Oracle® Communications Diameter Signaling Router

Virtual Signaling Transfer Point User's Guide

Release 8.1

E86290 Revision 01

July 2017

ORACLE®

Oracle Communications Diameter Signaling Router Virtual Signaling Transfer Point User's Guide, Release 8.1

Table of Contents

List of Figures

List of Tables

Chapter 1

Oracle References and Services

Topics:

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

My Oracle Support (MOS)

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

Call the CAS 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 MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Locate Product Release Software on the Oracle Software Delivery Cloud Site

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

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

Chapter 2

Introduction to vSTP

Topics:

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

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.

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.

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.

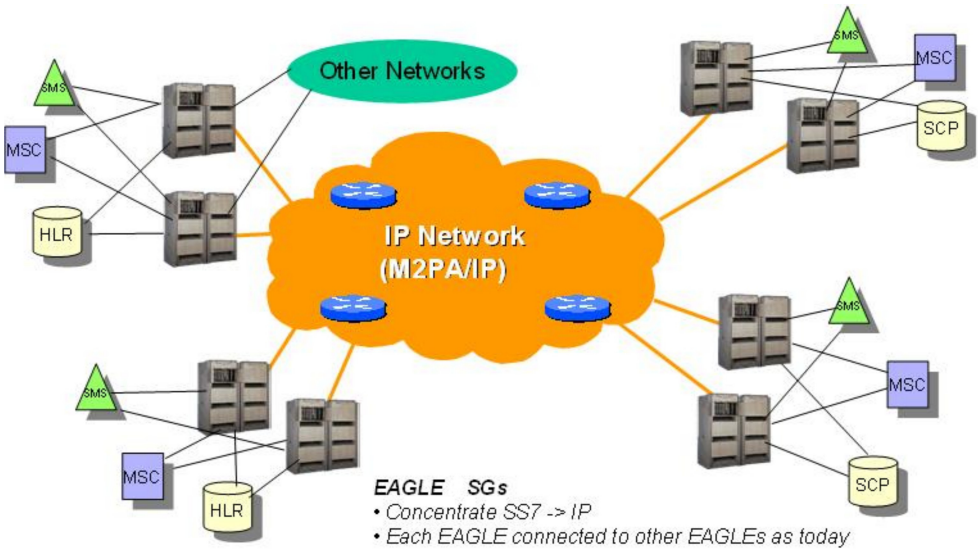

Figure 1: M2PA Network

Global Title Translation

The Global Title Translation (GTT) feature is designed for the signaling connection control part (SCCP) of the SS7 protocol

The GTT feature uses global title address (GTA) information to determine the destination of the MSU. The translation type (TT) indicates which global title translation table is used to determine the routing to a particular service database. Each global title translation table includes the point code (pc) of the node containing the service database, the subsystem number (ssn) identifying the service database on that node, and a routing indicator (ri). The routing indicator determines if further global title translations are required. GTA and TT are contained in the called party address (CDPA) field of the MSU.

The global title translation feature changes the destination point code and the origination point code in the routing label. The global title information is not altered.

Depending on how the global title translation data is configured, the routing indicator, the subsystem number, or the translation type in the called party address may also be changed by the global title translation feature. The gray shaded areas in *Figure 2: ANSI and ITU MSU Fields affected by the Global Title Translation Feature* show the message fields affected by global title translation.

ANSI MSU (ANSI Message Signal Unit)

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

ITU-I MSU (ITU International Message Signal Unit)

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

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

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

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

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

Figure 2: ANSI and ITU MSU Fields affected by the Global Title Translation Feature

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.

Flexible Intermediate GTT Load Sharing

Flexible Intermediate GTTLoad 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 GTTLoad Sharing feature. The Flexible GTTLoad Sharing and Intermediate GTTLoad Sharing features must be enabled and turned on 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 Flexible GTT Load Sharing feature *not* enabled, load shares post-GTT destinations when intermediate global title translation 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 global title translation 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.

Flexible Final GTT Load Sharing

Flexible Final GTTLoad 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 GTTLoad 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.

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 GTTLoad Sharing feature, which allows unequal traffic loads to be provisioned in mated application (MAP) and mated relay node (MRN) load sharing groups.

The MAP and MRN load sharing groups can be MAP or MRN load sharing groups without the Flexible GTTLoad Sharing enabled, or MAP or MRN sets with the Flexible GTTLoad Sharing feature enabled. Weighted GTTLoad 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.

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 GTTLoad 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 GTTLoad 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 1: RC Group Weight Example 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 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 traffic based on MTP parameters.

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: RC Group In-Service Threshold States* shows how the states of the RC group are determined.

Table 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 Sharing and 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 3: In-Service Threshold Example* , 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 3: In-Service Threshold Example

Entity	RC	Weight	RC Group Weight	In-Service Threshold	Required RC Group Weight	Entity Status	Entity Available Weight	RC Group Available Weight	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: RC Group In-Service Threshold States* .
- Available RC group weight – The sum of all entity available weights in the RC group.

Table 4: Load Shared Group with Weighted GTT Load Sharing Example shows an example of Weighted GTT Load Sharing applied to a load shared MAP or MRN group.

Table 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
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: RC Group In-Service Threshold States* .
- 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 5: Combined Dominant/Load Shared Group with Weighted GTT Load Sharing Example 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 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%

Entity	RC	Weight	RC Group Weight	In-Service Threshold	Required RC Group Weight	Entity Status
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. This action is equivalent to the action performed when the `mrc=no` parameter is specified with either the `ent-map` or `chg-map` commands.

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. This action is equivalent to the action performed when the `mrc=yes` parameter is specified with either the `ent-map` or `chg-map` commands.

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. 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 GTTLoad 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 loadshared 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.

The parameters used for Transaction-Based GTT Load Sharing are selected using the `chg-sccpopts` command. These parameters are:

- `:tgtt0` – enable or disable Transaction-Based GTTLoad Sharing for SCCP Class 0 UDT, UDTS, XUDT, or XUDTS messages.
- `:tgtt1` – enable or disable Transaction-Based GTTLoad 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 3: Transaction-Based GTT Load Sharing SCCP Options describes how the Transaction-Based GTT Load Sharing SCCP options are used.

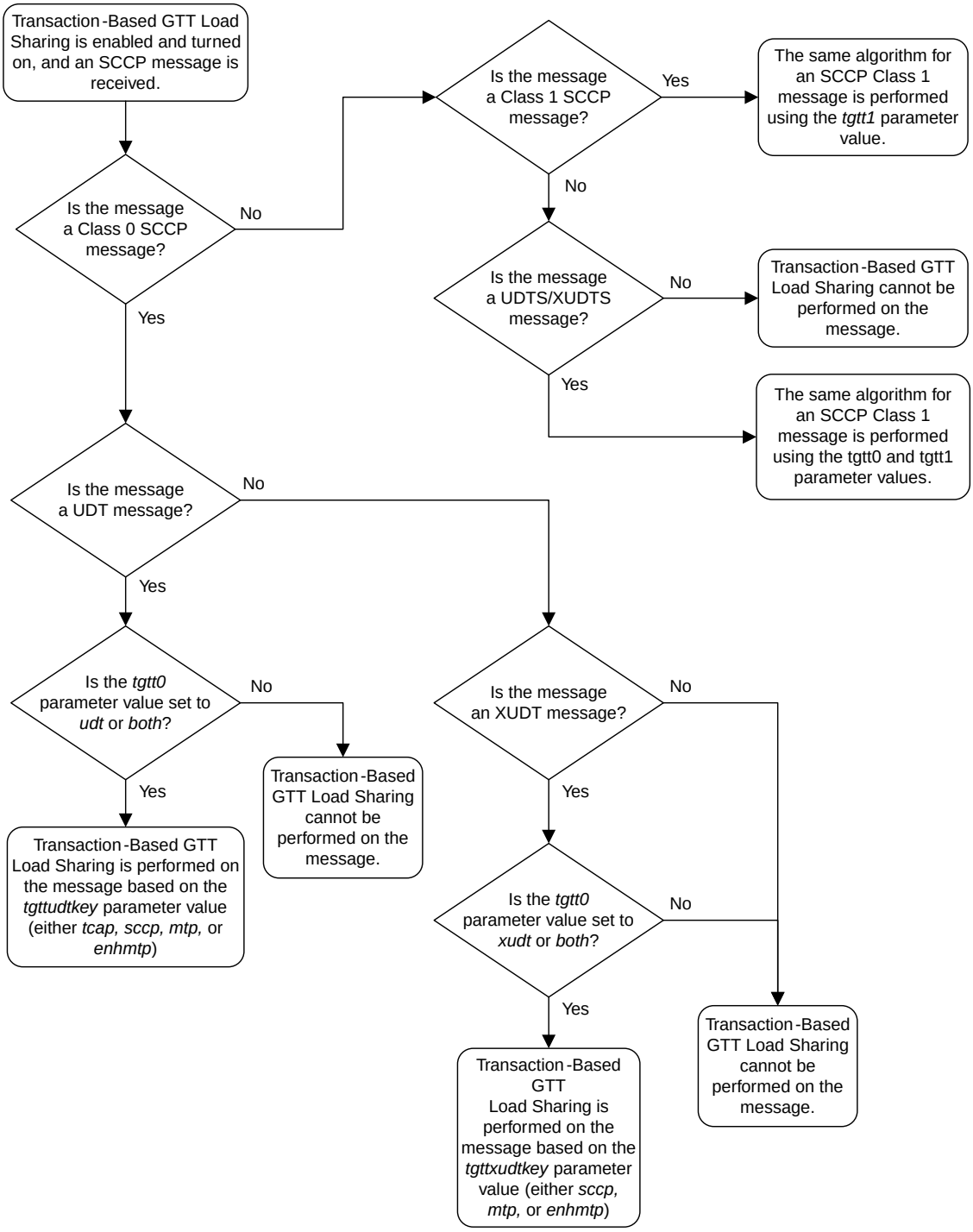

Figure 3: Transaction-Based GTT Load Sharing SCCP Options

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.

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 `chg-sccpopts` command is set to `on`.

When the `class1seq` parameter value is `on`, load sharing of these messages is performed in the dominant mode, overriding the load sharing configuration in the MAP and MRN tables. Delivering the UDT/XUDT Class 1 ITU messages in sequence is guaranteed only if the `randsls` parameter value of the `chg-stpopts` command is either `off` or `class0`. If you wish to guarantee delivering these messages in sequence, the `class1seq=on` and the `randsls=all` parameters should not be used together. The value of the `randsls` parameter is shown in the `rtrv-stpopts` command.

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.

Caution: If the`randsls` parameter value of the`chg-stpopts` command is`all`, thus activating the RandomSLS feature forITU Class 1SCCP messages, theUDT/XUDT Class 1 messages are not delivered in sequence. To ensure that Class 1UDT/XUDT messages are delivered in sequence, the`randsls` parameter value should be set to either`off` or`class0`.

Caution: However, if the`randsls` parameter value of the`chg-stpopts` command is`all`, Class 1UDT/XUDT messages are load shared across equal cost destinations by the WeightedSCP Load Balancing and Intermediate Global Title Load Sharing (IGTTLS) features. If the`randsls` parameter value of the`chg-stpopts` command is either`off` or`class0`, load sharing for all Class 1SCCP messages is supported only in the dominant mode.

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.

Support of SCCP XUDT Messages

The Support of SCCPXUDT Messages feature allows the global title translation feature and the following SCCP services to process XUDT messages.

- G-PORTMNP - XUDT response generation (that is, XUDTSRI_ack), when an XUDTSRI message is received, is supported if the SRI is not segmented. G-PORT treats any segmented message (SRI or non-SRI) as a non-SRI message and message relay is performed on the message. G-PORT Message Relay is supported for all non-SRI messages, including segmented and non-segmented, Class 0 and Class 1.

The following features do not support this feature:

- North American Local Number Portability (LNP)
- ANSI-ITUSCCP Conversion
- GSMEquipment Identity Register (EIR)

XUDT messages can be screened by Gateway Screening and all gateway screening stop actions can be applied to XUDT messages.

Chapter 3

MMI Managed Objects

Topics:

This chapter provides basic information to access MMI configuration elements used by vSTP.

MMI Managed Objects

MMI information associated with vSTP is accessed from a DSR NOAM or SOAM from **Main Menu** > **MMI API Guide**.

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

Chapter 4

DSR Managed Objects

Topics:

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.

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.

Groups

The **Groups Administration** page enables you to create, modify, and delete user groups.

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.

Permissions:

Resource	View	Insert	Edit	Delete	Manage
Global Action Permissions	☐	☐	☐	☐	☐
Administration Permissions	☐	☐	☐	☐	☐
General Options	☐		☐		
Users	☐	☐	☐	☐	☐
Groups	☐	☐	☐	☐	
Sessions	☐			☐	
Certificate Management	☐	☐	☐	☐	
Authorized IPs	☐	☐	☐	☐	
SFTP Users	☐	☐	☐	☐	
Software Versions	☐				
ISO Deployment	☐		☐		☐
Software Upgrade	☐		☐		☐
Remote LDAP Authentication	☐	☐	☐	☐	
Remote SNMP Trapping	☐		☐		
Remote Export Server	☐	☐	☐	☐	☐
DNS Configuration	☐		☐		
Licenses	☐	☐			

Figure 4: Global Action and Administration Permissions

Each permission checkbox on the **Groups Administration** page corresponds to a menu option on the GUI main menu or a submenu. If a checkbox is checked for a group, then the group has access to this option on the menu. If a checkbox is not checked, then the group does not have access to this option, and the option is not visible on the GUI menu.

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.

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.

Devices

The **Devices** page is used to configure and manage additional interfaces other than what was configured during the initial installation.

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.

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 6: Core Services*.

Table 6: 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.

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.
- Query Server (QS) - The Query Server is an independent application server containing replicated application data. A Query Server is located in the same physical frame as each NOAMP component.

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.

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. 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** > **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.

Chapter 5

Alarms, KPIs, and Measurements

Topics:

This chapter describes the types of alarm, KPI, and measurements information that is available for vSTP.

vSTP Alarms and Events

The vSTP alarms and events are described in the *Alarms and KPIs Reference*.

Active alarms and events and alarm and event history can be displayed on the **Alarms & Events** > **View Active** and **Alarms & Events** > **View History** pages.

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** > **Reports** page.

The *Measurements Reference* explain the report selection criteria, and describe each measurement in each measurement group.

Glossary

A

ANSI

American National Standards Institute

An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.

E

EIR

Equipment Identity Register

A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.

F

FGTTLS

Flexible GTT Loadsharing

Flexible GTT Load Sharing

FGTTLS provides more flexible GTT load sharing arrangements for GTT traffic.

G

G

GSM	Global System for Mobile Communications A second generation digital PCS mobile phone standard used in many parts of the world.
GT	Global Title Routing Indicator
GTA	Global Title Address
GTT	Global Title Translation A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE uses to determine which service database to send the query message when an MSU enters the EAGLE and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.

I

ID	Identity Identifier
IGTTLS	Intermediate Global Title Translation Load Sharing
ITU	International Telecommunications Union An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and

I

	operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing international telecommunications, and for harmonizing national political interests.

K

Key	For the ICNP feature, a unique DS value used to access a table entry, consisting of a number length and number type.

L

LNP	Local Number Portability The ability of subscribers to switch local or wireless carriers and still retain the same phone number.
Load Sharing	A type of routing used by global title translation to route MSUs This type of routing is used when a second point code and subsystem is defined for the primary point code and subsystem. Traffic is shared equally between the replicated point codes and subsystems.

M

M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MAP	Mobile Application Part An application part in SS7 signaling for mobile communications systems.

M

MAP Group	The MAP entities in an entity set used for the distribution of traffic.
MNP	Mobile Number Portability Allows a user to keep his or her mobile phone number despite changing provider. The subscriber also keeps the network carrier code.
MRN	Message Reference Number An unsolicited numbered message (alarm or information) that is displayed in response to an alarm condition detected by the system or in response to an event that has occurred in the system. Mated Relay Node A mated relay node (MRN) group is provisioned in the database to identify the nodes that the traffic is load shared with, and the type of routing, either dominant, load sharing, or combined dominant/load sharing.
MSU	Message Signal Unit The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information: • The forward and backward sequence numbers assigned to the message which indicate the position of the message in the

M

traffic stream in relation to the other messages.

- The length indicator which indicates the number of bytes the message contains.
- The type of message and the priority of the message in the signaling information octet of the message.
- The routing information for the message, shown in the routing label of the message, with the identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE uses to pick which link set and signaling link to use to route the message.

MTP

Message Transfer Part

The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 MSU through the network

Module Test Plan

O

OPC

Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

R

RC

Relative Cost

Restriction Criteria

Resource Controller

S

S

SCCP	Signaling Connection Control Part The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network using a connection-oriented or connectionless approach.
SCP	Secure Copy Service Control Point SCPs are network intelligence centers where databases or call processing information is stored. The primary function of SCPs is to respond to queries from other SPs by retrieving the requested information from the appropriate database, and sending it back to the originator of the request.
SLS	Signaling Link Selector
SRI	Send Routing Information Send_Route_Information Message
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

S

SSN

SS7 Subsystem Number

The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message, or the subsystem number of the destination point code to be assigned to the LNP subsystem of the EAGLE.

Subsystem Number

A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry.

Subsystem Number

Used to update the CdPA.

T

TCAP

Transaction Capabilities Application Part

A protocol in the SS7 protocol suite that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the Signaling Connection Control Part connectionless service. TCAP also supports remote control - ability to invoke features in another remote network switch.

TT

Translation Type

Resides in the Called Party Address (CdPA) field of the MSU and determines which service database is to receive query messages. The translation type indicates which Global Title Translation table

T

determines the routing to a particular service database.

U

UDT — Unitdata Transfer

UDTS — Unitdata Transfer Service

An error response to a UDT message.

UIM — Unsolicited Information Message

A message sent to a user interface whenever there is a fault that is not service-affecting or when a previous problem is corrected. Each message has a trouble code and text associated with the trouble condition.

Unified Inventory Management

X

XUDT — Extended Unit Data

Extended User Data

XUDTS — Extended Unitdata Service message

An error response to an XUDT message.