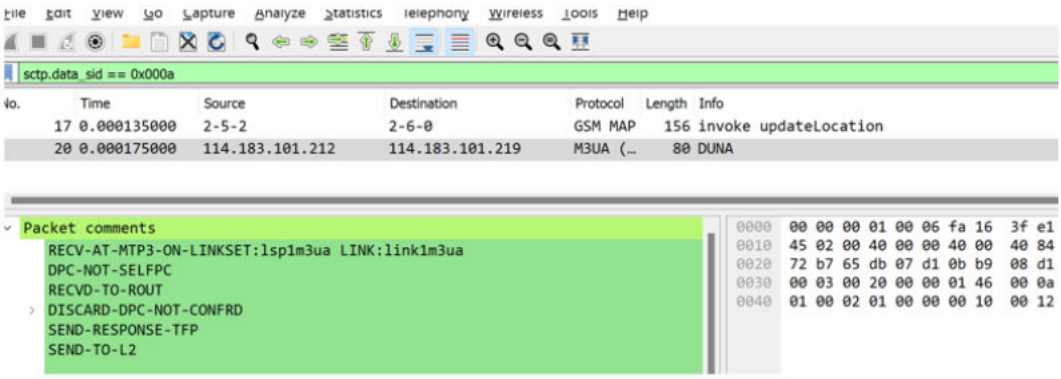
Figure 2-27 SCCP Routed Message



Annotations for MTP3 Routed Message, RSP not configured so DUNA generated.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m3ua LINK:link1m3ua
DPC-NOT-SELFPC
RECVD-TO-ROUT
DISCARD-DPC-NOT-CONFRD
SEND-RESPONSE-TFP
SEND-TO-L2
```

Figure 2-28 MTP3 Routed Message

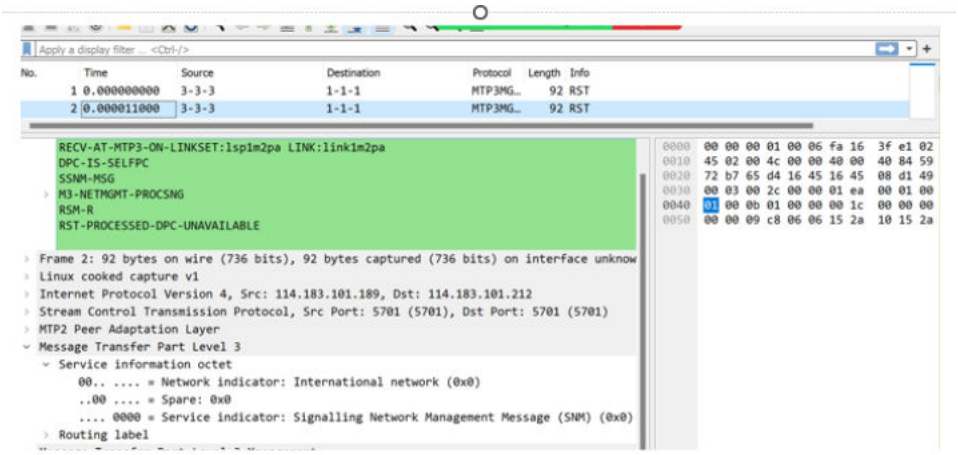


Annotations for SNM - RST From Peer , Processed At VSTP for unavailable DPC.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SSNM-MSG
M3-NETMGMT-PROCSNG
RSM-R
RST-PROCESSED-DPC-UNAVAILABLE
```

Annotations for SNM - RST From Peer, Processed At vSTP for unavailable DPC - Contd.

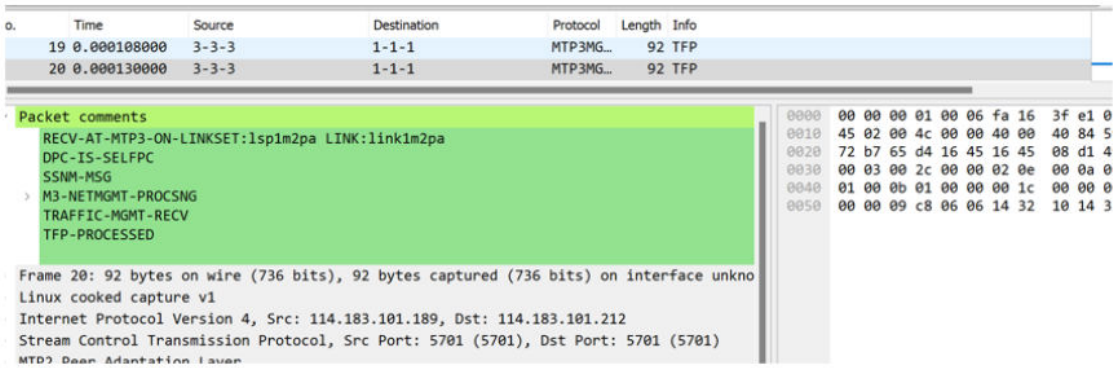
Figure 2-29 SNM



Annotations for SNM -TFP From Peer, Processed At vSTP.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SSNM-MSG
M3-NETMGMT-PROCSNG
TRAFFIC-MGMT-RECV
TFP-PROCESSED
```

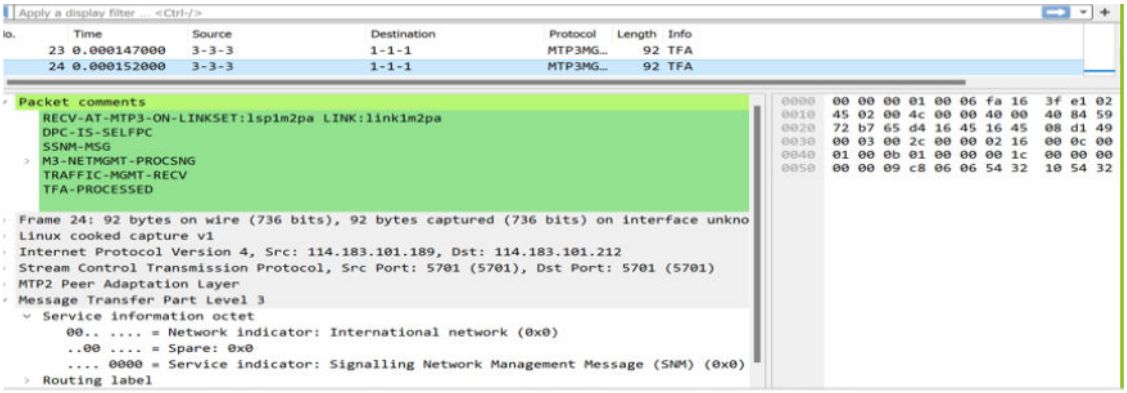
Figure 2-30 SNM -TFP



Annotations for SNM - TFA From Peer, Processed At vSTP.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SSNM-MSG
M3-NETMGMT-PROCSNG
TRAFFIC-MGMT-RECV
TFA-PROCESSED
```

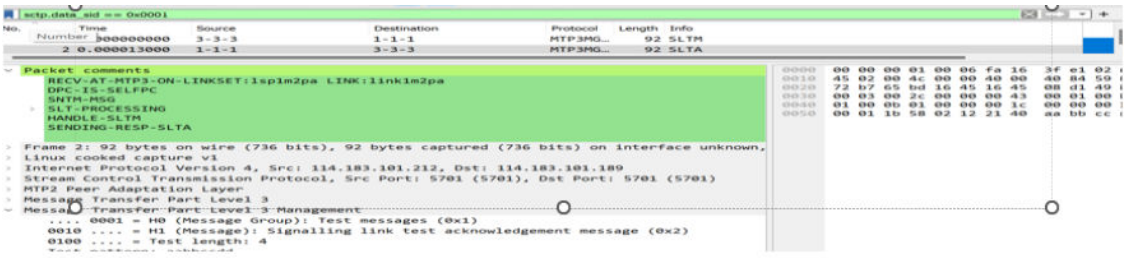
Figure 2-31 SNM - TFA



Annotations for Link Management Messages - Incoming SLTM responded with SLTA message

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SNTM-MSG
SLT-PROCESSING
HANDLE-SLTM
SENDING-RESP-SLTA
```

Figure 2-32 Link Management Message

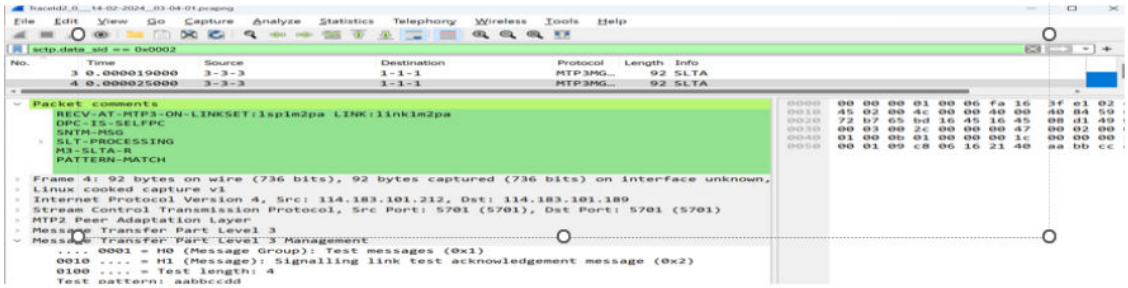


Annotations for Link Management Messages - Incoming SLTA processed at vSTP.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m2pa LINK:link1m2pa
DPC-IS-SELFPC
SNTM-MSG
SLT-PROCESSING
```

```
M3-SLTA-R
PATTERN-MATCH
```

Figure 2-33 Link Management Message

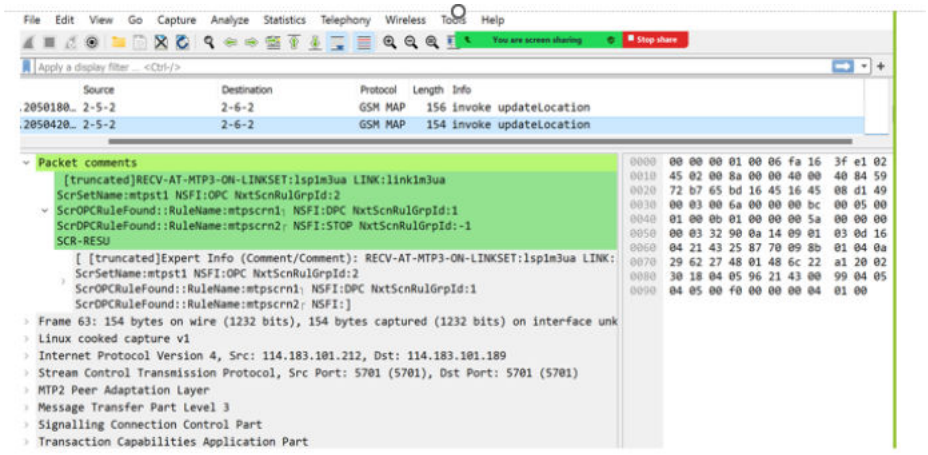


Annotations for `MTP3 Screened Message - OPC- DPC - STOP`

```
RECV-AT-MTP3-ON-LINKSET:lsp1m3ua LINK:link1m3ua
ScrSetName:mtpst1 NSFI:OPC NxtScnRulGrpId:2
ScrOPCRuleFound::RuleName:mtpscrn1 NSFI:DPC NxtScnRulGrpId:1
ScrDPCRuleFound::RuleName:mtpscrn2 NSFI:STOP NxtScnRulGrpId:-1
SCR-RESULT-CONTINUE
DPC-NOT-SELFPC
RECVD-TO-ROUT
ROUTING-TO-LINKSET:lsp1m2pa:2-006-2(ITUI)
SELECTED-OUTGOING-LINKNAME:link1m2pa
SEND-TO-L2
```

Annotations for `MTP3 Screened Message - OPC DPC - STOP - Contd.`

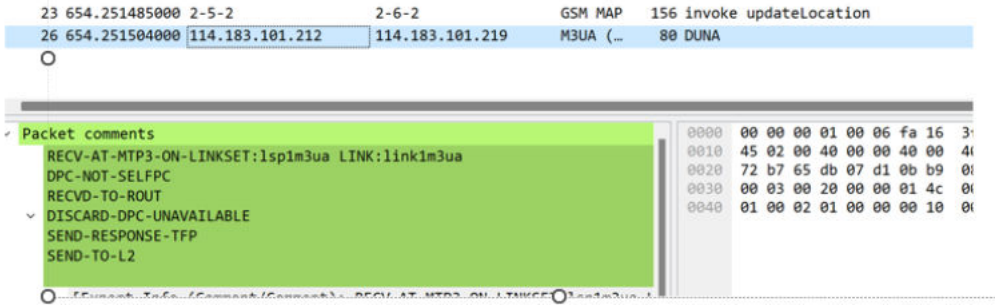
Figure 2-34 MTP3 Screened Message



Annotations for MTP3 Routed Message, RSP not available so DUNA generated.

```
RECV-AT-MTP3-ON-LINKSET:lsp1m3ua LINK:link1m3ua
DPC-NOT-SELFPC
RECVD-TO-ROUT
DISCARD-DPC-UNAVAILABLE
SEND-RESPONSE-TFP
SEND-TO-L2
```

Figure 2-35 MTP3 Routed Message



2.26.4 Dependencies for vSTP Tracing and Troubleshooting

Following are the dependencies for vSTP Tracing and Troubleshooting:

- To disable the `traceid` by SOAM takes time, hence extra tracing packet can be sent to MP through SOAM.
- If the last file used for PCAPNG file for a specific TRACEID does not exist, either deleted or renamed or moved , then PCAPNG file will be generated from 0th index.
- The maximum file size of `PCAPNG` is 50 to 60 MB.
- Routing context is an optional parameter for both M3UA data and management message, therefore it will not be included in the tracing `pcapng` file.
- When the SOAM process switches from standby to active, the disks for each SOAM are different, hence the file formation will start from index 0.

2.27 Support of 700M Subscribers for MNP/ENUM

UDR subscriber capacity is enhanced to support 700M subscribers to enable larger MNP deployments. There are 3 different VM profiles introduced for MNP, ENUM and MNP+ENUM deployments. For more information about UDR VM profiles see, appendix G of *Oracle Communications User Data Repository Installation Guide*.

2.28 Translation Type (TT) Maps

This section provides a brief description for Translation Type (TT) Maps Support feature.

Certain SCCP messages include a `Called Party Address` parameter, which has a translation type field. The translation type field indicates the type of global title processing required at the STP. The values utilized in any given network may differ from the standardized values defined for internetwork applications.

The translation type mapping feature enhances the functionality of the vSTP by allowing the standardized translation type code values for internetwork applications to be mapped to intranetwork values used within any particular network as well as intranetwork values to be mapped to internetwork values.

TT maps feature is only applicable on UDT and XUDT messages with global title indicator (GTI) is 2 (For ANSI/ITU Domain) or 4 (For ITU Domain).

Example:

```
A TT Map is defined as
{
"linksetName":"ls1",
 "existingTT":25,
 "modifiedTT": 40,
 "ingressEgress":"Ingress",
 "name": "ttmap1"
}
```

Any UDT or XUDT messages with global title indicator (GTI) is 2 (For ANSI/ITU Domain) or 4 (For ITU Domain) incoming on “ls1” linkset having SCCP Called Party TT as 25 will be modified to have SCCP Called Party TT as 40.

2.28.1 Feature Configuration

This section provides procedures to perform the TT Maps functionality.

The TT Map 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.

2.28.1.1 MMI Managed Objects for TT Maps

MMI information associated with TT Maps 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 TT Maps feature:

Table 2-36 Managed Objects

MO Name	Supported Actions	URI
M3RL Options	GET, PUT	/vstp/m3rloptions
TT Maps	GET, POST, PUT, DELETE	/vstp/ttmaps

M3rl Options - PUT

The `ttMapSupport` parameter must be On to enable TT Maps feature.

Create a file with following content. For example: "Test" can be used as filename:

```
$ vim Test.json
{
```

```
    "ttMapSupport": "On"
}
```

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

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

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

TT Maps - POST

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

```
$ vim ttMapTest.json
{
 "linksetName":"ls1",
 "existingTT":25,
 "modifiedTT": 40,
 "ingressEgress":"Ingress",
 "name": "ttmap1"
}
```

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

```
/vstp/ttmaps -v POST -r /<Absolute Path>/<File Name>.json


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

TT Maps - GET

Run the following command on Active SOAM to get the data:

```
/vstp/ttmaps/<name> -v GET

Sample Output:

{
    "data": [
        {
            "existingTT": 25,
```

```
            "ingressEgress": "Ingress",
            "linksetName": "ls1",
            "modifiedTT": 40,
            "name": "ttmap1"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

TT Maps - PUT

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

```
$ vim ttMapTest.json
{
 "linksetName":"ls1",
 "existingTT":25,
 "modifiedTT": 45,
 "name": "ttmap1"
}
```

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

```
/vstp/ttmaps/<name> -v PUT -r /<Absolute Path>/<File Name>.json
```

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

TT Maps - Delete

Run the following command on active SOAM to delete TT Map record:

```
/vstp/ttmaps/<name> -v DELETE
```

2.28.1.2 GUI Configurations for TT Maps

The TT Maps can be configured from Active System OAM (SOAM). Select **VSTP**, and go to the the **Configuration** page.

To perform the configuration, use the following parameter **M3RL Options MO**:

- `TT Map Support`: This parameter is used for turning on or off the TT Map feature. If On, only then the TT Mapping will be supported.

For more information, see M3rl Options.

Select TT Maps and configure the parameters.

For more information, see TT Maps.

2.28.1.3 Alarms/Events and Measurements for TT Maps

> **Note**
>
> No new alarm or Events are introduced for TT Maps feature.

The following measurements are added to TT Maps feature:

Table 2-37 Measurements

Measurement ID	Measurement Name	Description
22317	VstpIngressTTModified	Total number of Ingress TT modified.
22318	VstpEgressModified	Total number of Egress TT modified.
22319	VstpLinksetIngressTTMod	Number of Ingress TT modified on particular link set.
22320	VstpLinksetEgressTTMod	Number of Egress TT modified on particular link set.

2.29 PCT

This chapter provides the brief description for Point code and CIC Translation (PCT) Feature.

The feature enables vSTP to change the DPC or OPC and or CIC of a MTP routed message. This gives vSTP the capability to emulate a point code using other nodes in its network. This feature provides a table in which translations between an emulated point code and real point codes can be defined.

Other network nodes can send traffic to the emulated PC (EPC) and receive traffic from the EPC without knowing that the real PC that is emulating the EPC. This way the Real PC can be changed transparently from the rest of the network. The rest of the network can continue sending messages to the EPC.

The PCT feature can also be used to modify the CIC of ISUP messages. Translations can be defined between Emulated CIC range and Real CIC range.

2.29.1 Feature Configuration PCT

This section provides procedures to perform the Point Code and CIC Translation functionality.

The PCT 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.

2.29.1.1 GUI Configurations for PCT

The PCTs can be configured from Active System OAM (SOAM). Select **VSTP**, and then **Configuration** page.

The following parameter on the **M3RL Options MO** is used to perform the configurations:

- PCT: This parameter is used for turning on/off /lset the PCT feature. If On then PCT will be supported on all the linksets, whose Linkset PCT parameter is On. If PCT is Off then PCT feature will not be supported for any linksets.

For more information see M3rl Options.

The following new parameter on the **Link Set MO** is used to perform the configurations:

- Linkset PCT: It will only be considered if PCT is set to LSET in M3RL options. It will control whether PCT feature is applied to MSUs coming in or going out on links of a particular linkset.

Select PCTs and configure the parameters. For more information related to the above parameters, see PCT

2.29.1.2 MMI Managed Objects for PCTs

MMI information associated with PCT 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 PCTs feature:

Table 2-38 Managed Objects

Managed Object, Name	Supported Actions	URI
M3RL Options	GET, PUT	/vstp/m3rloptions
Link Sets	GET, POST, PUT, DELETE	/vstp/linksets
PCTs	GET, POST, DELETE	/vstp/pcts

M3rl Options - PUT

The pct parameter must be On or LSet to enable PCTs feature.

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

```
$ vim Test.json
{
    "pct": "On"
}
```

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

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

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

Link Sets - POST

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

```
$ vim linksetTest.json
 {
    "asNotification": true,
    "configurationLevel": "0",
    "cgGtmod": false,
    "enableBroadcastException": true,
    "gttmode": "Fcd",
    "ituTransferRestricted": false,
    "reservedLinkTransactionsPerSecond": 100,
    "maximumLinkTransactionsPerSecond": 120,
    "localSignalingPointName": "TestItua",
    "mtpScrSetName": "scrSet1",
    "mtpScrTestMode": true,
    "mtpScrEventLog": true,
    "name": "Test",
    "numberSignalingLinkAllowedThreshold": 1,
    "numberSignalingLinkProhibitedThreshold": 1,
    "remoteSignalingPointName": "gkAnsi",
    "routingContext": 8,
    "smsProxy": "Off",
    "type": "M3ua",
    "linksetPct":"On"
}
```

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

```
/vstp/linksets -v POST -r /<Absolute Path>/<File Name>.json


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

PCTs - POST

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

```
$ vim pctTest.json
{
   "domain": "Ansi",
   "epc": "2-3-4",
   "filtPc": "*",
   "pctSI": "*",
   "pctSsn": "*",
   "ecics": "*",
```

```
   "ecice": "*",
   "rcice": "*",
   "rcics": "*",
   "realPc": "2-2-2"
}
```

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

```
/vstp/pcts -v POST -r /<Absolute Path>/<File Name>.json
```

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

PCTs - GET

Run the following command on Active SOAM to get the data:

```
/vstp/pcts/<unique Identifier> -v GET

Sample Output:

{
   [
     {     "domain": "Ansi",
            "ecice": "*",
            "ecics": "*",
            "epc": "2-3-4",
            "filtPc": “*",
            "pctSI": "*",
            "rcice": "*",
"rcics": "*",
            "realPc": "2-2-2",
            “uniqueIdentifier”: 007d418c-ac05-4d68-ba55-3b8ea07ee74a
     },
 ],
    "links": {},
    "messages": [],
    "status": true
}
```

PCTs - Delete

Run the following command on active SOAM to delete PCT record:

```
/vstp/pcts/<unique Identifier> -v DELETE
```

2.29.1.3 Alarms/Events and Measurements for PCTs

> **Note**
>
> No Alarm is raised for this feature.

Table 2-39 Measurements

Measurement Id	Measurement Name	Description
22335	VstpPctDpcLookup	Number of MSUs for which the PCT DPC Lookup was done successfully.
22336	VstpPctOpcLookup	Number of MSUs for which the PCT OPC Lookup was done successfully.

Table 2-40 Events

Event Number	Event Name	Description	Raise Condition
70459	vSTPCTMSUDiscard	MSU discarded after successful PCT DPC Lookup due to DPC unavailability.	Case 1: DCP look up is successful, MSU is MTP routed and doesn't go to SCCP, and DPC is unavailable. Case 2: DCP look up is successful, MSU is MTP routed and go to SCCP because of screening, and MTP routed GTT is set to UsemtpPc and DPC is unavailable.

2.29.2 **Troubleshooting**

If the DPC Lookup changes the DPC of a MSU and the outgoing route selected for the MSU has the same linkset as incoming linkset, then vSTP will detect this as a circular route condition (incoming linkset is same as outgoing linkset for an MSU) and the MSU will be discarded.

2.30 vSTP Proxy Point Code Feature

When introducing vSTP to home network and replacing direct connect links to a foreign network, a method must be available for seamless migration. At present, if the home network

migrates links from direct connect to the vSTP, the foreign network must change the APC from the original node to the vSTP self Point Code. In many cases, the foreign network is resistant to change, and this may impact the rollout of the vSTP.

For example, if a foreign network SS7 node is directly connected to an SS7 node in the home network, vSTP can be deployed so that the transition is transparent to the foreign node. The foreign node can still function as if it is connected to the original node in the home network. vSTP will provide routing connectivity in the home network to the foreign node and will allow the foreign node to connect to the home network.

2.30.1 Feature Configurations

This section provides procedures to perform the Proxy point code functionality.

The Proxy point code 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.

2.30.1.1 GUI Configurations for Proxy point code

The Proxy point code can be configured from Active System OAM (SOAM). Select **vSTP** and select **Configuration** page.

The following parameter on the M3RL Options MO is used to perform the configurations:

- Proxy Point Code Support: This parameter is used for turning on or off the proxy point code feature. If On then only Proxy point code will be supported else not.

For more information see M3rl Options.

The following parameter on the Remote Signaling Point MO is used to perform the configurations:

- Proxy Point Code Indicator: Indicates if Point code is to be used as a proxy point code. For more information see Remote Signaling Point.

The following parameter on the Link Sets MO is used to perform the configurations:

- Proxy RSP Name: The parameter indicates Name of the Proxy Remote Signaling Point associated with this Link Set.
  For more information see Link Sets.

2.30.1.2 MMI Managed Objects for Proxy point code

MMI information associated with Proxy point code feature is accessed from a DSR NOAM or SOAM from Main Menu, and then MMI API Guide.

After 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 Proxy point code feature:

Table 2-41 Managed Objects

Managed Object Name	Operations Supported	URI
M3RL Options	GET/PUT	/vstp/m3rloptions
Remote Signaling Points	GET/POST/PUT/DELETE	vstp/remotesignalingpoint

Table 2-41 (Cont.) Managed Objects

Managed Object Name	Operations Supported	URI
Link Sets	GET/POST/PUT/DELETE	/vstp/linksets

M3rl Options - PUT

The `Proxy Point Code Support` parameter is used for turning on or off the proxy point code feature. Proxy Point Code Support parameter must be **On** to enable Proxy point code feature.

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

```
$ vim Test.json
{
    "Proxy Point Code Support": "On"
}
```

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

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

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

`remotesignalingpoints`

The **Proxy Point Code Indicator** parameter in `remotesignalingpoint` MO Indicates if Point code is to be used as a proxy point code.

POST

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

```
{
 "enableBroadcastException": true,
 "mtpPointCode": “1-2-1",
 "name": "RSP1",
 "nprst": "Off",
 “udtxudtcnv": "NOCONV",
 "ProxyPointCodeIndicator": "Yes"
}
```

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

```
/vstp/remotesignalingpoints –v POST –r .json


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

GET

Run the following command on Active SOAM to display the content:

```
/vstp/remotesignalingpoints

Sample Output:

{
    "data": [
        {
            "configurationLevel": "5",
            "enableBroadcastException": true,
            "mtpPointCode": "001-002-001",
            "name": "RSP1",
            "nprst": "Off",
            "udtxudtcnv": "NOCONV",
            "ProxyPointCodeIndicator ": "Yes"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

Link Sets – POST

`Proxy RSP Name` parameter in Link Sets MO indicates Name of the Proxy Remote Signaling Point associated with this Link Set.

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

```
$ vim linksetTest.json
 {
   "asNotification": true,
    "configurationLevel": "0",
    "cgGtmod": false,
    "enableBroadcastException": true,
    "gttmode": "Fcd",
    "ituTransferRestricted": false,
    "reservedLinkTransactionsPerSecond": 100,
```

```
    "maximumLinkTransactionsPerSecond": 120,
    "localSignalingPointName": "TestItua",
    "mtpScrSetName": "scrSet1",
    "mtpScrTestMode": true,
    "mtpScrEventLog": true,
    "name": "Test",
    "numberSignalingLinkAllowedThreshold": 1,
    "numberSignalingLinkProhibitedThreshold": 1,
    "remoteSignalingPointName": "TestItub",
    "routingContext":
    "smsProxy": "Off",
    "type": "M2PA",
    "ProxyRSPName": "RSP1"
}
```

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

```
/vstp/linksets -v POST -r /<Absolute Path>/<File Name>.json
```

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

2.30.2 Troubleshooting

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

2.30.3 Dependencies

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

Considerations

The following points must be considered while configuring Proxy Point Code feature:

- Proxy Destination not allowed in GTT, MAP, MRN tables from being assigned for the referenced point code parameter.
- SPC and PPC parameters must not be defined together (SPC and PPC are mutually exclusive).

2.31 vSTP Gateway Screening

The role of vSTP in the SS7 network is to transport messages between originating and destination signaling points. Gateway services need to perform a certain level of message screening. The message acceptance or rejection in the network is verified by the screening procedure that serves as network's initial security check. The message screening depends on the type of message received by vSTP.

It includes screening the incoming messages on the basis of MTP3 parameters and SCCP parameters, hence there is two level of screening:

- MTP3 Screening
- SCCP Screening

2.31.1 MTP3 Screening

In order to verify if a Message Signaling Unit (MSU) is permitted, the mtp screening feature compares the information of the unit attempting to pass the specific requirements of vSTP in the vSTP database. The screening functions are defined by using screening tables referred to as screen sets which contain a set of rules in which the MSU is compared. Each screen set is uniquely identified by a screen set name. MTP screening tables provide screening of MTP messages on the incoming link set.

2.31.1.1 Overview

MTP Screening feature consists of the following fields:

- Originating Point Code (OPC)
- Destination Point Code (DPC)
- Service Information Octet (SIO)
- Affected Destination in MTP Network Management messages
- Affected Point Code and Subsystem number in SCCP Management Messages

The above fields support range and wild card entries.

MTP screening groups screening rules together. This grouping of screening rules is referred to as Screen Rule Group Name which is based on rule type like OPC and DPC. Screen set refers to Screen Rule Group Name. Screen sets shall have unique screen set name and table key. A screen set shall be assigned to a link set. To end screening, a stop action is defined as the Next Screening Function Identifier (NSFI), screening either results in Fail or Stop. Fail causes discard of packet and Stop causes end of screening and further processing at vSTP.

> **Note**
>
> Default Screening Rule on SIO will lead to discard of SCMG messages, hence add appropriate screening rule for SI (Service Indicator)=3(SCCP) and scmg message type.

MTP screening features include:

- Creating screening rule and keeping rules of the same type in a group.
- Creating a screen set and referring to rule group created in the screen set.
- Attaching the screen set to incoming link set.
  - When a message appears on a linkset, the screen set related to that linkset is looked up, and the rule in that rule group is looked up based on the NSFI and rule group name linked with the screen set.
  - If the rule lookup is successful, the message will proceed to the next screen rule group name on the basis of NSFI.
  - If rule lookup does not find a match:

* In case of BLKOPC or BLKDPC rule type, the default rule for that rule group will be looked up and based on the NSFI and next screen rule group name associated.
* In case of `OPC/SIO/DPC/AFTDSTN` rule type, Fail NSFI will be performed.
* If rule type is Affected PC , then NSFI is either STOP or Affected PC SSN (AftPcSsn). Affected PC (eftpc) is configured the same way as OPC/DPC is configured in MTP3 Screening.
* If rule type is Affected PC SSN (AftPcSsn) , then NSFI is always STOP.

– After all the screening levels are completed, if last NSFI Fails, then message will be discarded.
– After all the screening levels are completed, if last NSFI STOPs, then message will go for further processing in VSTP.

2.31.1.2 Feature Configurations

This section provides procedures to perform the MTP3 screening functionality. MTP3 screen sets and screening rules are configured through MMI and GUI . See MTP Screen Sets and MTP Screening Rules for detailed configuration details.

2.31.2 SCCP Screening

SCCP (Signaling Connection Control Part) includes screening of signalling traffic on the basis of Called and Calling Party Addresses global title using appropriate CGPA (Calling Party Address), CDPA (Called Party Address) GTT (Global Title Translation) Set types, FLOBR (Flexible Origin Based Routing) and GTT actions.

Example Use Cases

- Use incoming linkset to screen messages on the basis of CDPA for SCCP routed Messages

Figure 2-36 Use Case 1

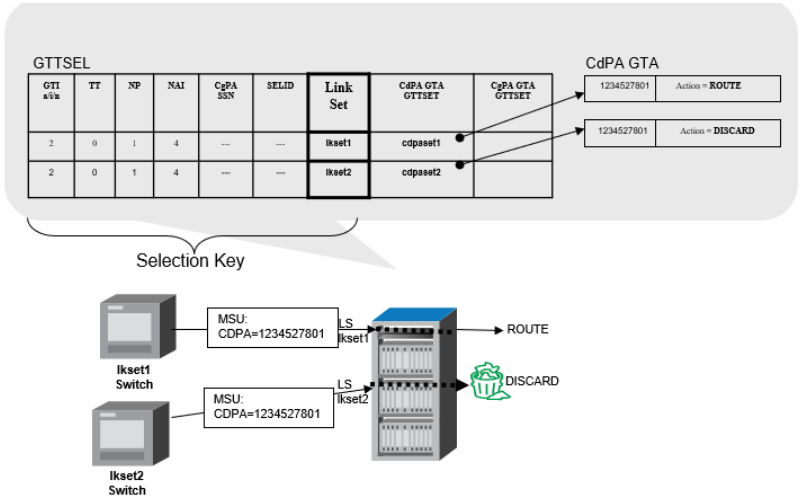


Figure 2-37 Linksets GTT Mode FLOBR_CDPA

Table Description: Link Sets Table

Link Set Name	Local Signaling Point Name	Remote Signaling Point Name	Adapter Type	Reserved Link Transactions Per Second	Maximum Link Transactions Per Second	Routing Context	Threshold of Allowed Links	Threshold of Prohibited Links	MTP Screening Set	MTP Screening Event Logging	MTP Screening Mode
lkset1	Lsp1	Rsp1	M3UA	2000	2000	0	1	1			
lkset2	Lsp1	Rsp2	M3UA	2000	2000	0	1	1			

ITU Transfer Restricted	GTT Mode	Enable Broadcast Exception	Calling Party GT Modification	Application Server Notification	Adjacent SLS 8-bit Indicator	Incoming Rotated Signaling Link Selection (SLS) bit	Random SLS	Rotate SLS by 5 or 8 bits	SLS Conversion Indicator	Rotated SLS Bit	Other CIC Bit	L2 Timer Set Name
No	FLOBR_CDPA	Yes	No	Yes	No	1	Off	No	No	1		Default
No	FLOBR_CDPA	Yes	No	Yes	No	1	Off	No	No	1		Default

L3 Timer Set Name	Security Logging	Link Set Accounting Measurement Option	CGPN BlackList Set	Generic Name Set	SMS Proxy
Default	OFF	No	None	BOTH	Off
Default	OFF	No	None	BOTH	Off

Figure 2-38 GTT Sets

Main Menu: VSTP -> Configuration -> GTT Sets

Wed Mar 15 14:29:05 2023

Filter*

Table Description: GTT Set Table

GTT Set Name	NPSN Name	GTT Set Domain	GTT Set Type	Check Multiple Components
cdpaset1		ITU	CDPAGTA	
cdpaset2		ITU	CDPAGTA	

Allow Segmented XUDT

Figure 2-39 SCCP GTT Selectors

Main Menu: VSTP -> Configuration -> SCCP GTT Selectors

Filter*

Table Description: Sccp GTT Selector Table

GTT Selector Name	CdPA GTT Set Name	CgPA GTT Set Name	CgPA Subsystem Number	Domain Type	Global Title Indicator	GTT Set Name	Linkset Name
cdpasel1	cdpaset1			ITUI	TT_NUM_ENCODING_NATURE		lkset1
cdpasel2	cdpaset2			ITUI	TT_NUM_ENCODING_NATURE		lkset2

CgPA Subsystem Number	Domain Type	Global Title Indicator	GTT Set Name	Linkset Name	Nature of Address Indicator	Nature of Address Indicator Value	Numbering Plan
	ITUI	TT_NUM_ENCODING_NATURE		lkset1	INTERNATIONAL	4	E164
	ITUI	TT_NUM_ENCODING_NATURE		lkset2	INTERNATIONAL	4	E164

Numbering Plan Value	Selector Id	Translation Type
1		0
1		0

Figure 2-40 GTT Actions

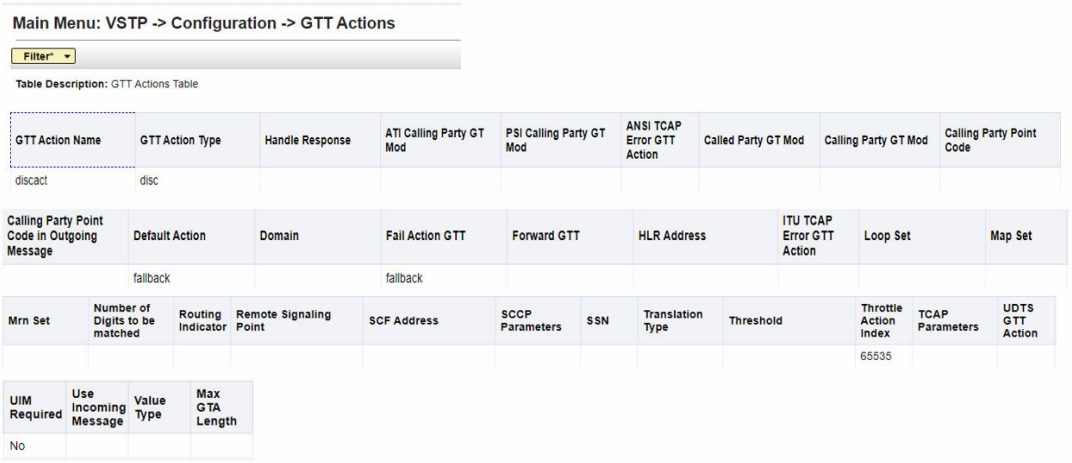


Figure 2-41 GTT Action Sets

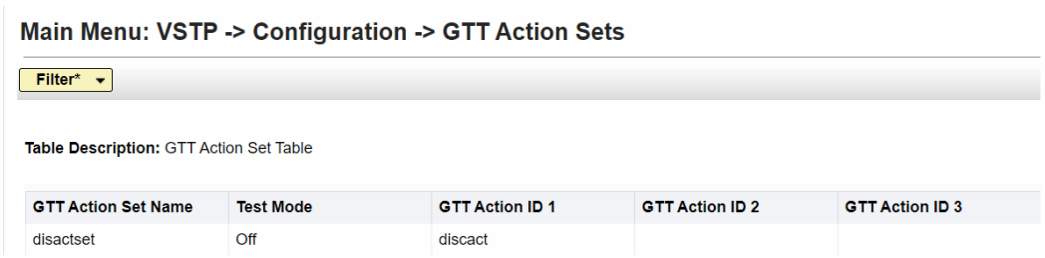
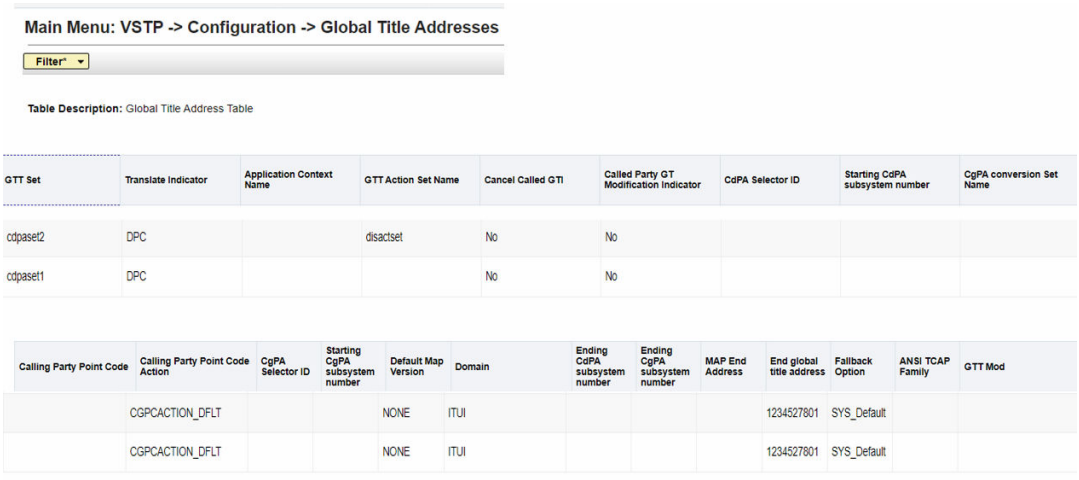


Figure 2-42 Global Title Addresses



- Use incoming linkset to screen messages on the basis of CDPA followed by Opcode translation for SCCP routed Messages.

Figure 2-43 Use case 2

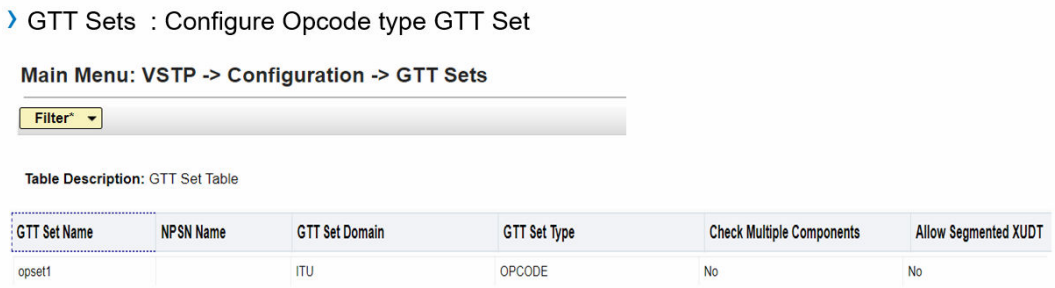


Figure 2-44 Global Title Addresses for opcode set

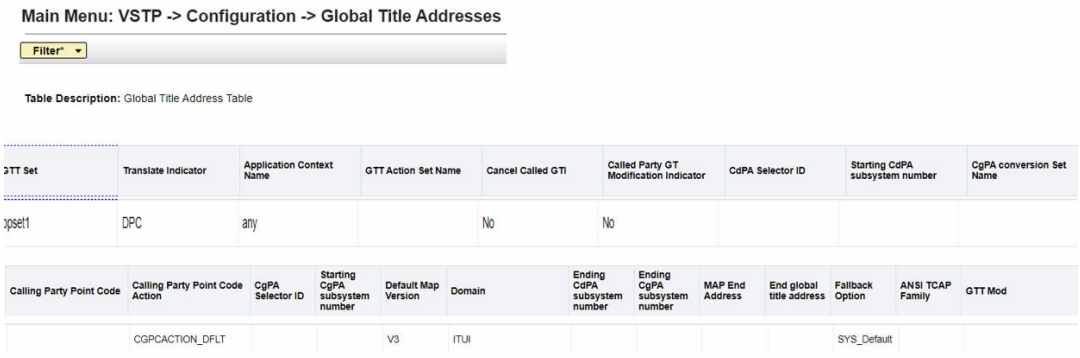


Figure 2-45 Global Title Addresses (Continued)

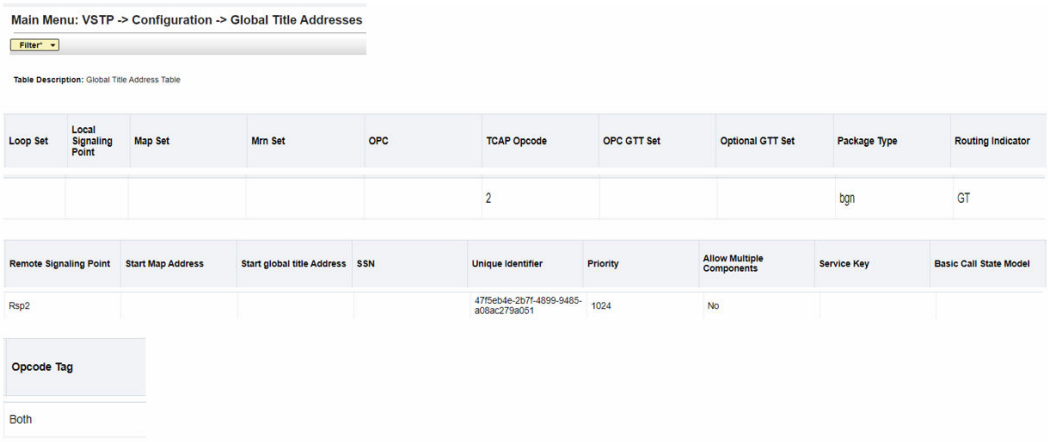
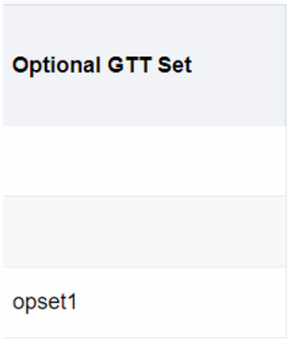


Figure 2-46 Global Title Addresses (continued)

› Configure Optional Set for Opcode to GTA of CDPA set “cdpaset1” configured in slide 11.



- Use incoming linkset to screen messages on the basis of CDPA/CGPA for MTP3 routed Messages.

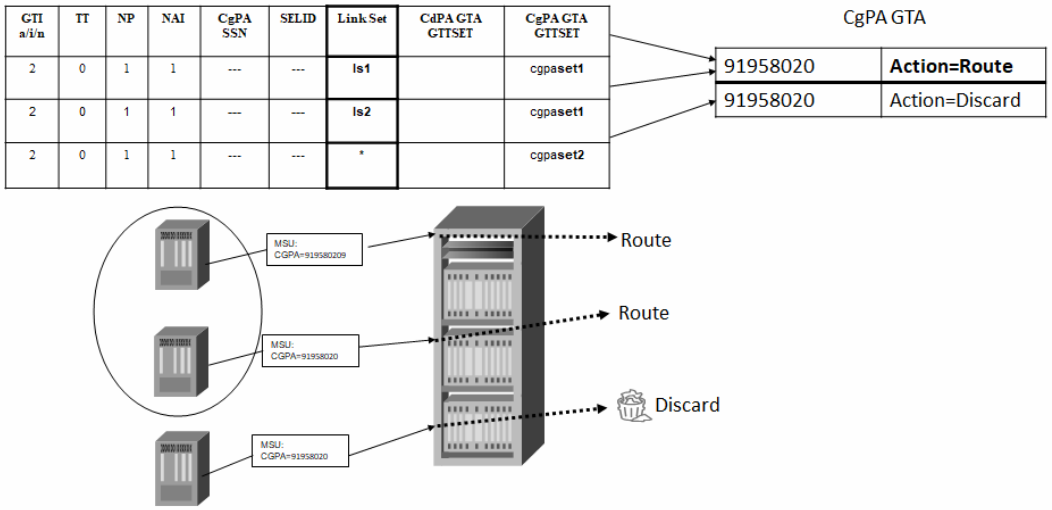
Figure 2-47 Use Case 3

› SCCP Options: MTP Routed GTT is to be set either to Use MTP PC or FULL GTT.

Rest configuration is similar to use case 2. Ensure to add MTP3 Screening Rules on SCCP SIO (Service Information Octet) so that packet reaches SCCP.

- SMS Fraud from an Outside Network

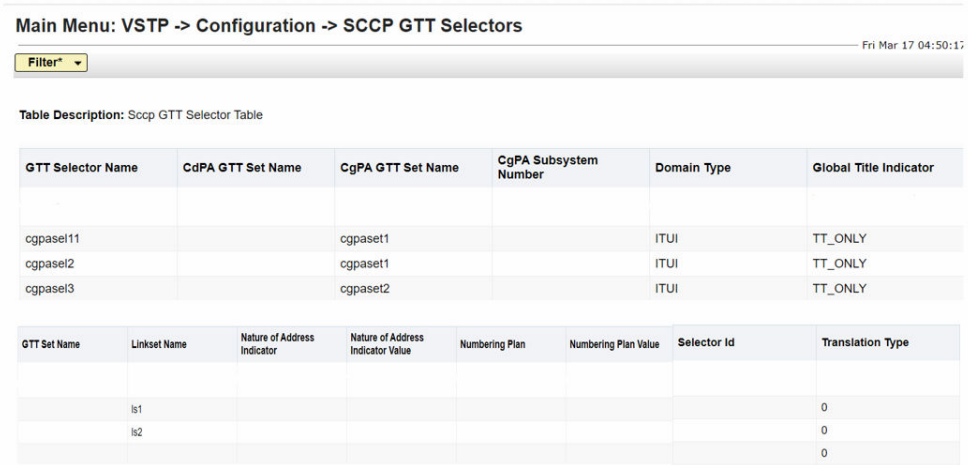
Figure 2-48 Use Case 4



Configure two GTT Sets cgpaset1 and cgpaset2.

- Configure GTT Selectors as follows:

Figure 2-49 SCCP GTT Selectors



Configure GTA (Global Title Address) for cgpaset2 as discard GTT action and GTA for cgpaset1 to be routed to RSP (Remote Signaling Point).

2.32 Cluster Routing Support

The Cluster Routing feature eliminates the need for a full point code (FPC) entry in the routing table to route to every signaling point in every network. The Cluster Routing feature allows the virtual Signaling Transfer Point (vSTP) to configure one routeset to a entire cluster of destinations. This feature also allows the vSTP to manage and switch traffic to more end nodes.

A cluster is defined as a group of signaling points in which point codes have identical values for the network and cluster fields. A cluster entry in the routing table is shown with an asterisk (*) in the member field of the point code, for example: 111-011-* with this feature, an ANSI

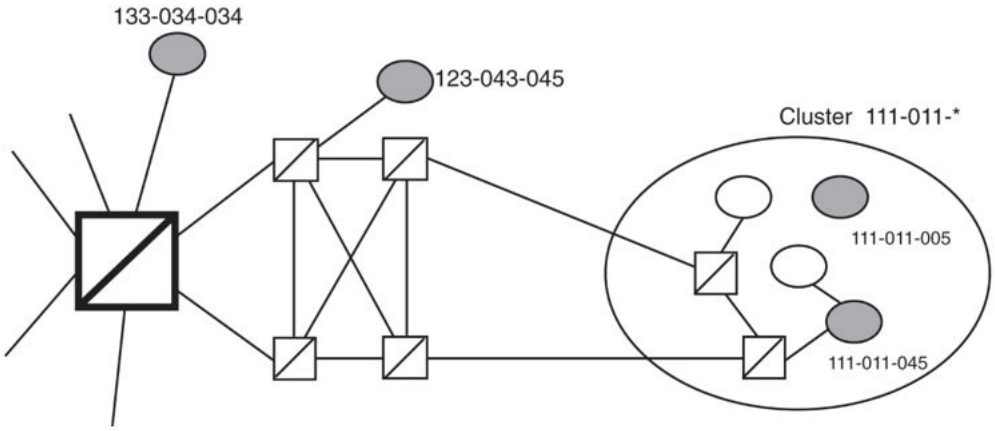
destination point code (DPC) can be specified as either an FPC, example: 123-043-045, or as a cluster of signaling point codes, example: 111-011-*.

By default, Cluster Routing is automatically enabled in vSTP and users cannot disable this feature.

> **Note**
>
> Cluster entries can only be provisioned as ANSI DPCs. Cluster entries cannot be provisioned for ITU international or ITU national DPCs. The ANSI alias point code for an ITU international or ITU national DPC must be an FPC.

The Cluster Routing feature supports provisioning of clusters and FPCs belonging to the same cluster as DPCs as illustrated below. The point codes 111-011-*, 111-011-005, and 111-011-045 entries can be provisioned. In the illustration, the cluster DPC 111-011-* represents all the point codes within the cluster. Cluster entries in the DPC table can also be used as DPCs for routes. A group of such routes with varying relative costs form a routeset to a cluster, similar to a routeset to an FPC.

Figure 2-50 Cluster Routing



Exception Lists (X-lists)

An exception list for a cluster is a list of point codes in a cluster whose routes are more restricted than other routes to that cluster. The term "more restricted" is used when comparing the route status of a cluster member to the route status of the cluster. A prohibited status is more restrictive than a restricted status, and a restricted status is more restrictive than an allowed status.

This list contains point codes that are not assigned to any individual routeset, and the only routeset to that node is through a cluster routeset. The exception list is a dynamic list that changes when the status of the cluster routeset changes.

The vSTP allows users to specify whether exception list entries need to be created on a per cluster basis. For each cluster, the user can specify an ELEI (Exception List Exclusion Indicator) when configuring the cluster point code. When the ELEI is **Yes**, the vSTP does not create Exception List entries or remove any existing exception list entries for the given cluster. When the ELEI is **No**, the vSTP creates and removes exception list entries. When the ELEI is **No**, it is not guaranteed that there will be space available to create each and every possible

exception list entry for provisioned cluster entries. All such exception list entries must compete for available exception list space.

Exception list entries are stored separately from the Remote Signaling Point Code table. Maximum 10,000 exception list entries can be stored.

Exception list entries have an expiration timer. There is a single vSTP wide expiration timer value for exception list entries. The exception list expiration timer and the percentage of occupancy that generates a minor alarm can be configured in M3RL Options MO (Managed Object).

XList Cluster Threshold = the exception list (X-list) occupancy threshold (in terms of percentage of space available). If this threshold is exceeded, the vSTP raises a minor alarm. The percentage of occupancy refers to the number of exception list entries (10000) as compared to the maximum number of entries the exception list can hold. For example: the exception list contains 5000 entries, the percentage of the exception list space used is 50%. If this threshold is exceeded, the vSTP raises a minor alarm.

The vSTP raises a major alarm when the exception list is completely full and the vSTP fails to create any more exception list entries.

An exception List entry's timer is restarted when an exception list entry gets created, updated, or used for routing. This expiration timer (the "XList Expiry Timer Duration" parameter in the M3RL Options MO) can be set from a minimum of 20 minutes to a maximum of 24 hours. The default value upon vSTP startup is 60 minutes. If the timer expires before it is restarted, the exception list entry is removed. The expiration timer allows the vSTP to save resources, if the exception list entry is idle for a long time.

An exception list entry can be created for two distinct set of conditions:

1. The first set of conditions creates exception list entries based on the status of the route (allowed, restricted, or prohibited), and these entries are marked as "XList due to routing".
2. The vSTP creates an exception list entry to maintain the congestion status of a non-provisioned, cluster-routed destination point code. These entries are marked "XList due to congestion".

An exception list entry for a particular cluster can be removed from the exception list when the following conditions are met:

1. Status of all routes to member M change to less or equally restrictive than corresponding status of cluster C's routes. This can happen due to network management message (TFA (Transfer Allowed Signal) or TFR (Transfer Restricted Signal)).
2. Expiry timer for "X-List due to routing" entry of member M expires.
3. When ELEI in Remote Signaling Point MO is changed to **Yes** for the cluster C, vSTP removes all X-List entries created for that cluster.
4. When congestion abates for "X-List due to congestion" entry.

Cluster Routing

When the vSTP receives an MSU to route, the routing function looks for the MSUs Destination Point Code as a FPC entry in the routing table. If found, the FPC entry is used to find the corresponding routeset and the outgoing route. If a FPC entry is not found, the routing function uses the DPCs network and cluster values to find a cluster entry to which the DPC belongs. If found, the cluster entry is used to find the corresponding routeset and the outgoing route. If neither a FPC entry or cluster point code entry is found, the vSTP generates existing "event `mtp3RouteingFailEvent` with reason DPC is not in routing table".

Compatibility with Non-Cluster Routing Nodes

It is possible that not all nodes in the network in which the vSTP is operating in are cluster routing nodes. In such case, the nodes not performing cluster routing will interpret TCx messages, and apply them to each individual point code belonging to the concerned cluster. This may cause an inconsistency in the status records for exception listed point codes in different nodes. In order to avoid such cases, the vSTP performs the following steps:

1. After broadcasting a TCR message for cluster C, vSTP will stop any T8 timers running for X listed members of cluster C and enable response method TFPs for cluster's X listed (prohibited) member point codes by stopping T8. This will allow sending of TFPs for prohibited members immediately after a TCR is broadcast.
2. After broadcasting a TCA message for cluster C, vSTP enables one-time response method TFR for cluster's X listed (restricted) member point codes by stopping T18 and enables response method TFPs for cluster's X listed (prohibited) member point codes by stopping T8. This allows TFPs for prohibited members and TFRs for restricted members to be sent immediately after a TCA is broadcast.

Cluster Management and the ITU Network

ITU SS7 networks lack concept of clusters of point codes and cluster network management messages. vSTP does not generate TCX messages towards ITU nodes. When vSTP is acting as gateway STP between a ITU network and ANSI network, during the broadcast phase of TCX messages, vSTP does not send TCX messages to adjacent ITU point codes. Message loss may occur in such cases. To reduce message loss and quickly notify the sender ITU node about the status, vSTP enables response method messages immediately (without T8 or T18) and relies on response method to convey the status information. While sending response method network management messages in response to a received MSU, vSTP will check MSUs OPC. If MSUs OPC is a ITU point code, always a TFX message will be returned.

Protocol features non preferred options:

- vSTP will respond with a TFP (Transfer Prohibited Signal), when a message is received for a inaccessible member and corresponding cluster does not exist.
- Upon receiving a TCR (Transfer Cluster Restricted Signal) message concerning cluster for which no cluster is provisioned, vSTP will mark all individually provisioned members as restricted and start RSR procedure for them.
- Upon receiving a TCP (Transfer Cluster Prohibited Signal) message concerning cluster for which no cluster is provisioned, vSTP will mark all individually provisioned members as prohibited and start RSP (RouteSet Prohibited) procedure for them.
- vSTP will stop T8 and T18 timers for prohibited and restricted member of the clusters after broadcasting a TCA for cluster. These members can be X listed point codes or full point code.
- vSTP will stop T8 timers for prohibited member of the clusters after broadcasting a TCR. These members can be X listed point codes or full point code.

Cluster Routing Rules

These rules apply to the Cluster Routing feature:

- If the provisioned number of exception list entries (10000) are already created, the vSTP will not create any more exception list entries. The vSTP raises an alarm in advance of such an occurrence, and logs each occurrence of failure to create an exception list entry.
- All adjacent point codes for linksets must be full point codes.

- When vSTP is used as an ITU ANSI gateway STP:
  - vSTP does not broadcast phase TCX procedures towards ITU nodes. This introduces possibility of message loss until response method kicks in. It is recommended that cluster routing is not used when acting as a gateway STP.
  - Cluster destination will not be allowed to have ITU alias point codes.
- All ANSI alias point codes specified for real ITU point codes are required to be full point codes.
- Point code specified in SCCP MapSet/MrnSet must have a Full point code entry in the routing table.
- Point code specified in GTA (Global Title Address) must be a full point code only. It may have FPC or cluster route.
- To configure unprovisioned member of provisioned cluster in GTA RSP, select cluster Rsp in RSP and then give the unprovisioned point code in newly added parameter “FullRspPc”.
- Point code specified in GTT Action must be full point code only. It may have FPC or cluster route. To configure unprovisioned member of provisioned cluster in Gtt Action RSP, select cluster RSP in RSP and then give unprovisioned point code in newly added parameter “FullRspPc”.
- In GTA MO, OPC and Calling Party Point Code can be Cluster Point Code.
- vSTP allows cluster routing for subsequent global title (GTT) messages.
- vSTP sends subsystem status messages to the concerned point codes using cluster routes.
- vSTP does not generate MTP status message for point codes using cluster routing. Hence all MAP table point codes must be full point code entries.
- The FiltPC in a PCT translation can be a cluster point code for ANSI domain.
- If a point code is in the routing table as an exception-listed (X-listed) member and the user provisions the same point code as a full point code, the X-listed entry is deleted. A new full point code entry is created, inheriting cluster’s route status.
- When a cluster destination point code is removed from the vSTPs database, all related exception-listed(XList) point codes of that cluster are removed.
- Due to the requirement of same routeset for cluster and its members, once a cluster and FPC members are provisioned in vSTPs Remote SP and Route MO, all routes must be deleted before a full point code member or a cluster can be removed. otherwise, entire cluster will be inaccessible before a member can be removed from Remote Signaling Point MO.
- The route assigned to a full point code DPC cannot be deleted directly from the Route Table if that DPC is a member of a cluster point code defined in Remote Signaling Point Table.
- if a route assigned to a cluster point is deleted from the route table, the same or corresponding inherited routes of all members of that cluster are also deleted from the Route Table.
- The cluster and its provisioned members must have the same routeset. Hence, if a cluster exists only cluster routes can be added or modified.
- If member routes exist, a newly added cluster inherits member routes. If cluster route exists, a newly added full point code member inherits all cluster routes.

Protocol features non preferred options:

- vSTP responds with a TFP (Transfer Prohibited Signal), when a message is received for an inaccessible member and the corresponding cluster does not exist.
- Upon receiving a TCR (Transfer Cluster Restricted Signal) message concerning cluster for which no cluster is provisioned, vSTP marks all individually provisioned members as restricted and start RSR procedure for them.
- Upon receiving a TCP (Transfer Cluster Prohibited Signal) message concerning cluster for which no cluster is provisioned, vSTP will mark all individually provisioned members as prohibited and start RSP (RouteSet Prohibited) procedure for them.
- vSTP stops T8 and T18 timers for prohibited and restricted member of the clusters after broadcasting a TCA for the cluster. These members can be X listed point codes or full point code.
- vSTP stops T8 timers for prohibited member of the clusters after broadcasting a TCR. These members can be X-listed point codes or full point code.

Home Cluster

A home cluster is a provisioned cluster point code to which vSTP itself is a member. example, if vSTPs true point code or any capability point code is 1-1-1 and a cluster 1-1-* is provisioned then 1-1-* is considered a home cluster.

Provisioning a home cluster causes a profound impact on network management regarding the home cluster and its members. These impacts are identified below:

- Ignore messages from X concerning cluster to which X belongs to.
- Send only TCA for Home Cluster for RCX.
- Send only individual TFP/TFR for the home cluster in response for message received for routing to inaccessible or restricted destination.
- As vSTP is an accessible member of the home cluster, it will not transmit TCP or TCR messages regarding the home cluster, except for the following::
  - Broadcast TCP: when cluster (except vSTP itself) becomes inaccessible.
  - Broadcast TCR: vSTP will stop T8 for all the members.
  - Preventive TCP: when starting to route to the cluster through an adjacent node.
- If individual full point code members are provisioned for the home cluster, vSTP will generate network management messages for these full point code.
- When the home cluster is inaccessible, vSTP will generate one response TFP per T8 timer for members of the home cluster. If vSTP continues to receive traffic for the home cluster, eit will eventually send TFP responses for all members of the cluster.
  All above impacts may compromise network management reliability for the home cluster and its members.

2.32.1 Feature Configuration Cluster Routing Support

This section provides procedures for enabling Cluster Routing functionality.

Cluster Routing is configured using the vSTP managed objects and vSTP GUI. The MMI API includes details about the URI, examples, and parameters for each managed object.

2.32.1.1 GUI Configuration Cluster Routing Support

The Cluster Routing Support can be configured from active SOAM. Select **vSTP** and select **Configuration** page.

The following parameters are used to perform the configuration:

- Full RSP Point Code: This parameter is used when a network PC or cluster is configured as a remote signaling point. For more information see, Global Title Addresses and GTT Actions.
- Exception List Exclusion Indicator: Applicable only for Cluster Point Codes. For more information see, Remote Signaling Point.
- Nested Cluster Allowed Indicator: This parameter specifies whether the route to the cluster point code can be different for provisioned members of the cluster. For more information see, Remote Signaling Point.
- XList Expiry Timer Duration: This parameter sets the timer for X-list when created, updated or used for routing. For more information see, M3rl Options.
- XList Cluster Threshold: This parameter sets the threshold, represented as a percentage. For more information see, M3rl Options.

2.32.1.2 MMI Managed Objects for Cluster Routing

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

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

The following table lists the managed objects and operations supported for Cluster Routing feature:

Table 2-42 Managed Objects Global Title Address

Managed Object, Name	Supported Actions	URI
Global Title Address	GET	/vstp/globaltitleaddresses/
Global Title Address	POST	//vstp/globaltitleaddresses/ -v POST -r gta.json
Global Title Address	PUT	/vstp/globaltitleaddresses/ -v PUT -r gta.json
Global Title Address	DELETE	/vstp/globaltitleaddresses/ <GTA> -v DELETE

Global Title Address - POST

Create a json file with following content.

```
{
        "ccgt": false,
        "cgGtmod": false,
        "cgpcaction": "Dflt",
        "configurationLevel": "60",
        "endAddress": "556",
        "fallback": "Sysdflt",
        "fullRspPcStr": "008-003-004",
        "gttSetName": "gttset1",
        "opcodeTag": "Both",
```

```
        "routingIndicator": "Gt",
        "rspName": "CPC830",
        "startAddress": "556",
        "translateIndicator": "Dpc"
    }
```

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

```
mmiclient.py /vstp/globaltitleaddresses/ –v POST –r /<Absolute path>/<File
Name>
```

Global Title Address - Get

Create a json file with the following content:

```
{
    "data":  {
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "configurationLevel": "181",
            "endAddress": "556",
            "fallback": "Sysdflt",
            "fullRspPcStr": "008-003-004",
            "gttSetName": "gttset1",
            "opcodeTag": "Both",
            "routingIndicator": "Gt",
            "rspName": "CPC830",
            "startAddress": "556",
            "translateIndicator": "Dpc",
            "uniqueIdentifier": "d1d90b1f-540d-4ddc-87b6-4d8b04a4daa9"
        },
    "links": {},
    "messages": [],
    "status": true
}
```

Global Title Address - PUT

Create a json file with updated Full RSP Point Code .

```
 {
            "ccgt": false,
            "cgGtmod": false,
            "cgpcaction": "Dflt",
            "configurationLevel": "181",
            "endAddress": "556",
            "fallback": "Sysdflt",
            "fullRspPcStr": "008-003-005",
            "gttSetName": "gttset1",
            "opcodeTag": "Both",
            "routingIndicator": "Gt",
            "rspName": "CPC830",
            "startAddress": "556",
```

```
            "translateIndicator": "Dpc",
            "uniqueIdentifier": "d1d90b1f-540d-4ddc-87b6-4d8b04a4daa9"
        }
```

Run the following command on active SOAM to update Global Title Address :

```
mmiclient.py /vstp/globaltitleaddresses/ -v PUT -r /<Absolute  Path>/<File
Name>
```

Global Title Address - Delete

Global Title Address - Delete

Run the following command on active SOAM to delete Global Title Address:

```
mmiclient.py /vstp/globaltitleaddresses/{name} -v DELETE
```

Table 2-43 Managed Objects Remote Signaling Point

Managed Object, Name	Supported Actions	URI
Remote SP	GET	/vstp/remotesignalingpoints/
Remote SP	POST	/vstp/remotesignalingpoints/ -v POST -r rsp.json
Remote SP	PUT	/vstp/remotesignalingpoints/ -v PUT -r rsp.json
Remote SP	DELETE	/vstp/remotesignalingpoints/ <RSPID> -v DELETE

Remote SP - POST

Create a json file with following content.

```
{
        "elei": "No",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
        "udtxudtcnv": "NOCONV"
    }
```

Run the following command on active SOAM to insert the Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints –v POST –r /<Absolute path>/<File
Name>
```

Remote SP - Get

Create a json file with the following content:

```
{
    "data": {
        "configurationLevel": "179",
        "elei": "No",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
        "udtxudtcnv": "NOCONV"
    },
   "links": {},
   "messages": [],
    "status": true
}
```

Remote SP - PUT

Create a json file with updated ELEI.

```
 {
        "elei": "Yes",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
        "udtxudtcnv": "NOCONV"
    }
```

Run the following command on active SOAM to update Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints/ -v PUT -r /<Absolute  Path>/<File
Name>
```

Remote SP - Delete

Run the following command on active SOAM to delete Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints/{name} -v DELETE
```

Table 2-44 Managed Objects GTT Actions

Managed Object, Name	Supported Actions	URI
GTT Action	GET	/vstp/remotesignalingpoints/
GTT Action	POST	/vstp/remotesignalingpoints/ -v POST -r rsp.json
GTT Action	PUT	/vstp/remotesignalingpoints/ -v PUT -r rsp.json
GTT Action	DELETE	/vstp/remotesignalingpoints/ <RSPID> -v DELETE

GTT Action - POST

Create a json file with following content.

```
{
            "act": "Dup",
            "actid": "gttact2",
            "cgpcogmsg": "Dflt",
            "fullRspPcStr": "003-003-003",
            "handlresp": "No",
            "ri": "Gt",
            "rspName": "CPC330",
            "ssn": 4,
            "useicmsg": false
        }
```

Run the following command on active SOAM to insert the GTT Action:

```
mmiclient.py /vstp/gttactions/ –v POST –r /<Absolute path>/<File Name>
```

GTT Action - Get

Create a json file with the following content:

```
{
    "data":  {
            "act": "Dup",
            "actid": "gttact2",
            "cgpcogmsg": "Dflt",
            "fullRspPcStr": "003-003-003",
            "handlresp": "No",
            "ri": "Gt",
            "rspName": "CPC330",
            "ssn": 4,
            "useicmsg": false
        },
     "links": {},
    "messages": [],
    "status": true
}
```

GTT Action - PUT

Create a json file with updated Full RSP Point Code .

```
{
            "act": "Dup",
            "actid": "gttact2",
            "cgpcogmsg": "Dflt",
            "fullRspPcStr": "003-003-004",
            "handlresp": "No",
            "ri": "Gt",
            "rspName": "CPC330",
            "ssn": 4,
            "useicmsg": false
        }
```

Run the following command on active SOAM to update GTT Action:

```
mmiclient.py /vstp/gttactions/ -v PUT -r /<Absolute  Path>/<File Name>
```

GTT Action - Delete

Run the following command on active SOAM to delete GTT Action:

```
mmiclient.py /vstp/gttactions/{name} -v DELETE
```

Table 2-45 Managed Objects M3rl Options

Managed Object, Name	Supported Actions	URI
GTT Action	GET	/vstp/m3rloptions/
GTT Action	PUT	

M3rl Options - Get

Create a json file with the following content:

```
{
   "data": {
       "ProxyPcSupport": "On",
       "cncfSupport": "Off",
       "cnvAInat": 1,
       "cnvCgda": false,
       "cnvCgdi": false,
       "cnvCgdn": false,
       "cnvCgdn24": false,
       "cnvClgItu": "Off",
       "gtCnvDflt": false,
       "islsbrEnabled": false,
       "m2paSctpRxbusyLink": "Off",
       "pct": "On",
       "performanceMeasurement": "Off",
       "randsls": "Off",
       "slsRotation": true,
       "slscnv": "Off",
```

```
            "slsocbEnabled": false,
            "slsreplace": false,
            "sparePCSupportEnabled": true,
            "ttMapSupport": "Off",
            "xListClusterThreshold": 90,
            "xListExpiryTimerDuration": 60
        },
        "links": {
            "update": {
                "action": "PUT",
                "description": "Update this item.",
                "href": "/mmi/dsr/v4.6/vstp/m3rloptions/",
                "type": "status"
            }
        },
        "messages": [],
        "status": true
}
```

M3rl Options - PUT

Create a json file with updated Cluster X list Expiry Timer Duration and Cluster X list Threshold.

```
{
          "xListClusterThreshold": 80,
        "xListExpiryTimerDuration": 70
}
```

Run the following command on active SOAM to update M3rl Options :

```
mmiclient.py /vstp/m3rloptions/ -v PUT -r /<Absolute  Path>/<File Name>
```

2.32.1.3 Alarms/Events and Measurements Cluster Routing Support

The following table lists the Alarms and Events specific to the Cluster Routing:

Table 2-46 Alarms

Alarm Name	Alarm Number	Alarm Type	Alarm Description
VSTP M3RL XList Buffer Utilization	70486	Major	The percent utilization of the vSTP MPs M3RL XList buffer is approaching its maximum capacity.
Vstp XList Space utilization Threshold Crossed	70487	Major	The percent utilization of the Total vSTP XList space available is approaching its maximum capacity.
Vstp Maximum Allowed XList Entries Configured.	70488	Major	The vSTP X-list dynamic table is full.

The following table lists the sysmetric defined similar to `VstpM3rlRspBuffer` for X-List which is called `VstpM3rlXListBuffer`.

Table 2-47 Metrics

Metric Id	Alarm Type	Set Threshold	Clear Threshold
VstpM3rlXListBuffer	Minor	60	50
VstpM3rlXListBuffer	Major	80	70
VstpM3rlXListBuffer	Critical	95	90

There are 7 events required, using new formats, to support the Cluster Routing feature. vSTP will generate these events upon expiration of X-list entries, upon reception of TCA/TCR/TCP and upon reception of invalid TFA/TFR messages.

The following table lists the events that support the Cluster Routing:

Table 2-48 Events

Event Reason	Event Number	New Format?	Name	Comments
X-list entry expired	70489	Yes	xListEntryExpired	X-list entry was removed as it was not used to switch traffic or changed.
TCP Received	70483	Yes	Mtp3TcpReceived	When TCP message received by MTP3 layer.
TCR Received	70485	Yes	Mtp3TcrReceived	When TCR message received by MTP3 layer.
TCA Received	70484	Yes	Mtp3TcaReceived	When TCA message received by MTP3 layer.
Unexpected TFA received	70379	No, already exist	unexpectedTfaReceived	A TFA is received for non-provisioned member (DPC) of a provisioned and prohibited/ restricted cluster.
Unexpected TFR received	70380	No, already exist	unexpectedTfrReceived	A TFR is received for non-provisioned member of a prohibited cluster.
Unexpected TFP received	70381	No, already exist	unexpectedTfpReceived	When Duplicate TFP is received for provisioned member of cluster.

Table 2-49 Measurements

Measurement Number	Measurement Name	Measurement Group	Interval	Measurement type
22350	VstpXListDiscardDueElei	VSTP MTP3 Exception	5mins	Single
22351	VstpXListCreationFailed	VSTP MTP3 Exception	5mins	Single
22352	VstpM3rlXListBufferPeak	VSTP X List Buffer	5mins	Arrayed Max
22353	VstpM3rlXListBufferAvg	VSTP X List Buffer	5mins	Arrayed Avg
22354	VstpM3rlXListBufferOverflow	VSTP MTP3 Exception	5mins	Arrayed Simple

2.33 Nested Cluster Routing

When a node switches traffic to remote (non-adjacent) nodes, it is possible for STP to use at least one route that differs from the other members of a cluster. This typically occurs when the node is directly connected to the member of a cluster. The nested cluster routing feature provides a mechanism that enables both cluster and member routes to be provisioned within the same cluster.

Nested Clusters and Cluster Members

The cluster routing feature requires that routes to a cluster and members of that cluster be in the same routeset. However, with the nested cluster routing feature, users can have certain members of the provisioned cluster with different full point code routesets. These routesets may be entirely different, partially different, or identical.

With this feature, routes to these members can be modified, removed, or added. Removing a full point code route entry within a cluster will result in the member using the cluster entry for routing. Deletion of a cluster route entry will not delete the full point code route entry. even if they share the same route.

The **vSTP** sends cluster network management messages (TCA, TCR, and TCP) based on the least restrictive status of the cluster's routeset, and any full point code entries within the cluster.

The nested cluster routing feature provides a new routing model. vSTP supports multiple routing models. The below table describes coupling between a cluster and its members. Coupling defines the relationship between the cluster and member routes.

Table 2-50 Routing Models

vSTP Routing Model	Characteristics	Issues and Resolution
Full Point Code Routing (FPR) No coupling	vSTP will behave as an FPC router when only FPC destinations are provisioned. vSTP will never generate TCX messages concerning clusters of provisioned members. Received TCX messages are applied to all members of the concerned cluster.	No issues. There is no coupling between cluster status and member status due to the lack of clusters.
Cluster Routing and Management Diversity (CRMD) Full coupling NCAI=No	In this mode, vSTP allows provisioning of clusters as well as members of same clusters. Here cluster and member have the same route set and they are fully coupled. All TCX messages are applied to members and TCX messages generated by vSTP reflect member status. In this mode, member status cannot be less restrictive than cluster.	No issues regarding network management message generation and processing. Cluster and members cannot have different route set.
Nested Cluster Routing No coupling NCAI=Yes	In this mode, the NCAI parameter is specified as "Yes" for cluster. The user can enter a cluster route set, then enter a different route set for a member of that cluster. In this case, member route set status can be less restricted than cluster route set status. There is an issue concerning the broadcast of (TCA, TCR, TCP) and the preventive TCP generation.	There is an issue regarding broadcasting network management messages. As members can be less restricted than the cluster, broadcast of cluster messages (TCA, TCR, TCP) is based on the least restrictive of the following: • The cluster’s route set status. • The route set status of any Full Point Code entries within the cluster. Also, when if NCAI is Yes, vSTP will not generate preventive TCPs.

Administration

The Nested Cluster Routing feature is provisioned using the NCAI parameter in Remote Signaling Point Managed Object. The NCAI parameter can only be specified for cluster point codes.

If the NCAI parameter is yes, the vSTP allows a certain members of the provisioned cluster to have a different full point code routeset.

If the NCAI parameter is **No**, standard rules apply (any full point code routeset within a cluster must have the same routeset as the cluster). If NCAI parameter is **yes**, new rules apply (full point code routeset can differ from the cluster routeset). The following illustration provides an example of provisioning a nested cluster and its associated members.

Figure 2-51 Nested Cluster

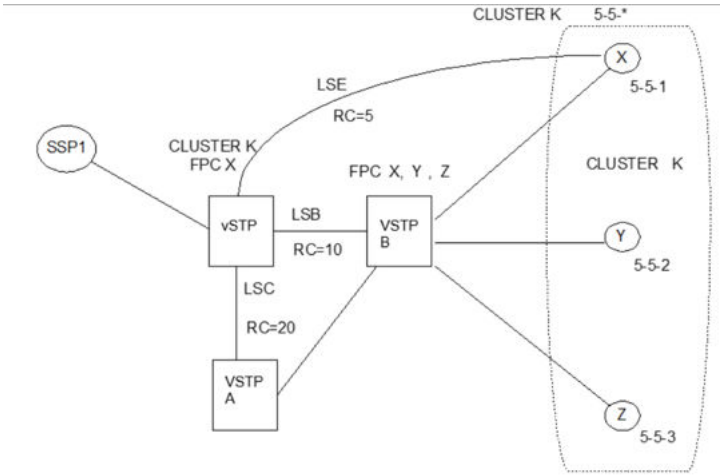


Table 2-51 Nested Cluster K Route Table (5-5-*)

Point Code	Linkset	Route Cost
5-5-*	LSB	10
5-5-*	LSC	20

Table 2-52 FPC Member X Route Table (5-5-1)

Point Code	Linkset	Route Cost
5-5-1	LSE	5
5-5-1	LSB	10
5-5-1	LSC	20

Table 2-53 Examples of Nested Cluster Routing Failure and Recovery Actions

Event	Action
All link sets are up and all routes are available	vSTP will not send preventive TCP (K) to vSTP-B as K is a nested cluster, start routing messages to X using LSE and K using LSB. vSTP will broadcast TCA (K) to SSP1, SSP-X, vSTP-A, and vSTP-B.
Link set between vSTP-B and SSP-Y (5-5-2) fails, vSTP-B sends a TFP (Y)	vSTP will create a (5-5-2) X-list entry and mark it to Prohibited on LSB. vSTP will broadcast TFP to SSP1, SSP-X and vSTP and sends response method TFP concerning 5-5-2 (Rule #3). vSTP will start RSP for Y on LSB.
Link set between vSTP-B and SSP-X (5-5-1) fails, vSTP-B sends a TFP (X) to vSTP	vSTP will mark FPC 5-5-1 to PROHIBITED on LSB, vSTP routes the traffic to X through LSE, vSTP will start RSP for X on LSB.
Link set between vSTP-B and SSP-Y (5-5-2) recovers and vSTP-B sends a TFA (Y) to vSTP.	vSTP will remove (5-5-2) X-list entry prohibited status on LSB, performs rerouting and start routing traffic to SSP-Y through LSB. vSTP will broadcast TFA (Y) to SSP1, SSP-X and vSTP-A. vSTP sends a preventive TFP (Y) to vSTP-B
Link set between vSTP-B and SSP-X (5-5-1) recovers and vSTP-B sends a TFA (X) to vSTP	vSTP will mark FPC 5-5-1 to allowed status on LSB.
LSB fails	vSTP will stop using LSB to send traffic to cluster K, mark Prohibited on LSB, perform forced rerouting, start T11 (K) and start using LSC to switch messages to K.
SSP1 sends an MSU with DPC=Y	MSU will be routed on LSC.
SSP1 sends an MSU with DPC=X	vSTP will route MSU to SSP-X using LSE.
LSB recovers	vSTP will stop using LSC to send traffic to cluster K, performs controlling rerouting on K, and mark cluster K as Allowed on LSB, starts routing traffic to cluster K through LSB.
SSP sends a route set test (RSR) concerning Y to vSTP	vSTP responds with a TFA (Y).
LSC fails.	vSTP will stop using LSC to send traffic to cluster K or FPC X and mark K and FPC X Prohibited on LSC.
LSC recovers.	vSTP will mark cluster K and FPC X Allowed on LSC.
LSE fails.	vSTP will stop using LSE to send traffic to SSP-X, marks Prohibited on LSE, perform forced rerouting, send preventive TFP (X) to vSTP-B and start using LSB to switch messages to FPC X.
SSP1 sends an MSU with DPC=SSP-Y	vSTP will route MSU to SSP-Y using LSB.
SSP1 sends an MSU with DPC=SSP-X	MSU will be routed to SSP-X using LSB.
LSE recovers.	vSTP will stop using LSB to send traffic to SSP-X, perform controlling rerouting on FPC X and mark FPC X as Allowed on LSE, start routing traffic to FPC X through LSE. vSTP broadcast TFA (X) to SSP1, vSTP-A, and vSTP-B.

Limitations

- vSTP supports a maximum of 500 nested cluster destinations.

  > **Note**
  >
  > This limit does not apply to non-nested clusters (clusters with NCAI=NO).

- If a cluster is more restrictive than one member, vSTP will broadcast status of the least restricted member and rely on response method for members of the cluster that do not have a full point code entry.

- vSTP does not broadcast preventive TCPs for nested cluster destinations. As vSTP will not send preventive TCPs when it begins routing towards a nested cluster, circular routing can occur. When routing begins toward a nested cluster, circular routing may occur. However, vSTP sends response method TFPs if it receives an MSU when there is a risk of circular routing.

2.33.1 Feature Configuration Nested Cluster Routing

This section provides procedures to perform the Nested Cluster Routing functionality.

The Nested Cluster routing is configured using the vSTP managed objects and vSTP GUI. The MMI API includes details about the URI, examples, and the parameters for each managed object.

2.33.1.1 GUI Configuration Nested Cluster Routing

The Nested Cluster Routing can be configured from active System OAM (SOAM). Select **VSTP**, and then **Configuration** page.

The following parameter on the **Remote Signaling Point** is used to perform the configuration:

- `Nested cluster allowed indicator`: This parameter specifies if the route to the cluster point code can vary for provisioned cluster members. A point code is a member of a cluster point code if it shares the same network identifier (NI) and network cluster (NC) values. Specify this parameter exclusively for cluster point codes.

For more information see Remote Signaling Point.

2.33.1.2 MMI Managed Objects for Nested Cluster Routing

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

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

The following table lists the managed objects and operations supported for Nested Cluster Routing feature:

Table 2-54 Managed Objects Remote Signaling Point

Managed Object, Name	Supported Actions	URI
Remote SP	GET	/vstp/remotesignalingpoints/
Remote SP	POST	/vstp/remotesignalingpoints/ -v POST -r rsp.json
Remote SP	PUT	/vstp/remotesignalingpoints/ -v PUT -r rsp.json
Remote SP	DELETE	/vstp/remotesignalingpoints/ <RSPID> -v DELETE

Remote SP - POST

Create a json file with following content.

```
{
        "elei": "No",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
```

```
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
        "udtxudtcnv": "NOCONV"
    }
```

Run the following command on active SOAM to insert the Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints –v POST –r /<Absolute path>/<File
Name>
```

Remote SP - Get

Create a json file with the following content:

```
{
    "data": {
        "configurationLevel": "179",
        "elei": "No",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
        "udtxudtcnv": "NOCONV"
    },
   "links": {},
   "messages": [],
    "status": true
}
```

Remote SP -PUT

Create a json file with updated ELEI.

```
 {
        "elei": "Yes",
        "enableBroadcastException": false,
        "mtpPointCode": "009-013-*",
        "name": "DUMMY",
        "ncai": "No",
        "nprst": "Off",
        "prx": "No",
        "rcause": "None",
        "splitiam": "None",
        "ss7DomainType": "Ansi",
```

```
    "udtxudtcnv": "NOCONV"
}
```

Run the following command on active SOAM to update Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints/ -v PUT -r /<Absolute  Path>/<File
Name>
```

Remote SP - Delete

Run the following command on active SOAM to delete Remote SP:

```
mmiclient.py /vstp/remotesignalingpoints/{name} -v DELETE
```

2.34 Network Routing

Network Routing allows the user to provision a single routeset which can be used for all MSUs destined to members of that specific network.

Network Routing Advantages:

- Reduces the number of entries in the route table.
- Enables routing to members of a network without having to add those members to the route table.

A vSTP user can connect to a remote network by provisioning a single route table element. As the remote network grows, the user need not add new route table entries for each new point code in the remote network.

> **Note**
>
> Network Routing can be used only with ANSI point codes. A Network Routing point code cannot be provisioned as a proxy point code.

Routing Strategy Types

vSTP currently supports three routing strategy types:

- Full point code routing.
- Cluster Routing
- Network Routing.

Network Routing allows the user to provision a third type of routing strategy. It is possible to provision full point code entries, cluster entries, and network entries for members of the same network. Any overlaps in the routing strategies are handled by a specific searching hierarchy.

The following route table entries can coexist:

- 8-1-1 – Full point code entry
- 8-1-* – Cluster entry
- 8-*-* – Network entry

The searching hierarchy tries to match against a full point code entry first, followed by a cluster entry, and finally a network entry. In the following example:

when the **vSTP** routes an **MSU** destined for 8-1-1, it uses the full point code entry.

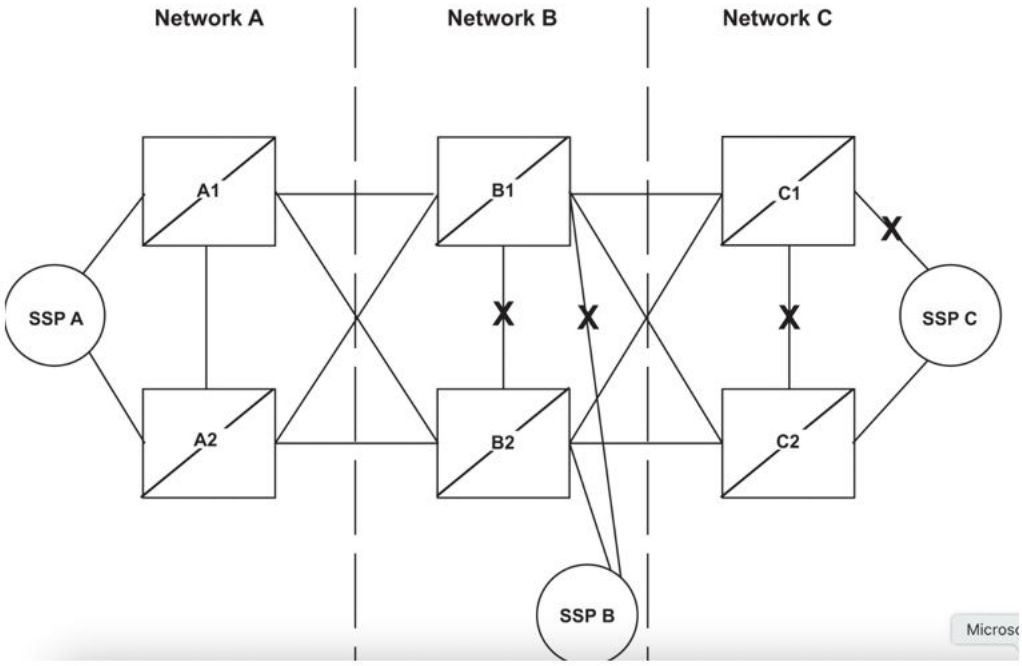
when the **vSTP** routes an **MSU** destined for 8-1-2 it uses the cluster entry.

when the **vSTP** routes an **MSU** destined for 8-2-2, it uses the network entry.

Applications

Network routing is beneficial when the destination node is distant from the source node. The reliability of network routing increases when the destination is further away. In the below illustration, routing from network A is more reliable to nodes in network C than to nodes in network B.

Figure 2-52 Applications



If the nodes in network A use network routing for network C, network A can still route traffic to **SSP** C, even if two linksets fail. In this example, one of the linksets to **SSP** C and the linkset between node C1 and node C2 fail. In this case, the vSTP in network A continues to route half of its traffic to node B1, and half to node B2. Node B1 and node B2 (which do not use network routing) route all traffic to **SSP** C through node C2.

If the nodes in network A use network routing for network B, traffic routed to **SSP** B may be lost if two linksets fail. In this example, one of the linksets to **SSP** B and the linkset between node B1 and node B2 fail. In this case, the vSTP in network A continues to route half of its traffic to node B1, and half to node B2. Traffic for SSP B routed through node B1 is discarded, resulting in message loss.

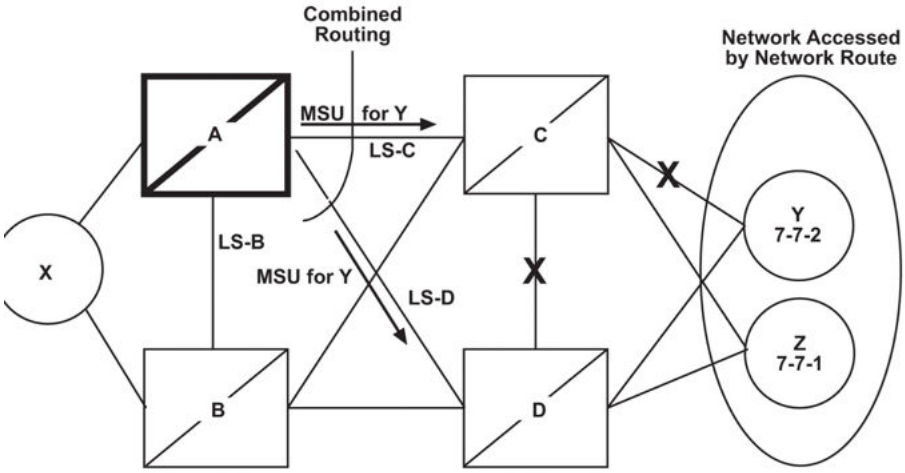
Route Availability

A route is one path to a destination. A routeset is a list of paths to a destination. Route availability consists of two parts:

- Local availability
- Remote availability

Remote availability is affected by TFx network management messages. Local availability is affected by linkset failures and recoveries. TFx messages do not affect point codes accessed by network route entries. Therefore, for network route entries, route availability consists of only local availability. The highest priority linkset available for traffic is used for routing MSUs, regardless of the remote availability of that route.

Figure 2-53 Route Availability



In the above illustration, linksets **LS**-C and **LS**-D form a combined route to network route 7-*-*. It is because 7-*-* is a network route, the vSTP always considers the non-adjacent status of the routes to be allowed. In the example shown, the vSTP routes traffic destined to 7-7-1 over **LS**-C and **LS**-D. The vSTP ignores **TFP**s concerning 7-7-1 or **TCP**s concerning 7-7-*.

Point Code Availability

A point code that is accessed by a network route entry is considered available if there is any linkset in the routeset that is available for traffic.

Local Link Congestion

This feature has no impact on the generation of TFC messages. A is generated concerning point code X-Y-Z, even if X-Y-Z is routed using a network route entry.

Remote Congestion

Since the vSTP has global title capabilities, it is possible for the vSTP to receive a TFC concerning a point code that is accessed by a network route entry. Network route entries are not affected by TFC messages.

Broadcast Transfer Messages

The vSTP does not broadcast TFx messages for network route entries.

Response Method Transfer Messages

The vSTP sends response method **TFx** messages for network routes as follows:

- Prohibited Network Routes: If the vSTP receives an MSU that is accessed by a network route entry, and that network route is Prohibited, the vSTP sends a response method TFP or TCP message, as follows:
  - If there is a Full Point Code defined in the same cluster as the MSU (for example, 8-*-* and 8-1-1 are defined in the vSTP routing table, and MSU is destined for 8-1-2), the **vSTP** sends a **TFP** with concerned point code set to the **vSTP's** DPC.
  - Otherwise, the vSTP sends a **TCP** with concerned point code set to the cluster of the **MSU**'s DPC.
    The vSTP sends response method **TCPs** or **TFPs** at a rate of one **TCP** or **TFP** during the T8 timer period for each network route.

    For example, in the above Applications illustration, the network route for 7-*-* becomes Prohibited due to the failure of **LS**-B, **LS**-C, and **LS**-D. When the vSTP receives an **MSU** from X destined for 7-7-1, the **vSTP** sends a response method **TCP** concerning 7-7-*. When the **vSTP** receives an **MSU** from X destined for 7-8-2, the **vSTP** sends a response method **TCP** concerning 7-8-*.
- System Detects Danger of Circular Routing
  If the vSTP receives an **MSU** that is accessed by a network route entry, and the **vSTP** detects danger of circular routing, the vSTP sends a response method **TFP** or **TCP** message, as follows:
  - If there is a Full Point Code defined in the same cluster as the **MSU** (for example, 8-*-* and 8-1-1 are defined in the **vSTP** routing table, and the **MSU** is destined for 8-1-2), the **vSTP** sends a **TFP** with concerned point code set to the **MSU**'s **DPC**.
  - Otherwise, the **vSTP** sends a **TCP** with concerned point code set to the cluster of the **MSU**'s DPC.

The **vSTP** sends response method **TCPs** at a rate of one **TCP** during T8 timer period for each network route.

For example, in Applications illustration, all linksets are available. If the vSTP receives an **MSU** from node **C** destined for 7-7-1, the vSTP detects danger of circular routing, and sends a response method **TCP** concerning 7-7-*. The vSTP also discards the **MSU**.

- Restricted Network Routes
  If the vSTP receives an **MSU** that is accessed by a network route entry, and that network route is **Restricted**, the vSTP sends a response method **TFR** or **TCR** message, as follows:
  - If there is a Full Point Code defined in the same cluster as the **MSU** (for example, 8-*-* and 8-1-1 are defined in the vSTP routing table, and **MSU** is destined for 8-1-2), the vSTP sends a **TFR** with concerned point code set to the **MSU**s DPC.
  - Otherwise, the **vSTP** sends a **TCR** with concerned point code set to the cluster of the **MSU**s DPC.

For example, in the Applications illustration , the network route for 7-*-* becomes **Restricted** and there is failure of **LS**-**C** and **LS**-**D**. When the vSTP receives an **MSU** from X destined for 7-7-1, the vSTP sends a response method **TCR** concerning 7-7-*, then routes the **MSU** over **LS**-B. When the vSTP next receives an **MSU** from X destined for 7-8-2, the vSTP does not send a response, and routes the **MSU** over **LS**-**B**.

Reception of an RSx Message

If a routeset test (RSP or RSR) is received, a Full Point Code reply (TFx) is generated. The responses to RSP or RSR have been changed according to the following table "Reception of an RSx Message".

> **Note**
>
> The searching hierarchy applies.

Table 2-55 Reception of an RSx Message

Concerned Point Code is:	Result
Found by a Full Point Code match	No change to existing rules.
Found by a cluster match	No change to existing rules.
Found by a network match	Send a **TFx** message based on the current routeset status. • Send a **TFP** if danger of circular routing. Otherwise: • Send a **TFA** if the network route is Allowed. • Send a **TFR** if the network route is **Restricted**. • Send a **TFP** if the network route is Prohibited.
Not found	No change to existing rules. Send a **TFP**.

Reception of an RCX Message

If a routeset clusterset test (RCP (RouteSet Cluster Prohibited Test) or RCR (RoteSet Cluster Restricted Test)) is received, a cluster reply (TCx) is generated. The responses to RCP or RCR is changed according to the below table.

> **Note**
>
> The searching hierarchy applies.

Table 2-56 Reception of an RCx Message

Concerned Point Code is:	Result
Found by a cluster match	No change to existing rules.
Found by a network match	Send a **TCx** message based on the current routeset status. • Send a **TCP** if danger of circular routing. Otherwise: • Send a **TCA** if the network route is Allowed. • Send a **TCR** if the network route is **Restricted**. • Send a **TCP** if the network route is Prohibited.
Not found	No change to existing rules. Send a **TCP**.

2.34.1 Feature configuration Network Routing

There is no GUI and MMI parameter added for the Network Routing.

2.35 Calling Name Conversion Facility (CNCF)

The CNCF (Calling Name Conversion Facility) simplifies the way calling name information is delivered in telecommunications. It converts ISUP IAM messages (used in traditional telephony) between two formats:

- Using a proprietary PIP (Party Information Parameter)
- Using the standard GN (Generic Name Parameter)

A new stop action called “CNCF” has been added to the Gateway Screening feature. When the screening process stops, specific stop actions can be assigned to the screen set. These stop actions define what the vSTP does with an MSU that passes gateway screening.

When the CNCF stop action is used:

- The PIP parameter in the incoming ISUP IAM message is converted to the GN parameter.
- The GN parameter is converted to the PIP parameter.
- The message is sent to the node identified by the DPC (Destination Point Code) in the routing label.

2.35.1 Feature Configuration CNCF

The CNCF 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.

2.35.1.1 GUI Configuration CNCF

To view the CNCF configuration page:

The CNCF can be configured from active SOAM, select **VSTP** and **Configuration** page.

- The following parameter on the M3RL Options MO is used to perform the configurations:
  - CNCF: This parameter is used for turning on or off the CNCF feature. If only enabled the CNCF will be supported. For more information see M3rl Options.
- The following parameter on the MTP Screening Rules MO is used to perform the configurations:
  - `Actname`: The parameter is used for applying new actname as CNCF. The actname parameter, specifying the gateway screening stop action set assigned to the screen, can only be specified with the `nsfi=stop` parameter. The `actname=None` parameter is specified for default case.

2.35.1.2 MMI Managed Objects CNCF

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

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

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

Table 2-57 MMI Managed Objects for CNCF

Managed Object Name	Operations Supported	URI
M3RL Options	GET/PUT	/vstp/m3rloptions
MTP Screening Rules	GET/POST/PUT/DELETE	/vstp/mtpscrrules

M3rl Options - PUT

The CNCF parameter is used for turning on or off the CNCF feature. CNCF parameter must be On to enable CNCF feature. Create a file with following content. File name could be anything, for example: Test can be used as filename:

```
$ vim Test.json
{
    "CNCF ": "On"
}
```

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

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

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

MTPScreeningRule

The `Actname` parameter in MTPScreeningRule MO indicates if CNCF stop action to be applied

POST

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

```
{
 " SCCPStopActionScreening": false,
 "tifstopAction": “None",
 "spare": "no",
 "scmgmessagetype": "1",
 “affectedPcSsn": "1",
 "Actname": "Cncf"
}
```

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

```
/vstp/mtpscrrules –v POST –r .json


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

GET

Run the following command on Active SOAM to display the content:

```
/vstp/mtpscrrules

Sample Output:

{
    "data": [
        {
            " SCCPStopActionScreening": false,
            "tifstopAction": “None",
            "spare": "no",
            "scmgmessagetype": "1",
            “affectedPcSsn": "1",
            "Actname": "Cncf"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}
```

2.35.1.3 Alarms/Events and Measurements CNCF

The following table lists the Alarms and Events specific to CNCF feature:

Table 2-58 Alarms/Events

Alarm/ Event ID	VstpCncfConversionFailed
70490	VstpCncfConversionFailed

For more information about alarms and events, refer to *Oracle Communications Alarms and KPI Guide*.

Measurements

The following table lists the measurements specific to the CNCF functionality for vSTP:

Table 2-59 Measurements

Measurements ID	Measurements Name
22356	VstpTotalMsuProcByCncf
22357	VstpGnToPipCnvSucc
22358	VstpPipToGnCnvSucc
22359	VstpRetransmitGn
22360	VstpNonGnNonPipNoCnv

2.35.2 Troubleshooting

In case of error scenarios, the vSTP measurements are pegged. For more information about CNCF measurements, see Alarms/Events and Measurements CNCF.

2.35.3 Dependencies

The CNCF feature has no dependency on any other vSTP operation. The following points must be considered while configuring CNCF feature:

- Gateway screening rules for Allowed OPC, Allowed DPC, and the Allowed SIO entities must be configured in the database before **cncf** actname can be specified.
- The **actname** parameter, specifying the gateway screening stop action set assigned to the screen, can only be specified with the `nsfi=stop` parameter.
- This feature applies only to ANSI networks.

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 fields 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 Fields

Fields	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. vSTP supports both IPv4 and IPv6 addresses as the primary Local host IP. This is a mandatory field.	Format: Drop down menu Range = 39 characters

Table 5-1 (Cont.) Local Hosts Fields

Fields	Description	Data Input Notes
Secondary Local Host IP Address	Secondary IP Address of Local Host. vSTP supports both IPv4 and IPv6 addresses as the secondary Local host IP.	

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 fields 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 Fields

Fields	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. vSTP supports both IPv4 and IPv6 addresses as the primary Remote host IP. This is a mandatory field.	Format: Drop down menu Range = 39 characters
Secondary Remote Host IP Address	Secondary IP Address of Remote Host. vSTP supports both IPv4 and IPv6 addresses as the primary Remote host IP.	

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 field 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 fields 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 Fields

Fields	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 if it is referenced in any other configuration.	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 5-3 (Cont.) Local Signaling Points Fields

Fields	Description	Data Input Notes
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 **Note:** The LSP cannot be edited when the PC Type parameter value is **Tpc**. Therefore, to change the true point code (PC type = TPC), you need to delete the LSP and add again.
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
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. Only one LSP can have this MTP Point Code if the PC type is TPC or SPC. The LSP may optionally be assigned up to two Capability Point Codes (CPCs), which are point codes that can be shared with other LSPs.	Valid characters are integers seperated with hyphen(-)
Group Code	A group may have multiple countries in it, or a country might have multiple groups in it. ITUN/ ITUI destinations are hence divided into groups	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**

> **Important**
>
> After adding an LSP, it is mandatory to restart the MP for the system to get updated. Restart of MP is mandatory for the MPs to get the update after adding a true point code (TPC) irrespective of the domain.

Editing a Local Signaling Point

Use this procedure to change the field values for a selected Local Signaling Point:

1. Select the **Local Signaling Point** row to be edited.
2. Click **Edit**
3. Enter the updated values.

> **Note**
>
> - The **Local Signaling Point Name** field cannot be changed.
> - The values of **MTP Point Code** and **Group Code** can be edited only if the value of **PC Type** is CPC.

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**.

> **Important**
>
> After deleting an LSP, it is mandatory to restart the MP for the system to get updated. Restart of MP is mandatory for the MPs to get the update after deleting a true point code (TPC) irrespective of the domain.

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 fields 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 Fields

Field	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	This defines ITUN/ITUI group code for duplicate point code feature. If left unconfigured as default, there should be a domain group code = aa mapping in LSP table.	Format: Input Text Box Range: aa, zz Default Value: aa
Alias Point Code 1	Alias Point Code1.	NA
Alias Point Code 2	This defines ITUN/ITUI group code for duplicate point code feature.	NA
Alias Point 1 Group Code	This defines ITUN/ITUI group code for duplicate point code feature.	NA
Alias Point 2 Group Code	This defines ITUN/ITUI group code for duplicate point code feature.	NA
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
Alias Point Code 2 Domain	Alias Point Code 2 Domain	NA

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
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
UDT XUDT Conversion	Defines the type of conversion allowed for respective Remote Signaling Point.	Allowed values: • NOCONV' • XUDTTOUDT' • UDTTOXUDT' • SXUDTTOUDT' Default value: NOCONV
Proxy Point Code Indicator	Defines if Point code is to be used as a proxy point code.	Default: No Range= Yes, No
Exception List Exclusion Indicator	Applicable only to Cluster Point Code.	Default: No Range: Yes, No
Nested Cluster Allowed Indicator	Applicable only to Cluster Point Code. This parameter specifies whether the route to the cluster point code can be different for provisioned members of the cluster.	Default: No Range: Yes, No
Enable	It enables the specific Remote signaling Point.	Range: Enable

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
Disable	It disables the specific Remote signaling Point. **Note** • When ever user disables any RSP, then all the direct link	Range: Disable

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
	specifictoRSPwillmovetoDisabledRspadminstateoverLink	

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
	Maintenance screen, and the Disabled RspLink will become unav	

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
	• ailable. Any link in Disabled RSP administrate will not be enable	

Table 5-4 (Cont.) Remote Signaling Point Fields

Field	Description	Data Input Notes
	d t h r o u g h l i n k s e t o r l i n k m a i n t e n a n c e s c r e e n .	

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 fields 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 Fields

Fields	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 = up to 9 characters
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. Must be an alphabetical value of upto 2 characters.	Format: Input Text Box

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 fields 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 Fields

Fields	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 fields 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 Fields

Fields	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 Fields

Fields	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. A non-zero value for sctpSackDelay gives the application time to bundle data chunks in the same SCTP message with the SACK, thereby reducing the number of packets in the network. Setting sctpSackDelay to zero disables this delay so that SACKs are sent as quickly as possible. This is a mandatory field.	Format: Input text box Range = Typical value is 10. Maximum: 200, Minimum: 1
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

Table 5-7 (Cont.) Connection Configuration Sets Fields

Fields	Description	Data Input Notes
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
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 false.
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
SCTP Bundling Enabled	This parameter is used for enabling or disabling SCTP Bundling.	Range: Yes, No Default value: Yes

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 fields on the **Links** View and Insert pages.

> **Note**
>
> Data Input Notes apply to the Insert pages only. The View page is read-only.

Table 5-8 Links Fields

Fields	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 Fields

Fields	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 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**

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 field 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 fields 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 Fields

Fields	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: 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; Maximum Length = 32
Remote Signaling Points	Name of the Adjacent Remote Signaling Point associated with this Link Set This is a mandatory field.	Format: Drop-down menu Range: a-z,A-Z,_,0-9 Maximum Length = 32
Reserved Link Transactions Per Second	This parameter specifies Guaranteed Link (/vstp/links) transactions per second defined for all the links of this Link Set. This is a mandatory field.	Range: 10 to 10000 for M3UA/M2PA, 10 to 15000 for MTP2
Maximum Link Transactions Per Second	This parameter specifies Maximum Link (/vstp/links) transactions per second defined for all the links of this Link Set. This is a mandatory field.	Format: Input text box Range: 10 to 10000 for M3UA/M2PA, 10 to 15000 for MTP2
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 to 4294967295
Number of Signaling Links Allowed Threshold	This threshold value signifies the number of signaling links allowed to be configured with this link set. This link count threshold is required for a linkset to transition from the **Restricted** or **Prohibited** state to the **Allowed** state. This is applicable only for M3ua linksets.	Format: Input text box Range: 0 to 16 Default Value: 1

Table 5-9 (Cont.) Link Sets Fields

Fields	Description	Data Input Notes
Number of Signaling Links Prohibited Threshold	This threshold value signifies the number of signaling links required to prohibit a link set. This link count threshold is required for a linkset to transition from the **Restricted** or **Allowed** state to the **Prohibited** state. This is applicable only for M3ua linksets	Format: Input text box Range: 0 to 16 Default Value: 1
Application Server Notification	Application Server (AS) notification.	Format: Drop-down menu Range: true, false
Calling Party GT Modification Indicator	Calling party GT modification indicator. This parameter specifies whether calling party global title modification is required.	Format: Drop-down menu Range: true, false Default value: false **Note**: To enable `Calling Party GT Modification` using GTT on CgPA, set `Calling Party GT Modification Indicator` to **true**. For more details, see SCCP GTT Mods.
Enable Broadcast Exception	When the linkset status changes, the VSTP broadcasts TFP/TFA to adjacent nodes. When `enableBroadcastException` is set to `true`, this broadcast is not performed.	Format: Drop-down menu Range: true,false Default value: false
GTT Mode	Global title translation mode. The GTT Mode hierarchy for this link set.	Format: Drop-down menu Range: • Cd • Fcd • Fcg • Fcgfcd • Fcdcg • Sysdflt Default value: Sysdflt
ITU Transfer Restricted	ITU TFR (Transfer Restricted) indicator. When set to false, the TFR procedure is turned off for this linkset. ituTransferRestricted only applies to ITU national linksets.	Format: Drop-down menu Range: true,false Default value: false
MTP Screening Set Name	Name of the MTP Screenset attached with this Linkset.	Format: Drop-down menu Range: a-z, A-Z, _, 0-9 Maximum Length: 8
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 Default value: false

Table 5-9 (Cont.) Link Sets Fields

Fields	Description	Data Input Notes
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 Default value: 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 Default Value: false
Incoming SLS Rotated Signaling Bit	Incoming rotated signaling 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 to 8 Default value: 1
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 Default value: Off
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 Default value: 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 Default value: false
Rotated 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 to 4 Default value: 1
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 to 16

Table 5-9 (Cont.) Link Sets Fields

Fields	Description	Data Input Notes
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. For MTP2 High Speed Links, configure `ItuHslDefault` or `AnsiHslDefault`.	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 Range: a-z,A-Z,0-9,_ Maximum length: 32
Security Logging	Options to generate logs linkset wise.	Default: Off, Range: Off, All, Risky
Link Set Accounting Measurement	Link Set Accounting Measurement Option. This parameter specifies whether the accounting measurement option for the link set is On or Off.	Default value: No Range: Yes, No
CGPN BlackList Set	CGPN Blacklist Set Id for screening directory number per linkset referred in Linkset table.	Default value: None Range: 1 to 255
Generic Name Set	Generic Name Set.	Default value: Both Range: SetA, SetB, Both
SMS Proxy	Option to send to SMS Proxy for HOMESMSC Feature.	Range: Off, On Default value: Off
Linkset PCT	Linkset Point Code and CIC Translation. It will only be considered if PCT is set to LSET in M3RL options. It will control whether PCT feature is applied to MSUs coming in or going out on links of a particular linkset.	Range: Off, On Default value: Off
Proxy RSP Name	Name of the Proxy Remote Signaling Point associated with this Link Set.	Range: 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, then 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 fields 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 Fields

Field	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.
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 fields 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 Fields

Field	Description	Data Input Notes
GTT Set Name	Name for the SCCP GTT Set, which must be unique within the VSTP site. This is a mandatory field.	Format: 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.
NPSN Name	Not Present Set Name (NPSN) is used to configure alternate GTT Set. While decoding the MSU to extract the key for lookup in the GTTSET of the set type, if the required parameter does not exist in the MSU and that parameter is optional for that opcode, then the NPSN parameter (if provisioned in the GTTSET) can be used to go to another GTTSET. If the NPSN is not provisioned, then it is treated as bad translation. NPSN comes in the FLOBR/MBR search path, 1 leading alphabetic character and up to 8 following alphanumeric characters and underscore.	Format: Drop down menu Range = Imsi/Msisdn/Vlrnb/ Smrpoa/Smrpd Value can have one leading alphabetic character, up to 8 following alphanumeric characters, and underscore.
Gtt Set Domain	Defines the type of incoming message network domain. **Note:** This GTTSET MO does not distinguish between ITU national or ITU international. This is a mandatory field.	Format: Drop down menu

Table 5-11 (Cont.) GTT Sets Fields

Field	Description	Data Input Notes
Gtt Set Type	Defines the type of GTT Set. This is a mandatory field.	Format: Drop down menu
Check Multiple Components	This parameter specifies whether to support TCAP multicomponent packets.	Format: Drop down menu
Allow Segmented XUDT	This parameter specifies whether TOBR processing must be allowed on Segmented XUDT(S) message or not. **Note:** This parameter can be configured only if the `GTT Set Type` parameter value is **OPCODE**.	Possible values are: • Yes • No Default value: No

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 fields 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 Fields

Fields	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 Fields

Fields	Description	Data Input Notes
CdPA GTT Set Name	CdPA GTT set name (/vstp/gttsets) associated with this GTT Selector.	Format: Drop down menu Valid characters are alphanumeric and underscore. Valid names are strings between one and 9 characters, inclusive. **Note** The name must contain at least one alphabet and must not start with a numeric character.

Table 5-12 (Cont.) SCCP GTT Selectors Fields

Fields	Description	Data Input Notes
CgPA GTT Set Name	CgPA GTT set name (/vstp/gttsets) associated with this GTT Selector.	Format: Drop down menu Valid characters are alphanumeric and underscore. Valid names are strings between one and 9 characters, inclusive. **Note** The name must contain at least one alphabet and must not start with a numeric character.
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	Name of the SCCP GTT Set (/vstp/gttsets) associated with this GTT Selector.	Format: Drop down menu Valid characters in the name are alphanumeric and underscore.
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

Table 5-12 (Cont.) SCCP GTT Selectors Fields

Fields	Description	Data Input Notes
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
SCCP Message Type	Defines SCCP message type in GTT selector.	Default: All Range = 'u', 'us', 'x', 'xs', 'all', 'u,us', 'u,x', 'u,xs', 'us,x', 'us,xs', 'x,xs', 'u,us,x', 'u,us,xs', 'u,x,xs', 'us,x,xs'.

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 fields 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 Fields

Fields	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: dropdown menu Range: Disc, Dup, Fwd, Scpval, Sfthrot, Indv_Throt, Tcaperr, Sfapp, Udts
Handle Response	Handle Response.	Format: dropdown menu Range: Yes, No Default: 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: dropdown 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: dropdown 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.

Table 5-13 (Cont.) GTT Actions Fields

Fields	Description	Data Input Notes
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: dropdown 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 (-)
Calling Party Point Code in Outgoing Message	The data that is used as the Calling Party Point Code in the outgoing message.	Format: dropdown menu Range = Dflt, Cgpcicmsg, Opcicmsg, Provcgpc, Remove Default = Dflt
Default Actions	The default action that is performed when the fwd GTT Action fails to route the MSU.	Format: dropdown 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: dropdown 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: dropdown 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: dropdown 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: dropdown 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

Table 5-13 (Cont.) GTT Actions Fields

Fields	Description	Data Input Notes
Loop Set	Name for the Loop set associated with GTA, it must be unique within the VSTP site.	Format: dropdown 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
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: dropdown menu Range: Gt, Ssn Default: Ssn
Remote Signaling Point	This defines the Remote Signaling Point name associated with this Global Title Address (GTA).	Format: dropdown 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: dropdown 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: 0-255
Threshold	If the number of MSUs serviced by the Sfthrot/Indv_Throt action exceeds threshold value, MSUs are discarded.	Format: dropdown menu Range: 1-4294967295 Default: 1
Throttle Action Index	Throttle Action Index for Measurements.	Format: Text box Range: Valid characters are integers.
TCAP Parameters	This TCAP parameter is used to decide whether the MAP digits, NP and NoN shall be picked form SMRPDA or SMRPOA for comparison.	Range: Smrpoa, Smrpda

Table 5-13 (Cont.) GTT Actions Fields

Fields	Description	Data Input Notes
UDTS GTT Action	The reason associated with the UDTS GTT Action for discarding the message.	Range: 0-255
UIM Required	This specifies whether a UIM should be generated. When set to true, UIM is not generated.	Default: false Range: true,false
Use Incoming Message	This specifies whether to apply GTT Action data to the message as the message was received (OFF).	Range: true,false Default: false (for ScpVal)
Value Type	This parameter is used to decide whether SCCP/TCAP parameter should be used for the validation of the MSU or IR21 data should be used for the validation of the MSU.	Default: SccpToTcap Range: SccpToTcap, IR21ToTcap
Max GTA Length	This parameter is used to decide maximum address length for a GTA entry with Indv_Throt action.	Range: 1- 21
Full RSP Point Code	The Unprovisioned Full Point Code. If Cluster/Network PC is configured as Remote Signaling Point, Full Point Code must be specified.	Range: Valid characters are integers, asterik (*) and none. Maximum allowed length is 4.
Cluster X-List Expire Timer	This timer will be restarted whenever a x-list entry gets created, updated or used for routing. If the timer expires before it is restarted, x-list entry will be removed.	Range: Valid characters are integers, asterik (*) and None. Maximum allowed length is 4.
ATI GTT Set Name	This parameter is used to add specific GTT Set for self generated ATI Message with Sfapp action. Must be of CDPA Set Type.	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.

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 fields 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 Fields

Field	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

Table 5-14 (Cont.) GTT Action Sets Fields

Field	Description	Data Input Notes
Test Mode	If TestMode parameter is off, GTT ACTION SET will follow the existing behavior i.e. actions will be executed on the MSU and event will be generated. If TestMode parameter is on, GTT ACTION SET will only generate event about the actions and will actually not execute any action on MSU.	Range = Off, On
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 fields 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 Fields

Field	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, up to 8 following alphanumeric characters, and underscore. A value is required.

Table 5-15 (Cont.) Global Title Addresses Fields

Field	Description	Data Input Notes
Translate Indicator	Defines translation actions and routing actions for this Global Title Address (GTA). **Note:** If translationIndicator is set as None, either startAddress or endAddress, and gttSetName should be set. If translateIndicator is set as Dpc, then routingIndicator, rspName, subsystem, mapSetId, and mrnSetId should be set. If translateIndicator is set as Dpcngt, then routingIndicator is set as Gt. If translateIndicator is set as Dpcssn, then routingIndicator is set as Ssn. 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
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 **Note**: To enable `Calling Party GT Modification` using GTT on CgPA, set `Calling Party GT Modification Indicator` to **true**. For more details, see SCCP GTT Mods.
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

Table 5-15 (Cont.) Global Title Addresses Fields

Field	Description	Data Input Notes
Calling Party Point Code	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn); or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range = Valid characters are numeric seperated by hyphen(-) and plus(+) sign and wildcard(*).
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 Fields

Field	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
Priority	Priority, is used to select translation when multicomponent packet is received. 1024 has the lowest priority and 1 being highest priority.	By default value will remain 1024. Valid values are in the range of [1-1024]
Allow Multiple Components	Allow Multiple Components. This parameter specifies if a certain component/opcode is required to be processed in multicomponent packet.	
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.
Remote Signaling Points	Defines the Remote 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.]
Loop Set	Name for the Loop set associated with Global title address, it must be unique within the VSTP site.	[Range = 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.]
Map Set	Defines the Map Set identifier associated with this Global Title Address (GTA). MAP Set id is a Mated Application set ID. MAP Set id is mandatory when routingIndicator is set to SSN.	[Range = 1-6000]
Mrn Set	Defines the Mated Relay Node (MRN) Set name associated with this Global Title Address (GTA).	[Range = 1-1500]

Table 5-15 (Cont.) Global Title Addresses Fields

Field	Description	Data Input Notes
OPC	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn); or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	[Range = Valid characters are integers, plus (+), minus (-) sign, wildcard(*). Maximum allowed length is 11.]
TCAP Opcode	The TCAP opcode field in the incoming MSU.	[Range = Valid characters are integers, asterik (*) and None. Maximum allowed length is 4.]
OPC GTT Set	The OPC GTT set name.	[Range = 1 leading alphabetic character, up to 8 following alphanumeric characters, and underscore.]
Optional GTT Set	Optional gtt set name.	[Range = 1 leading alphabetic character, up to 8 following alphanumeric characters, and underscore.]
Package Type	The ANSI and ITU TCAP package type.	[Default = Invalidpkgtype; Range = Bgn, End, Cnt, Ituabort, Ituuni, Qwp, Qwop, Resp, Cwp, Cwop, Ansiabort, Ansiuni,Any]
Routing Indicator	Routing indicator. GT allow a called party address with a routing indicator value of 'global title'. SSN allow a called party address with a routing indicator value of 'DPC/SSN'.	[Range = Gt, Ssn]
Start Map Address	Start Address (similar to startAddress). This parameter specifies the beginning of a range of MAP digits (IMSI/MSISDN/VLRNB/SMRPOA/SMRPDA).	[Range = a-f,A-F,0-9; Maximum Length = 21]
Start Global Title Address	Defines the start of a range of this Global Title Address. This specifies the start of a range of MAP digits (IMSI/MSISDN/VLRNB/SMRPOA/SMRPDA).	[Range = a-f,A-F,0-9; Maximum Length = 21]

Table 5-15 (Cont.) Global Title Addresses Fields

Field	Description	Data Input Notes
SSN	New translated subsystem number.	[Range = 2-255;]
SK	Service Key	[Range = Valid characters are either * or a-f, A-F, 0-9]
BCSM	Basic Call State Model	[Range = Valid characters are either * or a-f, A-F, 0-9]
Opcode Tag	Operation Code Tag. The tag helps to differentiate the message on SIGTRAN connections.	[Range = Both, Local, Global; Default = Both]
Full RSP Point Code	The Unprovisioned Full Point Code. If Cluster/Network PC is configured as Remote Signaling Point, Full Point Code must be specified.	[Range = Valid characters are integers, asterik (*) and None. Maximum allowed length is 4]

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 fields on the **SCCP GTT Mods** View, Insert, and Edit pages.

Note

The Calling Party GT Modification can be performed in the following ways:

- **Calling Party GT Modification using GTT on CgPA:**
  Perform the following steps to enable Calling Party GT Modification using **GTT on CgPA**:
  1. Set `Calling Party GT Modification Indicator` to **true** for the incoming Linkset or the GTT Translation configurations on the **Linkset** or **Global Title Address** page respectively..
     This indicates that the Calling Party GT Modification needs to be performed.
  2. The Calling Party GT Modification data is extracted by performing GTT on the Calling Party GTA using the **Cd** GTT Mode / Hierarchy. If the GTT Selectors and GTT Translation for CgPA GTA is configured, then the GT Modification data attached with is used to perform Calling Party GT Modification on outgoing messages.
     a. Configure the GTT Translation for the incoming CgPA GTA in a CDPA GTT Set. Attach the required GTT Modification data to this translation.
     b. Create GTT Selector as per the parameters in the CgPA of incoming message. Attach the previously configured GTT Set to the “CDPA GTT Set” of this GTT Selector.
- **Calling Party GT Modification using “GTT Action - Forward”**
  Perform the following configurations to enable Calling Party GT Modification using **GTT Action - Forward**:
  1. Go to **GTT Actions** and set `GTT Action Type` parameter value to **Fwd**.
  2. For the GTT action, set values of the `Called Part GTT Mod Name` and `Calling Part GTT Mod Name` parameters. Configure remaining parameters for **Fwd GTT Action** as per the routing requirement.
  3. Attach **Fwd - GTT Action** to a GTT Action Set. This could be a new GTT Action Set or an existing one.
  4. Attach the GTT Action Set to the GTT Translation where, the GT Modifications needs to be performed.

Table 5-16 SCCP GTT Mods Fields

Fields	Description	Data Input Notes
CgPA Subsystem Number	CgPA subsystem number.	Maximum: 255 Minimum: 2
GT Filler Indicator	GT filler indicator in case of GTI change	
GTT Mod 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.

Table 5-16 (Cont.) SCCP GTT Mods Fields

Fields	Description	Data Input Notes
New Global Title Indicator	Defines the new Global Title Indicator for this GTT Mod.	Values: • When set to TtNumEncodingNature, then 4 value is assigned corresponding to the itu domain set. • When set to TtOnly, then 2 value is assigned corresponding to the domain that is set. Multiple entries can exist for TtOnly corresponding to each domain.
New Nature of Address Indicator	Defines new Nature of Address indicator for this GTT Mod.	Maximum: 127 Minimum: 0 Values: • Value 1 refers to Subscriber natureOfAddressIndicator • value 2 refers to Reserved natureOfAddressIndicator • value 3 refers to National natureOfAddressIndicator • value 4 refers to International natureOfAddressIndicator • value 5-127 refer to spare values • value 0 refers to unknown natureOfAddressIndicator
New Numbering Plan	Defines new Numbering plan (NP) for this GTT Mod.	Maximum: 15 Minimum: 0 Values: • Value 1 refers to Isdn numberingPlanValue • value 2 refers to Generic numberingPlanValue • value 3 refers to Data numberingPlanValue • value 4 refers to Telex numberingPlanValue • value 5 refers to Maritime numberingPlanValue • value 6 refers to Land • value 7 refers to IsdnMobile numberingPlanValue • value 8 refers to Private numberingPlanValue • value 9-15 refers to Spare nnumberingPlanValue • value 0 refer to Unknown numberingPlanValue
New Translation Type	Defines the new translation type (TT) for this GTT Mod.	Maximum: 255 Minimum: 0

Table 5-16 (Cont.) SCCP GTT Mods Fields

Fields	Description	Data Input Notes
Number of Prefix Digits to be Deleted	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
New Prefix Digits String	New prefix digits string. The digits to be prefixed to the received GT address.	
Number of Suffix Digits to be Deleted	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
New Suffix Digits String	New suffix digits string. The digits to be suffixed to the received GT address.	
Suffix Prefix Processing Precedence Indicator	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 Global Title Address (/vstp/globaltitleaddresses), the GTT Modification cannot be deleted.

1. Select the **SCCP GTT Mod** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

> **Note**
>
> The GTT modification is not applicable for CDPA.

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 fields 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 Fields

Fields	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 Fields

Fields	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 fields 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 Fields

Fields	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 fields 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 Fields

Fields	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.
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,Blk Dpc
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/).

From the main menu of **vSTP**, navigate to **Configuration**, select **MTP Screening Rules** page.

> **Note**
>
> Data Input Notes apply to the **Insert** and **Edit** pages, the **View** page is read-only.

Table 5-20 MTP Screening Rules Fields

Fields	Description	Data Input Notes
MTP Screening Name	This defines MTP screening rule name. It is a mandatory field.	Range: 1 leading alphabetic character and up to 7 following alphanumeric characters
Screening Rule Group Type	This parameter indicates screening rule type. It is a mandatory field.	Range: • AftDstn • AftPc • AftPcSsn • BlkDpc • BlkOpc • Dpc • Opc • Sio
MTP Screening Rule Group	This defines the allowed screening rule group. It is a mandatory field.	Range: 1 leading alphabetic character and up to 7 following alphanumeric characters
Next Screening Rule Group	This defines the allowed next screening rule group name.	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. It is a mandatory field.	Range: • AftDstn • AftPc • AftPcSsn • BlkDpc • BlkOpc • Dpc • Fail • Opc • Sio • Stop
Network Indicator	This parameter defines Network indicator value. It specifies one or more values for the network cluster and network cluster member values identified in the nc and ncm parameters. It specifies the network indicator 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]$'
Network Cluster	This parameter defines Network cluster value. It specifies one or more values for the network indicator and network cluster member values specified in the network indicator and ncm parameters. It specifies the network cluster of the point code represented by ni-nc-ncm.	Range: • Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. • Regular expression to represent the range is: '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'

Table 5-20 (Cont.) MTP Screening Rules Fields

Fields	Description	Data Input Notes
Network Cluster Member	This parameter defines Network cluster member value. The 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]$'
ITU International Area	This defines ITU international area. The area in the point code represented by zone-area-id.	Range: • Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. • Maximum allowed length is 7. Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
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]$'
ITU International Zone	This parameter defines ITU international zone. This parameter specifies the zone in the point code represented by zone-area-id.	Range: • Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 3. • Regular expression to represent the range is '^(([0-7])(-))?([0-7])$\|^[D]$'
ITU National Point Code	This parameter defines ITU national point code.	Range: • Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 11. • Regular expression to represent the range is '^((([0]?[0-9]{1,4})|([1][0-5][0-9]{1,3})|(16[0-2][0-9]{1,2})|(163[0-7][0-9])|(1638[0-3]))(-))?(([0]?[0-9]{1,4})|([1][0-5][0-9]{1,3})|(16[0-2][0-9]{1,2})|(163[0-7][0-9])|(1638[0-3]))$\|^[D]$'
ITU National Signaling Area	This parameter defines 24-bit ITU-national main signaling area value. The msa of the point code represented by msa-ssa-sp.	Range: • Valid characters are integers seperated by hyphen (-) and D (Uppercase letter D) for default range. Maximum allowed length is 7. • Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[D]$'

Table 5-20 (Cont.) MTP Screening Rules Fields

Fields	Description	Data Input Notes
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]$'
ITU National Signaling Point	This parameter defines 24-bit ITU national signaling point. This parameter specifies the sp in the point code represented by msa-ssa-sp.	Range: • Valid characters are integers seperated by hyphen (-),asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 7. • Regular expression to represent the range is '^((([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))(-))?(([0-1]?[0-9]?[0-9])|([2][0-4][0-9])|(25[0-5]))$\|^[*]$|^[D]$'
ITU National 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 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]$'
ITU National Main Number Area	This parameter defines 16-bit ITU national main number area. The mna in the point code represented by un-sna-mna.	Range: • Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range and D (Uppercase letter D) for default range. Maximum allowed length is 5. • Regular expression to represent the range is '^((([0-2]?[0-9])|([3][0-1]))(-))?(([0-2]?[0-9])|([3][0-1]))$\|^[*]$|^[D]$'
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])$\|^[*]$'

Table 5-20 (Cont.) MTP Screening Rules Fields

Fields	Description	Data Input Notes
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]))$'
H0 Heading code	This defines H0 Heading code. New H0 heading code for SSNM message.	Range: • Valid characters are integers seperated by hyphen (-), asterik (*) to mark full range. • Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[0-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$\|^[*]$'
H1 Heading code	This defines H1 heading code. New H0 heading code for SSNM message.	Range: • Valid characters are integers separated by hyphen (-), asterik (*) . • Maximum allowed length is 5. Regular expression to represent the range is '^((([0]?[0-9])|([1][0-5]))(-))?(([0]?[0-9])|([1][0-5]))$\|^[*]$'
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	This field is valid only for SIO, if SI equals 5 only valid when nsfi equals stop.	Range: • Tif_Ruleset_1 • Tif_Ruleset_2 • Tif_Ruleset_3
Spare	This parameter signifies if the domain is a spare type or not.	Range: Yes or No Default: None. Allowed only for ITUI_S and ITUN_S domains.
SCMG Message Type	This parameter will specify the type of SCMG MSG. It's allowed only when the rule type is SIO and SI is 3. The valid values are [1,2,3,4,5,6,253,254,255]. Here, 1 indicates Subsystem Allowed, 2 indicates Subsystem Prohibited, 3 indicates Subsystem Status Test, 4 indicates Subsystem Out of Service Request, 5 indicates Subsytem out of Service Grant, 6 indicates SCCP/ Subsystem Congested, 253 indicates Subsystem Backup Routing, 254 indicates Subsystem normal routing, 255 indicates Subsystem routing test.	Range: 1, 2, 3, 4, 5, 6, 253, 254,255

Table 5-20 (Cont.) MTP Screening Rules Fields

Fields	Description	Data Input Notes
Affected PC SSN	This is a must parameter for AftPcSsn rule type.	Range: 1 to 255
Actname	This is a parameter for choosing the action name.	Range: Cncf, None

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

Perform the following procedure to change the field values for a selected MTP Screening Rule:

> **Note**
>
> 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

Perform the following procedure to delete an 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 fields 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 Fields

Fields	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 fields 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 Fields

Field	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 Fields

Field	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).	
Mosmstcapseg	MO-based SMS TCAP Segmentation for GSM. This parameter specifies whether Mobile-Originated segmented TCAP messages are supported.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
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.	
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.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
Defcc	Default country code	The `Defcc` value for a subscriber number should be up to 3 digits. Range: "^([a-fA-F0-9]{1,3})$\|^(None)$"
Defndc	Default network destination code.	The `Defndc` value for a subscriber number should be up to 5 digits.
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 Fields

Field	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 Fields

Field	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 Fields

Field	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.	
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.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
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.	
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.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
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.	
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.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
Inpsprestype	INP option that indicates the type of message the vSTP 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.	
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.	

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
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.	
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.	
sriPrepaid	This parameter is use to turn on/off SRI functionality for Prepaid Message.	Range: On/Off

Table 5-22 (Cont.) SCCP Mnp Options Fields

Field	Description	Data Input Notes
Dfltrn	GPORT sri default Routing Number.	Range: Alphanumeric string [0-9] [a-e]

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 fields on the **SCCP Options** View and Edit pages.

Table 5-23 SCCP Options Fields

Fields	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).	NA

Table 5-23 (Cont.) SCCP Options Fields

Fields	Description	Data Input Field
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
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]

Table 5-23 (Cont.) SCCP Options Fields

Fields	Description	Data Input Field
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)).	NA
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)).	NA

Table 5-23 (Cont.) SCCP Options Fields

Fields	Description	Data Input Field
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)).	NA
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)).	NA
Velocity of Travelling	Defines the velocity of travelling.	Default - NA , [Minimum,Maximum] - [1,700]
SMS Delivery	SMS Proxy Delivery Functionality Status	. [Range = On, Off; Default = Off;]
SMS Origination	SMS Proxy Origin Functionality Status.	[Range = On, Off; Default = Off;]
SMS Termination	SMS Proxy Terminate Functionality Status.	Range = On, Off; Default = Off

Table 5-23 (Cont.) SCCP Options Fields

Fields	Description	Data Input Field
Allowed First Segment Length	Specifies the allowed length of the first XUDT segment.	Allowed Value: Maximum:272 Minimum:0 Default: 0
TCAP Error Discard	TCAP Error Discard. If it is turned Off, MSU will be processed. While if it is turned on, MSU will be discarded.	Range = On, Off Default = Off
Send UDTS on Opc	If this is turned on, VSTP generated UDTS on Opc is sent	.Range = On, Off Default = Off
CGPA GTT On Response UDTS	Enables or disables routing of response UDTS message on GT/OPC of incoming route on GTT SCCP request/Message. While it is turned On, the response UDTS routes on GT. While it is turned Off, the response UDTS routes on OPC.	.Range = On, Off Default = On
Enable Intermediate GTT Act	This parameter allows gttaction to be applied to intermediate gttsets.	Range = On, Off, Default = Off

You can perform edit task on **VSTP**>**Configuration**>**SCCP Options** page.

Editing a SCCP Option

Use this procedure to change the field values for a selected SCCP Option. :

1. On the **VSTP**>**Configuration**>**SCCP 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 fields 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 Fields

Field	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 service nature of address indicator. This parameter overrides the incoming Nature of Number in AIN Info_Analyzed CalledPartID.	
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.	
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.

Table 5-24 (Cont.) AINP Options Fields

Field	Description	Data Input Notes
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 fields 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 Fields

Fields	Description	Data Input Notes
Type of Application	Type of Appplication. This is a mandatory field.	Range = Eir, Atinp, Inpq, Sfapp, SMSProxy
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 fields 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 Fields

Field	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.	
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**
>
> The 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 fields 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 Fields

Fields	Description	Data Input Notes
Action	Action to be taken when Sccp Loop is detected.	Format: Drop down menu Range = notifyOnly, discardOnly.
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 1 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.

Table 5-27 (Cont.) SCCP Loop Sets Fields

Fields	Description	Data Input Notes
Domain 1	Defines the type of incoming message network domain. [A value is required.]	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 1	List of signaling Pointcodes.	-
Domain 2	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 2	List of signaling Pointcodes.	-
Domain 3	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 3	List of signaling Pointcodes.	-
Domain 4	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 4	List of signaling Pointcodes.	-
Domain 5	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 5	List of signaling Pointcodes.	-
Domain 6	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 6	List of signaling Pointcodes.	-
Domain 7	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 7	List of signaling Pointcodes.	-
Domain 8	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 8	List of signaling Pointcodes.	-
Domain 9	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 9	List of signaling Pointcodes.	-
Domain 10	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 10	List of signaling Pointcodes.	-
Domain 11	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
Point Code 11	List of signaling Pointcodes.	-

Table 5-27 (Cont.) SCCP Loop Sets Fields

Fields	Description	Data Input Notes
Domain 12	Defines the type of incoming message network domain.	Format: Drop down menu Range: Ansi Itun Itui Itun24 Itui_s Itun_s Itun16.
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**
>
> The 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","Dn6","Dn7","Dn8","Dn9","Dn10","Dn11","Dn12","Dn13","Dn14","Dn15","Dnx","Fpfx","Ign1","Ign2","Ign3","Ign4","Ign5","Ign6","Ign7","Ign8","Ign9","Ign10","Pfxa1","Pfxa2","Pfxa3","Pfxa4","Pfxa5","Pfxa6","Pfxa7","Pfxa8","Pfxb1","Pfxb2","Pfxb3","Pfxb4","Pfxb5","Pfxb6","Pfxb7","Pfxb8","Pfxc1","Pfxc2","Pfxc3","Pfxc4","Pfxc5","Pfxc6","Pfxc7","Pfxc8","Pfxd1","Pfxd2","Pfxd3","Pfxd4","Pfxd5","Pfxd6","Pfxd7","Pfxd8","Pfxe1","Pfxe2","Pfxe3","Pfxe4","Pfxe5","Pfxe6","Pfxe7","Pfxe8","Pfxf1","Pfxf2","Pfxf3","Pfxf4","Pfxf5","Pfxf6","Pfxf7","Pfxf8","Sn1","Sn2","Sn3","Sn4","Sn5","Sn6","Sn7","Sn8","Sn9","Sn10","Sn11","Sn12","Sn13","Sn14","Sn15","Snx","Znx"

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
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", "Selscr", "Skgtartg", "Snscgpn" , "Tifgnbl", "Tiflsbl", "Tifrdnbl"
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"
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"

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
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"
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

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
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
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

Table 5-28 (Cont.) NPP Action Sets Elements

Element	Description	Data Input Notes
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
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 fields 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 Fields

Field	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', 'Tif', 'Tif2', 'Tif3', 'Tifcgpn', 'Tifcgpn2', 'Tifcgpn3'
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'
FPFX	Filter prefix. The prefix used to filter incoming digit strings. This is a mandatory field.	Range = Allowable values 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]*)$\|^([A-Fa-f0-9]*(\?){0,15}[a-fA-F0-9])*$|^(*)$
FDL	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(*). Allowed values are 1-32, * and the regular expression to be followed : ^([1-9]|[1-2][0-9]|[3][0-2]|*)$
NPP Action Set	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.

Table 5-29 (Cont.) NPP Service Rule Sets Fields

Field	Description	Data Input Notes
Invoke Service	Invoke service name. The name of the NPP service to be invoked.	The default value is None. Range = 'None', 'Idprcdpn', 'Idprcgpn', 'Mosmsgcdpn', 'Mosmsgcgpn', 'Idprcdpn2', 'Idprcdpn3', 'Idprcdpn4', 'Tif', 'Tif2', 'Tif3', 'Tifcgpn', 'Tifcgpn2', 'Tifcgpn3'

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 fields 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 Fields

Field	Description	Data Input Notes
SRVN	The name of the NPP Service. This is a mandatory field.	The name cannot be changed. Range: • The SA and Precedence of Idprcdpn Service (i.e Idprcdpn, Idprcdpn2, Idprcdpn3, Idprcdpn4) is ccncchk->100, inprtg->95, cdpnnp->80, lacck->60, cgpnsvcrqd-> 60, asdlkup->50, grnlkup->50, cgpnasdrqd->50, cgpngrnrqd->50, inprtg->95, skgtartg->50 cdial->10. • The SA and Precedence of Idprcgpn service is inprtg->95, blklstqry->90, blklstrly->90, cgpnnp->80, cgpnrtg->70, asdlkup>50, grnlkup->50, cdial->10. • The SA and precedence of Mosmsgcdpnservice is pprelay->80, cdpnnp->60, asdlkup->50, grnlkup->50, cgpnasdrqd->50, cgpngrnrqd->50, cdial->10. • The SA and Precedence of Mosmsgcgpn service is fraudchk->90, pprelay->80, asdlkup->50, grnlkup->50, cdial->10. • The SA and Precedence of Tif Cdpn Service (i.e Tif, Tif2, Tif3) is crp->92, fpfxrls->92, blrls->91, blnfndrls->91, selscr->91, npnrls->91, asdlkup->90, cgpnasdrqd->90, grnlkup->90, cgpngrnrqd->90, cgpnsvcrqd->80, nprelay->80, nprls->80, nocgpnrls->80, nscdpn->80, snscgpn->75, nscgpn->75, cdial->10, fwdscs->5 • The SA and Precedence of Tifcgpn service (i.e Tifcgpn, Tifcgpn2, Tifcgpn3) is fpfxrls->92, blrls->91, blnfndrls->91, asdlkup->90, grnlkup->90, cgpnnp->80, snscgpn->75, nscgpn->75, cdial->10.
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

Table 5-30 (Cont.) NPP Services Fields

Field	Description	Data Input Notes
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
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

Table 5-30 (Cont.) NPP Services Fields

Field	Description	Data Input Notes
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
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 fields 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 Fields

Field	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 fields 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 Fields

Field	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': 'Imsipfx'

Table 5-32 (Cont.) Common Screening Lists Fields

Field	Description	Data Input Notes
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 fields 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 Fields

Field	Description	Data Input Notes
CondCGPN	The preconditioning required when a CgPN lookup is needed.	Default='None' Range = 'Addcc', 'None'
CondRDN	The preconditioning required when redirecting number.	Default='None' Range = 'Addcc', 'None'
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 Fields

Field	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'
NSPUBLIC	The value of the Calling Party Category that indicates that the Calling Party number is public.	Default=0 and Range = 0-255

Table 5-33 (Cont.) TIF Options Fields

Field	Description	Data Input Notes
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'
SPLITIAM	This parameter specifies when to split the IAM into IAM + 1 SAM.	Default='None' and Range = 15-31
SUBCDPN	Substitute CdPN, provides a set of digits to substitute for CdPN. Use this when SA is TIFRDNBL.	[Default='None' and Range = a-f, A-F, 0-9 and Maximum Length = 10]

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 fields 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 Fields

Field	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
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'

Table 5-34 (Cont.) IDPR Options Fields

Field	Description	Data Input Notes
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'
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'

Table 5-34 (Cont.) IDPR Options Fields

Field	Description	Data Input Notes
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
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

Table 5-34 (Cont.) IDPR Options Fields

Field	Description	Data Input Notes
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']
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 fields 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 Fields

Fields	Description	Data Input Notes
Board Type	This field defines the Type of Board.	Default = eLynx Range = eLynx, ADAX
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]
Encoding Scheme	Indicator for use of B8ZS, HDB3 or AMI encoding/decoding	.
Minimum Signal Unit Rate	Minimum signal unit rate. The minimum number of SUs present on a link uniformly distributed.	Default = 1000 Range = 400-2000

Table 5-35 (Cont.) Interface Mapping Fields

Fields	Description	Data Input Notes
2 Spare International Bits	Value of two Spare International bits of NFAS data.	[Default = 0; Range = 0-3]
5 Spare National Bits	Value of five Spare International bits of NFAS data.	[Default = 0; Range = 0-31]
Framing	Indicator for framing format.	Default: FRAMING_SF
CRC	Defines if crc should be enabled or disabled.	Default: Yes
T1 Cable Length	T1 cable length in feet between the nodes	[Default = 133; Range = 0-655]
Error Correction Method	Error Correction Method.	Default: BASIC
MSU Retransmission Threshold	Threshold of the number of MSUs available for retransmission. If the error correction method being used is PCR and this threshold is reached, no new MSUs or FISUs are sent. The retransmission cycle is continued up to the last MSU entered into the retransmission buffer in the order in which they were originally transmitted.	[Range = 1-1023]
MSU Octet Retransmission Threshold	Threshold of the number of MSU octets available for retransmission. If the error correction method being used is PCR, and this threshold is reached, no new MSUs or FISUs are sent. The retransmission cycle is continued up to the last MSU entered into the retransmission buffer in the order in which they were originally transmitted.	[Range = 300-287744]

You can perform add, edit, or delete tasks on **VSTP>Configuration>Interface 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 fields 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 Fields

Field	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.
T1 Timer	Alignment timer in milliseconds. The amount of time M2PA waits to receive a Link Status Alignment message from the peer.	Typical value is 10000. Default: 35000, minimum: 1000, maximum: 350000

Table 5-36 (Cont.) M2PA Config Fields

Field	Description	Data Input Notes
T2 Timer	M2PA Timer "not aligned" in milliseconds.	Typical value is 2000. Default: 20000, minimum: 5000, maximum: 150000
T3 Timer	Ready Timer in milliseconds. The amount of time after proving that M2PA waits to receive a Link Status Ready message from the peer.	Typical value is 2000. Default: 2000, minimum: 1000, maximum: 60000
T4 Emergency Timer	Emergency proving timer in milliseconds. The amount of time M2PA generates Link Status Proving messages during emergency proving.	Typical value is 500. Default: 500, minimum: 400, maximum: 5000
T4 Normal Timer	Normal proving timer in milliseconds. The amount of time M2PA generates Link Status Proving messages during normal proving.	Typical value is 10000. Default: 30000, minimum: 1000, maximum: 70000
T5 Timer	Busy rate timer in milliseconds. The amount of time between sending Link Status Busy messages while the link is in service.	Typical value is 100. Default: 100, minimum: 80, maximum: 10000
T6 Timer	Remote congestion timer in milliseconds. The amount of time that a congested link will remain in service.	Typical value is 3000. default: 3000, minimum: 1000, maximum: 6000
T7 Timer	Excessive acknowledgment delay timer in milliseconds. The maximum amount of time that can pass between transmission of a user data message and receipt of an acknowledgment for that message from the peer. If this timer expires, the link is taken out of service.	Typical value is 1200. default: 1200, minimum: 200, maximum: 2000
T16 Timer	Proving rate timer in milliseconds. The amount of time between sending Link Status Proving messages while T2N or T2E is running.	Range: 1 - 500 Default: 200
T17 Timer	Ready rate timer in milliseconds. The amount of time between sending Link Status Ready messages while T3 is running.	Typical value is 250. default: 250, minimum: 100, maximum: 500
T18 Timer	Processor outage rate timer in milliseconds. The amount of time between sending Link Status Processor Outage messages while the link is in service.	Range: 100 - 10000 Default: 1000

> **Note**
>
> The timer values discussed in the above table are in milliseconds.

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 fields 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 Fields

Field	Description	Data Input Notes
Name	Name for this M3ua 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.
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 500. Minimum 500, Maximum: 10000 Default: 2000

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 fields 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 Fields

Fields	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.	Default: false
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.	Default: false
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.	Default: false

Table 5-38 (Cont.) M3rl Options Fields

Fields	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.	Default: false
CnvClgItu	This parameter enables or disables the CGPA conversion for Itui/Itui_s/Itun/Itun_s domain crossing during SCCP conversion.	Default: Off
GtCnvDflt	This parameter enables routing of SCCP messages using system defaults when an appropriate entry is not found in the Default GT Conversion Table.	Default: false
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.	Default: false
Randsls	Random SLS (signaling link selection).This parameter is used to apply random SLS generation on a per linkset basis.	Default: Off
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.	NA
Slscnv	This parameter is used as Per node SLS conversion indicator.	Default: Off
SlsReplace	This parameter allows to replace the SLS for an ANSI message with a random generated SLS value by Random SLS feature	Default: false
SlsocbEnabled	This parameter turns on the Other CIC (Circuit Identification Code) Bit Used feature	Default: false
SparePCSupportEnabled	Checks whether the support for ITUN-Spare and ITUI-Spare is enabled or disabled.	Default: true
Performance Measurement	This parameter is used for turning on/off the performance counter measurements. If turned on, it will start updating timing data on various layers.	Default: Off

Table 5-38 (Cont.) M3rl Options Fields

Fields	Description	Data Input Notes
M2PA Rx Busy Link	This parameter is used for enabling early detection of congestion by monitoring SCTP receive buffers and sending of M2PA Busy Link Indication based on the SCTP buffer status. By default, the parameter is Off and the existing implementation of Reserved Link TPS and Max Link TPS will be used to send M2PA Busy Link Indication.	Default value: Off
PCT	PCT presents three options: On, Off, and Lset: • PCT "On": The PCT will apply on all the MSUs. • PCT "Off": The PCT will not apply on any of the MSUs. • PCT is set to LSet: The PCT table lookup will only be used for MSUs entering or exiting a link that is a part of a linkset for which PCT is enabled.	Default "value": Off
`ttMapSupport`	This parameter is used for turning on or off the TT Map feature.	Enum Value: "On", "Off" Default Value: Off Data Type: String
Proxy Point Code Support	This parameter is used for turning on or off the Proxy point code feature.	Enum Value: "On", "Off" Default Value: Off Data Type: String
XList Expiry Timer Duration	This parameter is used for setting timer whenever a x-list entry is created or updated or used for routing.	Range: 20-1440 mins Default: 60 mins
XList Cluster Threshold	This parameter is used for setting threshold. It is represented in percent.	Range: 0-100 percent Default: 90 percent
CNCF	This parameter is used for turning On or Off the CNCF feature.	Range: On, Off

Navigate to **VSTP** and then, **Configuration**, click **M3rl Options** page to perform the edit task.

Editing a M3rl Option

Following are the steps to change the field values for a selected M3rl Option. :

1. Go to **VSTP**, then click **Configuration** and select **M3rl Options** page.
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 fields 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 Fields

Field	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	Waiting to repeat signalling route set test message.	Default value is 30000. [MIN,MAX] = [20000,90000]
Timer 11	Transfer restricted timer.	Default value is 30000. [MIN,MAX] = [1000,90000]
Timer 12	Waiting for uninhibit acknowledgement.	Default value is 800. [MIN,MAX] = [100, 2000]
Timer 13	Waiting for force uninhibit.	Default value is 800.[MIN,MAX] = [100, 2000]
Timer 15	Waiting to start signalling route set congestion test.	Default value is 3000.[MIN,MAX] = [200,4000]
Timer 16	Waiting for route set congestion status update.	Default value is 1400.[MIN,MAX] = [200,3000]
Timer 17	Delay to avoid oscillation of initial alignment failure and link restart.	Default value is 800.[MIN,MAX] = [500, 2000]
Timer 18	Repeat transfer restricted (TFR) once by response method.	Default value is 10000. [MIN,MAX] = [2000,20000]
Timer 1	Delay to avoid message mis-sequencing on changeover.	Default value is 800.[MIN,MAX] = [100,2000]

Table 5-39 (Cont.) MTP3 Configs Fields

Field	Description	Data Input Notes
Timer 2	Waiting for changeover acknowledgement.	Default value is 1400.[MIN,MAX] = [100,3000]
Timer 23	Remote inhibit test timer.	Default value is 180000. [MIN,MAX] = [180000,360000]
Timer 3	Time controlled diversion-delay to avoid mis-sequencing on changeback.	Default value is 800.[MIN,MAX] = [100,2000]
Timer 4	Waiting for changeback acknowledgement (first attempt).	Default value is 800.[MIN,MAX] = [100,2000]
Timer 5	Waiting for changeback acknowledgement (second attempt).	Default value is 800.[MIN,MAX] = [100,2000]
Timer 6	Delay to avoid message mis-sequencing on controlled rerouting.	Default value is 800.[MIN,MAX] = [100,2000]
Timer 8	Transfer prohibited inhibition timer (transient solution).	Default 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 fields 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 Fields

Field	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.
T1 Timer	Alignment or Ready timer.	Range = Minimum: 5000, Maximum: 350000 (milliseconds) **Values:** • ANSI timer sets 5000 – 20000 • ITU timer sets 40000 – 50000 • E1 HSL timer sets 25000 – 350000 • T1 HSL timer sets 16000 – 151000
T2 Timer	Not Aligned timer.	Range = Minimum: 5000, Maximum: 480000 (milliseconds) **Values:** • ANSI timer sets 5000 – 30000 • ITU timer sets 5000 – 150000 • E1 HSL timer sets 5000 – 150000 • T1 HSL timer sets 5000 – 14000

Table 5-40 (Cont.) MTP2 Config Fields

Field	Description	Data Input Notes
T3 Timer	Aligned timer.	Range = Minimum: 1000, Maximum: 20000 (milliseconds) **Values:** • ANSI timer sets 5000 – 20000 • ITU timer sets 1000 – 2000 • E1 HSL timer sets 1000 – 2000 • T1 HSL timer sets 5000 – 14000
T4 Emergency Timer	Proving period Emergency timer.	Range = Minimum: 200, Maximum: 10000 (milliseconds) **Values:** • ANSI timer sets 200 – 1000 • ITU timer sets 400 – 600 • E1 HSL timer sets 400 – 600 • T1 HSL timer sets 3000 – 10000
T4 Normal Timer	Proving period normal timer.	Range = Minimum: 500, Maximum: 70000 (milliseconds) **Values:** • ANSI timer sets 500 – 5000 • ITU timer sets 7500 – 9500 • E1 HSL timer sets 3000 – 70000 • T1 HSL timer sets 3000 – 30000
T5 Timer	Sending SIB timer.	Range = Minimum: 40, maximum: 500 (milliseconds) **Values:** • ANSI timer sets 40 – 500 • ITU timer sets 80 – 120 • E1 HSL timer sets 80 – 120 • T1 HSL timer sets 80 – 120
T6 Timer	Remote congestion timer.	Range = Minimum: 1000, Maximum: 10000 (milliseconds) **Values:** • ANSI timer sets 1000 - 10000 • ITU timer sets 3000 - 6000 • Q.703 timer sets 3000 - 6000 • T1 HSL sets 3000 - 6000
T7 Timer	Excessive delay of acknowledgment timer.	Range = Minimum: 200, maximum: 3000 (milliseconds) **Values:** • ANSI timer sets 200 – 3000 • ITU timer sets 500 – 2000 • E1 HSL timer sets 500 – 2000 • T1 HSL timer sets 500 – 2000

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. This is a mandatory field.	Valid vlr number are numerical values having length between one and 16 characters, inclusive.
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, 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']
Skip Cross Protocol Check	This parameter defines whether or not to skip 3G/4G cross protocol validation for same MCC.	[Default='No', Range= 'No', 'Yes']
Home MCC	Home Mobile Country Code is a three digit unique code which identifies a country or geographical area.	It should support any 3 digits hexa decimal number or None.
CommonDbAging	This parameter verifies the aging of UDR record.	Default: On or Off

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.	Allowed pattern is digit strings of 5 or 6 characters length.
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**

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.	

Table 5-48 (Cont.) CAT2 GTAs Elements

Element	Description	Data Input Notes
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**

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. This is a mandatory field.	Upto 20 alphanumeric characters allowed.
Direction of Conversion	Direction of Conversion This is a mandatory field.	
Global Title Indicator Conversion	Global Title Indicator conversion. This is a mandatory field.	
ANSI Translation Type	ANSI Translation Type. This is a mandatory field.	Upto 3 numerical characters allowed.
ITU Translation Type	ITU Translation Type. This is a mandatory field.	Upto 3 numerical characters allowed.
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 numerical 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 numerical 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	Numerical characters with 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 hexadecimal 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.	Numerical characters with 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 hexadecimal 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. MMI clients never define vSTP feature names, but instead discover the available names from the collection GET response. A client must then use the vSTP provided feature name string when making a GET or PUT request for a particular Feature.	
Feature Status	A vSTP Feature's administrative state can either be Enabled or Disabled. **Note:** The administrative state of a vSTP feature can either be **Enabled** or **Disabled** as follows: • The vSTP feature **TBGTTLS** is initially in the **Disabled** administrative state when the system is installed and it cannot be disabled once enabled. • The vSTP feature **WGTTLS** is initially in the **Disabled** administrative state when the system is installed and can be enabled and disabled any number of times. Enabling and disabling the **WGTTLS** feature requires restart of the MPs.	A vSTP feature remains in the **Disabled** administrative state after system installation.

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

Table 5-52 (Cont.) 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**

5.1.54 Security Log Config

The Security Log Config maintains all configuration values that governs the functionality of security logging in the file directory of SOAM.

All configurations of Security Log Config is done at the SOAM.

The Security Log Config can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **Security Log Config** page. The page displays the elements on the **Security Log Config** Edit pages.

> **Note**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-53 Security Log Config Elements

Element	Description	Data Input Notes
Security Logging Feature	Global Parameter for Security Logging feature which should be enabled before provisioning any logging task.	Default = Off Range = On,Off
Site Identifier	Parameter to identify logging site.	Range = Allowable values are single word with alphanumeric characters or nothing at all. Words may have '_' or '-' aswell. Default = null
Directory Path of MP Log	Directory path of MP for logging.	Default: `/var/TKLC/db/filemgmt/securityLog/` Maximum Length: 300
Timeout for Log File	Timeout in seconds after which new file will be created for logging.	Default: 90 Range: 60-120
Maximum Logs Per File	Maximum logs to be created per file, after which new file would be created.	Default: 1500000 Range = 600000 - 3000000
Minimum Disk Space for Logging	Minimum available disk space in current directory filesystem to be allocated for logging.	Default: 30 Range = 10-100

You can perform edit task on **VSTP**>**Configuration**>**Security Log Config** page.

Editing a Security Log Config

Use this procedure to change the field values for a selected Security Log Config:

1. Enter the updated values on **Editing Security Log Config** page.
2. Click , **Apply** or **Cancel**

5.1.55 Accounting Measurement Options

The Accounting Measurement Options are those configuration values that govern the overall Accounting Measurement functionality. There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The Accounting Measurement Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **Accounting Measurement Options** page. The page displays the elements on the **Accounting Measurement Options** Edit page.

Table 5-54 Accounting Measurement Options Elements

Element	Description	Data Input Notes
Account Measurement Feature Option	This parameter defines whether system wide Accounting Measurement is On or Off.	Default: No Range: Yes, No

Table 5-54 (Cont.) Accounting Measurement Options Elements

Element	Description	Data Input Notes
DPC CDPA Account Measurement Option	This parameter defines whether DPC with SCCP Called Party Accounting Measurement is On or Off.	Default: No Range: Yes, No
DPC CGPA Account Measurement Option	This parameter defines whether DPC with SCCP Calling Party Accounting Measurement is On or Off.	Default: No Range: Yes, No
DPC Linkset Account Measurement Option	This parameter defines whether Linkset with DPC Accounting Measurement is On or Off.	Default: No Range: Yes, No
DPC SI NI Account Measurement Option	This parameter defines whether DPC with SI and NI Accounting Measurement is On or Off.	Default: No Range: Yes, No
GTT On Inter Network Connect Account Measurement Option	This parameter defines whether GTT on Inter Connecting Network Measurement is On or Off.	Default = No Range = No, Yes
GTT Rule Per Linkset Account Measurement Option	This parameter defines whether GTT rule per Linkset Accounting Measurement is On or Off.	Default = No Range = No, Yes
Linkset SI Account Measurement Option	This parameter defines whether Linkset with SI Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC CDPA Account Measurement Option	This parameter defines whether OPC with SCCP Called Party Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC CGPA Account Measurement Option	This parameter defines whether OPC with SCCP Calling Party Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC DPC Account Measurement Option	This parameter defines whether OPC with DPC Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC DPC SI Account Measurement Option	This parameter defines whether OPC with DPC and SI Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC Linkset Account Measurement Option	This parameter defines whether Linkset with OPC Accounting Measurement is On or Off.	Default: No Range: Yes, No
OPC SI NI Account Measurement Option	This parameter defines whether OPC with SI and NI Accounting Measurement is On or Off.	Default: No Range: Yes, No

You can perform edit task on **VSTP**>**Configuration**>**Accounting Measurement Options** page.

Editing a Accounting Measurement Options

Use this procedure to change the field values for a selected Accounting Measurement Options. (The **Accounting Measurement Options Name** field cannot be changed.):

1. Enter the updated values on the **Editing a Accounting Measurement Option** page.
2. Click **Apply** or **Cancel** .

5.1.56 SMS Proxy Options

The SMSProxy Options are those configurable values which govern the overall of Service MP framework.There is a single instance of this resource, which contains each of the individual options that can be retrieved and set.

The SMS Proxy Options can only be updated and cannot be created or deleted.

Select the **VSTP**, and then **Configuration**, and then **SMS Proxy Options** page. The page displays the elements on the **SMS Proxy Options** Edit page.

Table 5-55 SMS Proxy Options Elements

Element	Description	Data Input Notes
MOFSM Default Action	Default Action for MOFSM message validation failure.	Range:FallBack, Discard, Udts, TcapError, Default: Discard
MOFSM Error Code	If Default action is Udts or TcapError, this error code is sent in response.	Maximum: 255, Minimum: 0, Default: 0
MTFSM Default Action	Default Action for MT-FSM message validation failure.	Range:FallBack, Discard, Udts, TcapError, Default: Discard
MTFSM Error Code	If Default action is Udts or TcapError, this error code is sent in response.	Maximum: 255, Minimum: 0, Default: 0
MOFSM SCCP Validation	Whether to perform SccpVal for MO-FSM message.	Range:On/Off, Default: On
MTFSM SCCP Validation	Whether to perform SccpVal for MT-FSM message.	Range:On/Off, Default: On
MTFSM Invoke Timer	MT-FSM Timer. The MT-FSM should be received within this timer once the SRI-SM-Ack is sent to the originator.	Maximum:120, Minimum: 30, Default: 60
SMS Delivery Status Timer	Initiated after MTFSM is forwarded to the VLR. The SMS Delivery Status (if required) should be received before this timer expires.	Maximum:120, Minimum: 30, Default: 60
Sms Proxy GTA	Global Title Address digits to identify the SMS Proxy Service.	Range:5-15 Digits.
SMS Proxy Service Translation Type	Translation type of CGPA to be used by the SMS Proxy service when generating Messages towards HLR.	Maximum: 255, Minimum: 0, Default: 0
Scrambled IMSI Range Prefix	Prefix Digits for the Scrambled IMSI. Also defines the range of Scrambled IMSIs to be used.	Range:5-10 Digits

Table 5-55 (Cont.) SMS Proxy Options Elements

Element	Description	Data Input Notes
Defcc	Default country code.	

You can perform edit task on **VSTP**>**Configuration**>**SMS Proxy Options** page.

Editing a SMS Proxy Options

Use this procedure to change the field values for a selected SMS Proxy Options:

1. Enter the updated values on the **Editing a SMS Proxy Option** page.
2. Click **Apply** or **Cancel** .

5.1.57 SMS Proxy SMSC Status

This table informs if SMSC status is Allowlist or BlockList.

Select the **VSTP**, and then **Configuration**, and then **SMS Proxy SMSC Status** page. The page displays the elements on the **SMS Proxy SMSC Status** View, Insert, and Edit pages.

> **Note**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-56 SMS Proxy SMSC Status Elements

Element	Description	Data Input Notes
SMSC GTT Address	Global Title Address of SMSCs to be allowlisted or blocklisted. [A value is required.]	
SMSC Status	Indicates allowlist or blocklist status of SMSC. [A value is required.]	

You can perform add, edit, or delete tasks on **VSTPConfigurationSMS Proxy SMSC Status** page.

Adding a SMS Proxy SMSC Status

Perform the following steps to configure a new SMS Proxy SMSC Status:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a SMS Proxy SMSC Status

Use this procedure to change the field values for a selected SMS Proxy SMSC Status. (The **SMS Proxy SMSC Status Name** field cannot be changed.):

1. Select the **SMS Proxy SMSC Status** row to be edited.

2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a SMS Proxy SMSC Status

Use the following procedure to delete a SMS Proxy SMSC Status.

1. Select the **SMS Proxy SMSC Status** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.58 Generic Name

Using Generic name, you can block messages with specific generic name on certain linkset.

Select the **VSTP**, and then **Configuration**, and then **Generic Name** page. The page displays the elements on the **Generic Name** View, Insert, and Edit pages.

> **Note**
>
> Data Input Notes apply to the Insert and Edit pages only; the View page is read-only.

Table 5-57 Generic Name Elements

Element	Description	Data Input Notes
Generic Name	Generic Name. [A value is required.	Generic Name is case insensitive. Valid values are (0-9, A-Z), * as Wildcard, and following special characters: **! @ # $ ^ & ? ( ) { } [ ] ; , + : _ . \" - / ' space.** Preceeding and succeeding spaces will be trimmed, whereas consecutive spaces in the middle of generic name are not allowed.
Set Type	Generic Name Set type. [A value is required.]	[Range = SetA, SetB, Both]

You can perform add, edit, or delete tasks on **VSTPConfigurationGeneric Name** page.

Adding a Generic Name

Perform the following steps to configure a new Generic Name:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Editing a Generic Name

Use this procedure to change the field values for a selected Generic Name. (The **Generic Name Name** field cannot be changed.):

1. Select the **Generic Name** row to be edited.
2. Click **Edit**
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**

Deleting a Generic Name

Use the following procedure to delete a Generic Name.

1. Select the **Generic Name** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

5.1.59 TT Maps

Using the TT Map, the Signaling Connection Control Part (SCCP) known as party address translation type of UDT/XUDT message incoming or outgoing on certain `linkset` can be changed by defining alternative TT Mapping.

TT Maps displays the elements View, Insert, and Edit pages.

Select the **VSTP**, and then **Configuration**, and then **TT Maps** page.

Table 5-58 TT Maps Elements

Element	Description	Data Input Notes
TT Map Name	Unique name of the TT Map	Default Value: NA Data Type: String Range: 32 characters Valid characters are alphanumeric and underscore. Range must contain at least one alpha and must not start with a digit. This is a mandatory value.
LinkSet Name	Name of the linkset associatied with the TT Map.	Default Value: NA Format: Drop-down menu
Ingress Egress	Defines Ingress Egress for this TT map. When set to ingress the TT map is applied to the incoming MSU at vSTP. When set to egress the TT map is applied to the outgoing MSU from vSTP.	Range: Ingress or Egress This is a mandatory value.
Existing Translation Type	Defines the existing translation type (TT) for this TT Map	Range: 0 to 255 This is a mandatory value.
Modified Translation Type	Defines the modified translation type (TT) for this TT Map	Range: 0 to 255 This is a mandatory value.

Adding a TT Map

Perform the following steps to configure a new TT Map:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**.

Editing a TT Map

Use this procedure to change the field values for a selected TT Map.

> **Note**
>
> The **TT Map Name** field cannot be changed.

1. Select the **TT Map** row to be edited.
2. Click **Edit**.
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**.

Deleting a TT Map

Use the following procedure to delete a TT Map:

1. Select the **TT Map** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

> **Note**
>
> A linkset cannot be deleted if it is used in any of the TT Maps.

5.1.60 PCT

Using Point code and CIC translation (PCT), you can define different translations that can change Destination Point Code (DPC), Origination Point Code (OPC), or Circuit Identifier Code (CIC) of an MTP-routed message.

Mandatory parameters

> **Note**
>
> The View page is read-only, and the Data Input Notes only apply to the Insert page.

Table 5-59 PCT Elements

Element	Description	Data Input Notes
Domain	This defines the valid PCT domain.	Range: ["Ansi", "Itui", "Itun"] This is a mandatory value.

Table 5-59 (Cont.) PCT Elements

Element	Description	Data Input Notes
Emulated Point Code	This defines the Emulated Point Code. More than one PCT can have this point code.	Data Type: String Format: "^([0-9]+-){2}[0-9]+$" For Ansi: Full point codes only. For ITUI and ITUN: Spare are not allowed. This is a mandatory value.
Emulated PC Group Code	This defines the ITUN group code for the duplicate point code feature for Emulated Point Code. This is allowed for ITUN Domain.	Data Type: String Format: "^([a-z]{2})$" Default Value: “aa” for ITUN Domain. Other domain: NA
Real Point Code	This defines the Real Point Code. More than one PCT can have the Real Point Code.	Data Type: String Format: "^([0-9]+-){2}[0-9]+$" For Ansi: Full point codes only. For ITUI and ITUN: Spare are not allowed. This is a mandatory value.
Real PC Group Code	This defines ITUN group code for duplicate point code feature for Real Point Code. Only allowed for ITUN Domain.	Data Type: String Format: "^([a-z]{2})$" Default Value = “aa” for ITUN Domain. Other domain: NA
Filter Point Code	It defines the Filter Point Code.	Data type: String Format: "^(([0-9]+-){2}[0-9]+|*)$" For Ansi: Full point code and Wildcard(*) is allowed. For ITUI and ITUN: Spare are not allowed.
Filter PC Group Code	This defines the ITUN group code for duplicate point code feature for Filter Point Code, only allowed for ITUN Domain.	Data Type: String Format: "^([a-z]{2})$" Default Value = “aa” for ITUN Domain. Other domain: NA
ECICS	This defines the Start of Emulated CIC range, only used if SI is 5 (ISUP), 13 (Q.BICC).	Data Type: String Wildcard(*) is allowed. Range: • 0-4095 (For ITU ISUP). • 0-16383 (For ANSI ISUP). • 0- 4294967295 (For ANSI Q. BICC).
ECICE	This defines the End of Emulated CIC range, only used if SI is 5 (ISUP), 13 (Q.BICC).	Data Type: String Wildcard(*) is allowed. Range: • 0-4095 (For ITU ISUP). • 0-16383 (For ANSI ISUP). • 0- 4294967295 (For ANSI Q. BICC).

Table 5-59 (Cont.) PCT Elements

Element	Description	Data Input Notes
RCICS	This defines the Start of Real CIC range, only used if SI is 5 (ISUP), 13 (Q.BICC).	Data Type: String Wildcard(*) is allowed. Range: • 0-4095 (For ITU ISUP). • 0-16383 (For ANSI ISUP). • 0- 4294967295 (For ANSI Q. BICC).
RCICE	This defines the End of Real CIC range; Only used if SI is 5 (ISUP), 13 (Q.BICC).	Data Type: String Wildcard(*) is allowed. Range: • 0-4095 (For ITU ISUP). • 0-16383 (For ANSI ISUP). • 0- 4294967295 (For ANSI Q. BICC).
PCT Service Indicator	This describes the SS7 Service Indicator code, which uses the destination code to deliver the message to the MTP user.	Data Type: String Range: • 0 (NM) • 3 (SCCP) • 5 (ISUP) • 13 (Ansi Q BICC) • Wildcard(*) is allowed.
PCT Subsystem Number	This defines the PCT Subsystem Number, used when SI is 3.	Data Type: String Range: • 0-255 • Wildcard(*) is allowed.
Unique Identifier	Defines a unique identifier for this Point code and CIC Translation. This Unique identifier value will be used for GET and DELETE operations. Unique identifier for PCT will be auto generated UUID. You can fetch auto generated Unique Identifier (UUID) from MMI Get response.	Data type: UUID Auto generated, not editable by user.

Adding a PCT

Perform the following steps to configure a new PCT:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**.

Deleting a PCT

Resource PCT (/vstp/pcts)

Perform the following steps to delete a PCT:

1. Select the **PCT** to be deleted.
2. Click **Delete**.

3. Click **OK** or **Cancel**.

5.1.61 Trace Filter Params

Using Trace Filter Params, a customer can apply filter on traces through filter parameters. All configuration of Trace Filter Params is done at the SOAM

Select the **VSTP**, and then **Configuration**, and then **Trace Filter Params** page. The page displays the elements on the **Trace Filter Params**. View, Insert, and Edit pages.

Table 5-60 Trace Filter Params

Element	Description	Data input Notes
Trace Enabled	Defines a filter's administrative state, that can be either Enabled or Disabled. A Trace's rep & duration parameter can only be modified if the state is Disabled.	Default Value: No Range: Yes, No.
Rep	Rep can be configured to enable maximum number of messages, tracing can be applicable for respective `traceId`.	Default Value: 10 (If duration is not configured), 5000 (If duration is configured). Range: 1-5000
Duration	The duration for which the trace filter will act upon.	Default Value: 15(If rep is not configured), 60 (if rep is configured). Range: 1-60
SI	Defined as 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: 0-5
MSG Type	Defined as SCCP Message Type.	Default enum value: • UDT: 9 • UDTS: 10 • XUDT: 17 • XUDTS: 18 Range: UDT, UDTS, XUDT, XUDTS.
CDSSN	Defined as CdPA subsystem number.	Range: 2-255
CGSSN	Defined as CgPA subsystem number.	Range: 2-255
Domain	Defined as a type of SS7 domain.	Range: None, ANSI, ITUI, ITUN, ITUN24, ITUI_S, ITUN_S.
OPC	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn), or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range: Valid characters are integers, plus (+) and minus (-) sign. Maximum allowed length is 11.

Table 5-60 (Cont.) Trace Filter Params

Element	Description	Data input Notes
DPC	Ansi destination point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn); or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range: Valid characters are integers, plus (+) and minus (-) sign. Maximum allowed length is 11.
CDPC	Ansi called party point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn); or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range: Valid characters are integers, plus (+) and minus (-) sign. Maximum allowed length is 11.
CGPC	Ansi calling party point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn), or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range: Valid characters are integers, plus (+) and minus (-) sign. Maximum allowed length is 11.
CDRI	Defined as Calling Party Routing indicator.	Range: None, SSN, GT.
CGRI	Defined as Calling Party Routing indicator.	Range: None, SSN, GT.
CDTT	Defines the Called Party Translation Type (TT).	Range: 0 - 255
CGTT	Defines the Calling Party Translation Type (TT).	Range: 0 - 255
CDNAI	Defines Called Party Nature of Address Indicator. When set to International, then Nature of Address indicator (NAI) is International number. When set to National, then Nature of Address indicator (NAI) is National significant number. When set to Reserved, then Nature of Address indicator (NAI) is Reserved for National use. When set to Subscriber, then Nature of Address indicator (NAI) is Subscriber Number. When we set Spare then nature of address indicator(NAI) is Spare.	Range: Subscriber, Reserved, National, International, Spare.

Table 5-60 (Cont.) Trace Filter Params

Element	Description	Data input Notes
CDNAIV	Value for the Called nature of Address indicator. Value 1 refers to Subscriber `natureOfAddressIndicator`. Value 2 refers to `Reserved natureOfAddressIndicator`. Value 3 refers to `National natureOfAddressIndicator`. Value 4 refers to `International natureOfAddressIndicator`. Value 5-127 refer to spare values, value 0 refers to Unknown `natureOfAddressIndicator`.	Enum Value: There is no enum corresponding to 0 and 5-127 range For these values, only `natureOfAddressIndicatorValue` can be set. Maximum: 127 Minimum: 0
CDNP	Value for the Called Party Numbering Plan. When set to E164, then Numbering plan is ISDN/telephony numbering plan. When set to X121, then Numbering plan is Data numbering plan. When set to F69, then Numbering plan is Telex numbering plan. When set to E210, then Numbering plan is Maritime mobile numbering plan. When set to E212, then Numbering plan is Land mobile numbering plan. When set to E214, then Numbering plan is ISDN/mobile numbering plan. When set to Private, then Numbering plan is Private network or network-specific numbering plan. When set to Generic, then Numbering plan is Generic numbering plan.	Range: E164, X121, F69, E210, E212, E214, Private, Generic.
CDNPV	Value for the called numbering plan. Value 1 refers to Isdn numberingPlanValue. Value 2 refers to Generic numberingPlanValue. Value 3 refers to Data numberingPlanValue. Value 4 refers to Telex numberingPlanValue. Value 5 refers to Maritime numberingPlanValue. Value 6 refers to Land. Value 7 refers to IsdnMobile numberingPlanValue. Value 8 refers to Private numberingPlanValue. Value 9-15 refers to Spare numberingPlanValue. Value 0 refer to Unknown numberingPlanValue.	Enum Value: There is no enum corresponding to 0 and 9-15 range For these values, only `numberingPlanValue` can be set. Maximum: 15 Minimum: 0
CGNAI	Defines Called Party Nature of Address indicator. When set to International, then Nature of Address indicator (NAI) is International number. When set to National, then Nature of Address indicator (NAI) is National significant number. When set to Reserved, then Nature of Address indicator (NAI) is Reserved for National use. When set to Subscriber, then Nature of Address indicator (NAI) is Subscriber Number. When we set Spare then nature of address indicator(NAI) is Spare.	Range: Subscriber, Reserved, National, International, Spare.

Table 5-60 (Cont.) Trace Filter Params

Element	Description	Data input Notes
CGNAIV	Value for the Calling nature of Address indicator. Value 1 refers to Subscriber `natureOfAddressIndicator`. Value 2 refers to Reserved `natureOfAddressIndicator`. Value 3 refers to National `natureOfAddressIndicator`. Value 4 refers to International `natureOfAddressIndicator`. Value 5-127 refer to spare values. value 0 refers to Unknown `natureOfAddressIndicator`.	Enum Value: There is no enum corresponding to 0 and 5-127 range For these values, only `natureOfAddressIndicatorValue` can be set. Maximum: 127 Minimum: 0
CGNP	Value for the Calling Party Numbering Plan. When set to E164, then Numbering plan is ISDN/telephony numbering plan. When set to X121, then Numbering plan is Data numbering plan. When set to F69, then Numbering plan is Telex numbering plan. When set to E210, then Numbering plan is Maritime mobile numbering plan. When set to E212, then Numbering plan is Land mobile numbering plan. When set to E214, then Numbering plan is ISDN/mobile numbering plan. When set to Private, then Numbering plan is Private network or network-specific numbering plan. When set to Generic, then Numbering plan is Generic numbering plan.	Range: E164, X121, F69, E210, E212, E214, Private, Generic.
CGNPV	Value for the calling numbering plan. Value 1 refers to Isdn numberingPlanValue. Value 2 refers to Generic numberingPlanValue. Value 3 refers to Data numberingPlanValue. Value 4 refers to Telex numberingPlanValue. Value 5 refers to Maritime numberingPlanValue. Value 6 refers to Land Value 7 refers to IsdnMobile numberingPlanValue. value 8 refers to Private numberingPlanValue. Value 9-15 refers to Spare nnumberingPlanValue. Value 0 refer to Unknown numberingPlanValue.	Enum Value: There is no enum corresponding to 0 and 9-15 range For these values, only `numberingPlanValue` can be set. Maximum: 15 Minimum: 0
CDPA Address	Defined as Called party address.	Range:[a-f,A-F,0-9,*; Maximum Length = 21]. Only '*' is not allowed.
CGPA Address	Defined as Calling party address.	Range: [a-f,A-F,0-9,*; Maximum Length = 21]. Only '*' is not allowed.
Linkset Name	Name of the Link Set associated with trace filter, 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.	Range: [^(([A-Za-z][A-Za-z0-9_]*)|(_[A-Za-z0-9_]*[A-Za-z][A-Za-z0-9_]*))$]. Maximum length: 32

Adding a Trace Filter Params

Perform the following steps to configure the new trace filter params:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**.

Editing a Trace Filter Params

Use this procedure to change the field values for a selected trace filter params.

> **Note**
>
> **Trace ID** field cannot be changed. Only **Rep**, **Duration**, and **Trace Enabled** can be updated.

1. Select the **Trace Filter Params** row to be edited.
2. Click **Edit**.
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**.

Deleting a Trace Filter Params

Use the following procedure to delete a trace filter params:

1. Select the **Trace Filter Params** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

> **Note**
>
> If the **Trace Enabled** state is **Yes**, then the Trace Filter Params cannot be deleted.

5.1.62 Gserv Data

Select the **VSTP**, **Configuration**, and **Gserv** page. The page displays the fields on the **Gserv Data**. View and Insert pages.

Table 5-61 Gserv Data fields

Fields	Description	Range
Translation Type	Translation type of this G Serv. It can be any integer in the range 0 to 255.	Range: 0-255

Table 5-61 (Cont.) Gserv Data fields

Fields	Description	Range
OPC	Ansi originating point code with subfields network indicator-network cluster-network cluster member (ni-nc-ncm). ITU international originating point code with subfields zone-area-id. The prefix subfield indicates a spare point code (prefix-zone-area-id). ITU originating point code in the format of a 5-digit number (nnnnn); or 2, 3, or 4 numbers (members). The prefix subfield indicates a spare point code (prefix-nnnnn, prefix-nnnnn-gc, prefix-m1-m2-m3-m4, prefix-m1-m2-m3-m4-gc). 24-bit ITU national originating point code with subfields main signaling area-sub signaling area-signaling point (msa-ssa-sp).	Range: Maximum length allowed is 11
GTA	GTA can be any valid string.	Range: Maximum length allowed is 11
Domain	This defines the type of SS7 domain.	Range: None, ANSI, ITUI, ITUN, ITUN24, ITUI_S, ITUN_S

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.

Field	Description
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 • RspDisabled • LinksetDisabled
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
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.

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.
Route Status	The status of the route.
Route Cost	The relative cost assigned to this route. Lower cost routes are preferred over higher cost routes.
Adjacent PC	The specified adjacent point code.
Linkset	Name of the Linkset.
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	Time stamp that shows the last time the status information was updated.
Admin State	It displays the status (enable/disable) of the Remote Signaling Point.
Enable	It enables the specific Remote signaling Point.

Field	Description
Disable	It disables the specific Remote signaling Point. **Note** • Whenever user disables any RSP, then all the direct links specific to RSP will move to `DisabledRsp` admin state over Link Maintenance screen, and the `DisabledRsp` Link will become unavailable. • Any link in `DisabledRSP` admin state will not be enabled through linkset or link maintenance screen.

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.

Field	Description
Link Set Name	Name of the Linkset.
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.
Enable	It enables the specific Remote signaling Point.
Disable	It disables the specific Remote signaling Point. **Note** • Whenever user disables any linkset, then all the links specific to linkset will move to `DisabledLinkset` admin state over Link Maintenance screen, and the `DisabledLinkset` Link will become unavailable. • Any link in `DisabledLinkset` admin state will not be enabled through link maintenance screen.

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.
- 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.

5.2.7 XList Status

The **VSTP** > **Maintenance** > **XList Status** page allows you to view information about XLists.

vSTP Maintenance XList Status Fields

The following table describes fields on the XList Status maintenance page:

Field	Description
MP Server	Name of the vSTP MP server that is currently reporting the status of the XList.
RSP Name	Name of the RSP.
Point Code	Unique address of the RSP.
X List Status	
Routes	RSP route
Route Adjacent Status	The status of adjacent part. It can have the following 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. • UnavailableRspBlocked : The non-adjacent part to RSP is unavailable as it is blocked.
Route Status	
Route Cost	The relative cost assigned to this route.
Adjacent PC	The unique address of the adjacent RSP.
Linkset	Linkset configured with the RSP.
Status Known	Status can have the following values: • True: The RSP status is known. • False: The RSP status is unknown.
Last Updated	Time stamp that shows the last time the status information was updated.

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**.

> **Note**
>
> IR21.xml file uploads are not supported through GUI but are supported through the CLI.

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
Alarms, Errors, KPIs, and Measurements

This chapter describes the types of alarm, error, KPI, and measurements information that is available for vSTP.

6.1 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.

6.2 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.

6.3 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 6-1 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 6-1 (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.
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.

Table 6-1 (Cont.) GTT Actions Errors

Error Code Number	Description
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.
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 6-2 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.

Table 6-2 (Cont.) GTT Action Sets Errors

Error Code Number	Description
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.
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 6-3 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.
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.

Table 6-3 (Cont.) GTT Selectors Errors

Error Code Number	Description
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.
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 6-4 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.
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.

Table 6-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
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.
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.
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.

Table 6-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
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.
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.

Table 6-4 (Cont.) GTT Addresses Errors

Error Code Number	Description
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.
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 6-4 (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 6-5 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.
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.

Table 6-5 (Cont.) GTT Sets Errors

Error Code Number	Description
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 6-6 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.
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.

Table 6-6 (Cont.) Link Sets Errors

Error Code Number	Description
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.
50919 - ERR_LINK_SET_ASSOCIATED_WITH_TTMAP	Linkset associated with TT Map cannot be deleted.
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 6-7 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.

TT Maps

Resource TT Maps (/vstp/ttmaps)

TT Maps are those configuration values that define different TT Mapping that changes the SCCP.

Table 6-8 TT Maps Errors

Error Code Number	Description
ERR_OPR_FAILED_NO_ENTRY	TT Map does not exist.
ERR_TT_MAP_INVALID_ATTR' => '{attr}: Unknown Attribute.'	Any other invalid parameter is provided by MMI.
ERR_ONT_001	The value of mandatory parameter is not set.
ERR_ONT_002	An invalid value set for a parameter.

Table 6-8 (Cont.) TT Maps Errors

Error Code Number	Description
ERR_ONT_003	Linksetname provided in MMI does not exist.
50920	Cannot insert the provided value as the maximum number of TT Maps has already been configured (16,320).
50921	Cannot insert the provided value as the maximum number of TT Maps has already been configured for a given Linkset (64).
50922	Existing TT and Modified TT cannot be the same for a TT Map.
50923	Combination of Ingress Egress, Linkset, and Existing TT should be unique.
50924	linksetName given in MMI does not exist.
50925 - ERR_TT_MAP_DELETE_REQUIRES_A_VALUE	TT map name not given for deletion.
50926 - ERR_TT_MAP_EXISTING_TT_UPDATE_NOT_ALLOWED	Existing TT map value cannot be updated.
50927 - ERR_TT_MAP_INGRESS_EGRESS_UPDATE_NOT_ALLOWED	Ingress Egress value cannot be updated.
50928 - ERR_TT_MAP_LINKSET_NAME_UPDATE_NOT_ALLOWED	TT Map Linksetname cannot be updated.
50929	For edit or PUT to be successful, the modified TT should not be same as existing modified TT.

PCT

Resource PCT (/vstp/pcts).

Using PCT, you can define different translations that can change Destination Point Code(DPC) or Origination Point Code (OPC) or Circuit Identifier Code (CIC) of a MTP routed message.

Table 6-9 PCT Errors

Error Code Number	Description
ERR_ONT_001	The value of mandatory parameter is not set.
ERR_ONT_002	An invalid value set for a parameter.
50930	Cannot insert as maximum number of PCTs with given EPC have already been configured.
50931	Cannot insert as maximum number of PCTs with given Real PC have already been configured.
50932	Cannot insert as maximum number of distinct EPC have already been configured.
50933	Cannot insert as maximum number of distinct Real PC have already been configured.
50934 - ERR_PCT_ECICS_ECICE_RCICS_RCICE_NOT_ALLOWED_FOR_GIVEN_SI	ECICS , ECICE, RCICS, and RCICE is allowed only for SI 5, 13.
50935 - ERR_VSTP_PCT_ECICS_RANGE_INVALID_FOR_GIVEN_SI_AND_DOMAIN	Emulated CIC start range invalid for given Service indicator and domain.

Table 6-9 (Cont.) PCT Errors

Error Code Number	Description
50936 - ERR_VSTP_PCT_ECICE_RANGE_INVALID_FOR_GIVEN_SI_AND_DOMAIN	Emulated CIC end range invalid for given Service indicator and domain.
50937 - ERR_VSTP_PCT_RCICS_RANGE_INVALID_FOR_GIVEN_SI_AND_DOMAIN	Real CIC start range invalid for given Service indicator and domain.
50938 - ERR_VSTP_PCT_RCICE_RANGE_INVALID_FOR_GIVEN_SI_AND_DOMAIN	Real CIC end range invalid for given Service indicator and domain.
50939- ERR_PCT_ECICS_ECICE_RCICS_RCICE_NOT_ALLOWED_FOR_GIVEN_SI_AND_DOMAIN =	ECICS, ECICE, RCICS, and RCICE not allowed for given Service indicator and Domain.
50940- ERR_VSTP_PCT_ECICS_GREATER_THAN_ECICE	Emulated CIC start range should be less than Emulated CIC end range.
50941- ERR_VSTP_PCT_RCICS_GREATER_THAN_RCICE	Real CIC start range should be less than Real CIC end range.
50942 - ERR_VSTP_PCT_CIC_START_NOT_DEFINED	If the ECICE or RCICE parameter is specified, then the ECICS or RCICS parameter must be specified.
50943 - ERR_PCT_SSN_NOT_ALLOWED_FOR_GIVEN_SI	PCT Subsystem number is allowed only for service indicator 3.
50944 - ERR_VSTP_PCT_RECORD_ALREADY_EXISTS	PCT with same values already exist.
50945 - ERR_VSTP_PCT_EMULATED_RANGE_OVERLAPPING_FOR_GIVEN_PARAMETERS	Emulated CIC Range is overlapping for given parameters.
50946 - ERR_VSTP_PCT_REAL_RANGE_OVERLAPPING_FOR_GIVEN_PARAMETERS	Real CIC Range is overlapping for given parameters.
50948- ERR_VSTP_PCT_DOMAIN_CANNOT_BE_NONE	PCT Domain cannot be 'None'.
50949- ERR_EPC_GROUP_CODE_NOT_ALLOWED_FOR_GIVEN_DOMAIN	Group code can be defined for Emulated Point Code with ITUN domain only in PCT.
50950 - ERR_FILTPC_GROUP_CODE_NOT_ALLOWED_FOR_GIVEN_DOMAIN	Group code can be defined for Filter Point Code with ITUN domain only in PCT.
50951 - ERR_REALPC_GROUP_CODE_NOT_ALLOWED_FOR_GIVEN_DOMAIN	Group code can be defined for Real Point Code with ITUN domain only in PCT.
50952 - ERR_VSTP_PCT_EMULATED_AND_REAL_CIC_RANGE_WIDTH_NOT_EQUAL	In PCT difference between Emulated start and end should be same as difference between real start and end value that is the width of emulated CIC range and real CIC range must be equal.
50953 - ERR_PCT_EMULATED_PC_EXIST_IN_LOCAL_SP	True PC, Capability PC or a Secondary PC cannot be used as an Emulated PC in the PCT.
50954 - ERR_PCT_FILT_PC_EXIST_AS_ALIAS_IN_REMOTE_SP	Aliases provisioned in the routing table cannot be provisioned as Filt PC in PCT.
50955 - ERR_PCT_REAL_PC_EXIST_AS_ALIAS_IN_REMOTE_SP	Aliases provisioned in the routing table cannot be provisioned as Real PC in PCT.
50956 - ERR_PCT_REAL_PC_DOESNOT_EXIST_IN_REMOTE_SP	Real Pc of PCT must exist as RSP Mtp Point Code.

Table 6-9 (Cont.) PCT Errors

Error Code Number	Description
50957 - ERR_PCT_ROUTE_DOESNOT_EXIST_FOR_GIVEN_REALPC	The Real PC must have at least one route provisioned in route table.
50958 - ERR_PCT_FILTER_PC_DOESNOT_EXIST_IN_REMOTE_SP	Filt Pc of PCT must exist as RSP Mtp Point Code.
50959 - ERR_PCT_ROUTE_DOESNOT_EXIST_FOR_GIVEN_FILTERPC	The Filter PC must have at least one route provisioned in route table.
50960 - ERR_MAX_PCT_ALREADY_CONFIGURED	Maximum number of PCT on one site is 1000.
50961 - ERR_PCT_EPC_REALPC_SAME_AND_CIC_RANGE_SAME	In every PCT translation either the EPC or Real PC must be different or the Emulated CIC Range or the Real CIC Range must be different.
50983 - ERR_EPC_REALPC_GROUP_CODE_SHOULD_BE_SAME	Group code of Emulated, Real, and filter pc should be same. Different Group codes are not allowed for ITUN translations. Different Group codes are not allowed for ITUN translations.
50963 - ERR_EPC_REALPC_FILTPC_GROUP_CODE_SHOULD_BE_SAME	Group code of Emulated, Real, and filter pc should be same.
50947 - ERR_PCT_UNIQUE_IDENTIFIER_NOT_SET_FOR_DELETE_OPERATION	Unique Identifier must be specified for delete operation.
ERR_PCT_RECORD_DOES_NOT_EXIST => 'PCT : {ERR_OPR_FAILED_NO_ENTRY}	PCT record doesn't exist.
50993 - ERR_VSTP_PCT_ECICS_MANDATORY_WITH_RCICS	If the ECICE or RCICE parameter is specified, then the ECICS or RCICS parameter must be specified.
50994 - ERR_VSTP_PCT_RCICE_MANDATORY_WITH_ECICS_ECICE_RCICS	If the ECICS, ECICE, and RCICS parameters are specified, then the RCICE parameter must be specified.
50995 - ERR_VSTP_PCT_ECICE_MANDATORY_WITH_ECICS_RCICS_RCICE	If the ECICS, ECICE, and RCICS parameters are specified, then the RCICE parameter must be specified.

Route Errors

Table 6-10 Route Errors

Error Code Number	Description
50962 - ERR_VSTP_ROUTE_RSP_REFERENCED_IN_PCT_REALPC_FILTPC	Route cannot be deleted if RSP in route is used as Real PC or FiltPc in PCT.

Table 6-11 MTP Screening Rules

Error Code Number	Description
ERR_MTP_SCR_RULE_AFTPCSSN_INVALID' => 'AFT PC SSN {ERR_ONT_002}	Invalid value set for AftPcSsn parameter
ERR_MTP_SCR_RULE_SCMG_MSG_TYPE_INVALID' => 'SCMG MSG TYPE : {ERR_ONT_002}	Invalid value set for ScmgMsgType parameter

Table 6-11 (Cont.) MTP Screening Rules

Error Code Number	Description
50987 - ERR_SCMG_MSG_TYPE_NOT_ALLOWED_FOR_GIVEN_S	scmgMsgType parameter is only allowed for service indicator 3
50988 - ERR_SCMG_MSG_TYPE_NOT_ALLOWED_FOR_RULE_TYPE	scmgMsgType parameter is only allowed for SIO Screening Rule Group Type.
50292 - ERR_MTP_SCR_RULE_OPTIONAL_PARAMETERS_NOT_SET	AftPcSsn Parameter must be specified for AftPcSsn Rule type.
50296 - ERR_MTP_SCR_RULE_ATTR_MUST_BE_SET	AftPcSsn Parameter must be specified for AftPcSsn Rule type.
50990 - ERR_MTP_SCR_AFTPCSSN_ONLY_ALLOWED_FOR_RULE_TYPE_AFTPCSSN	AftPcSsn Parameter can only be specified for AftPcSsn Rule type.
50293 - ERR_MTP_SCR_RULE_TYPE_NSFI_INVALID	If scmgMsgType is configured, then nsfi allowed range = {stop, fail, AFTPC}
50293 - ERR_MTP_SCR_RULE_TYPE_NSFI_INVALID	If rule type is AFTPC, then nsfi allowed range = {stop, AFTPCSSN}
50293 - ERR_MTP_SCR_RULE_TYPE_NSFI_INVALID	If rule type is AFTPCSSN, then nsfi allowed range = {stop}