Megisto Mobile Services Delivery Platform
MS950 Configuration Guide
Release 2.0

802-0103-0002 • Revision 3.0

© 2003 Megisto Systems, Inc. All rights reserved.

Megisto Systems, Inc. (Megisto) retains all ownership rights to all computer programs offered by Megisto, their products, and the contents of this manual. The source code for both software and firmware are confidential trade secrets of Megisto. You may not attempt to decipher, decompile, develop or otherwise reverse engineer Megisto software, firmware, or products. Information necessary to achieve interoperability is furnished upon request.

This manual is furnished under license and may only be used or copied in accordance with the terms of such license. The information in the manual is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Megisto. Megisto assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual. No part of this manual may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the express written permission of Megisto.

Existing artwork or images that you may desire to scan may be protected by copyright law. Be sure to obtain permission for use of existing artwork.

Trademarks

This product carries the Trademark of Megisto Systems, Inc. (Megisto) All the trademarks of component parts used by Megisto Systems in the manufacture of this product are the property of their respective owners. The Megisto logo is a registered trademark of Megisto Systems, Inc.

All brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Manufacturer's Statement

Limited Warranty, Disclaimer, Limitation of Liability

Megisto warrants this product for a limited period of time from initial purchase against defects in materials and workmanship. This warranty does not cover damage caused by misuse or abuse of this product or by acts of God or accidents or other causes beyond the control of Megisto. Also not covered by this warranty are claims other than by the original purchaser. Your sole remedy and our sole liability to you shall be to repair or replace this product at our discretion if it does not meet the requirements of this warranty.

Megisto and its distributors shall under no circumstances be liable for any damages arising from the use of or the inability to use this product or from any loss of revenue or profit, business interruption, or other loss which may arise from the use of this product.

THE WARRANTIES ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Contents

Section I: Getting Started

Section II: Network Connection

Section III: Management Configuration

Section IV: Subscriber Services

Chapter 1: About this Guide

In This Chapter

Objective

This document describes the tasks required to configure the MS950 and the MS950-ES, which are components of the Megisto Mobile Services Delivery Platform (MSDS). It provides a detailed overview of each configuration task, configuration steps, and an example.

Related Publications

The Megisto Systems documentation set consists of:

- *MS950 CLI Reference Guide:* Describes all command line interface (CLI) commands. It should be used in conjunction with this manual. It contains parameter descriptions and default values for the command line interface (CLI)
- *MS950 Installation and Maintenance Guide:* Provides instructions to install and maintain the MS950.
- *MS950-ES Installation and Maintenance Guide:* Provides instructions to install and maintain the MS950-ES.

Intended Audience

This guide is intended for use by system and network administrators experienced with general networking hardware/software architecture and basic TCP/IP. It assumes that you are familiar with the hardware configuration, specifically the cards, and that the

MS950 and MS950-ES are installed (and initially configured) as described their respective Installation and Maintenance Guides. You need hardware configuration information to perform some configuration tasks.

Conventions

The following conventions are used when describing CLI commands.

Convention	Description
`Courier`	Indicates CLI inputs or outputs.
Bold	Command names or indicates you should type data exactly as shown.
Italics	Arguments in which you must supply a value.
[]	Optional arguments.
{ }	Required arguments.
A I B	The pipe indicates alternative parameters (A or B).
>	Indicates Operator exec mode.
#	Indicates Administrator or Superuser mode.
SSN ~~SSN~~	Indicates the command is only used for SSN or is not used for SSN.
GGSN ~~GGSN~~	Indicates the command is only used for GGSN or is not used for GGSN.
CDMA ~~CDMA~~	Indicates the command is only used for SSN or is not used for CDMA.

Document Structure

This manual is divided into sections that provide a concept-level division of configuration tasks. The sections are presented in the order in which you would perform tasks. For example, you would typically configure the MS950 for network operation prior to configuring subscriber services. Examples of complete configurations are described in the last section of the book.

CD Structure

On the CD that accompanies your MS950 you can find an electronic copy of this manual in PDF and HTML format. You can also find electronic versions of all other available documentation. In addition, all MIBs are available in the MIBs directory.

Getting Help

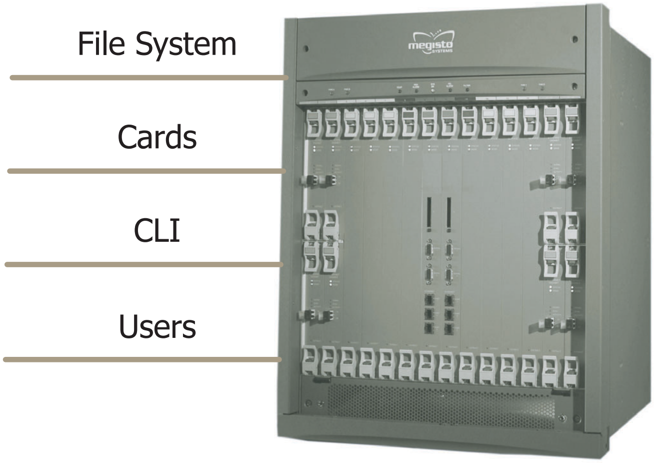
CLI help is available by typing a question mark (?) at any command line. Context-sensitive help is provided for the command or the command mode. You may also use the **`help`** command, as described in the *MS950 CLI Reference Guide*.

If you need further assistance, please contact Megisto immediately by e-mail at support@megisto.com. Megisto's URL is http://www.megisto.com. You also can send correspondence to the addresses in the table below.

Megisto USA	**Megisto Europe**
20251 Century Boulevard Suite 120 Germantown, MD 20874 USA +1 (301) 444-1700	Thames Court 1 Victoria Street Windsor Berkshire SL4 1YB United Kingdom

Section I: Getting Started

The chapters in this section familiarize you with the MS950 and provide the information you need to get the MS950 up and running. These operations are typically performed prior to configuring the MS950 for operation in your network and configuring subscriber services.



Chapter 2: System Overview

Megisto's Mobile Services Delivery System (MSDS) is a carrier-grade services platform designed uniquely to cater to mobile users. The MSDS is designed for effectively delivering services to professional and consumer mobile users from various access networks including 2.5G GPRS, 3G UMTS, and WLANs. The central component of the MSDS is the MS950.

The MS950 acts as a mobile service anchor point for GPRS, UMTS, and WLAN users. It is a point of mobility session termination, user identity, and service delivery. It provides flexible Layer 4 processing and load balancing, including 6-tuple differential charging for e-mail, file downloads, source and destination-based charging, and charging based on QoS.

The MS950 extension shelf (MS950-ES) houses application-service engines (ASEs) in which application specific software resides. The MS950-ES is used to extend the MS950's prepaid charging capabilities. It is used for performing content processing at Layer 7, including application-aware charging for MMS, WAP 1.x, WAP 2.0, HTTP, and other applications and downloads

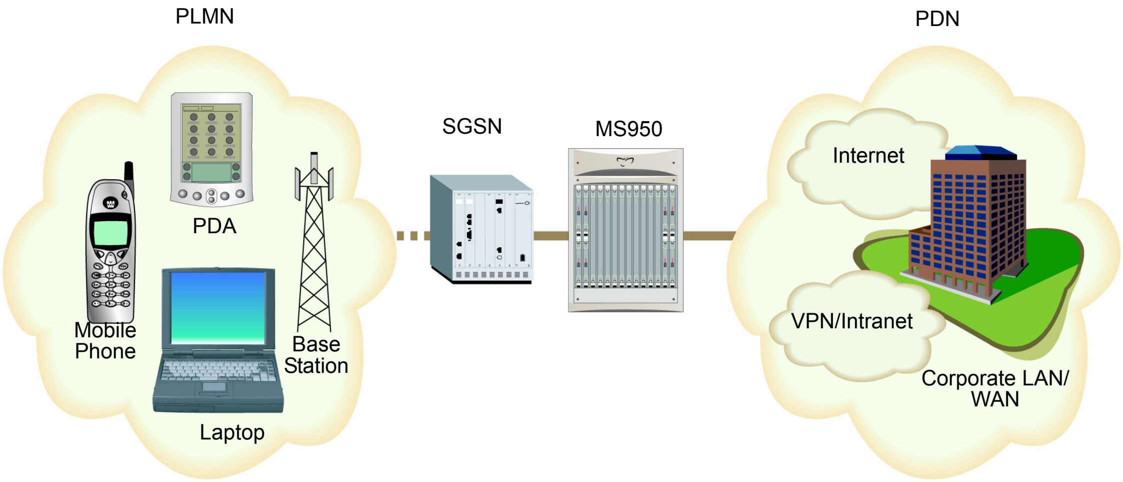
The MS950 is an advanced, carrier-grade mobile delivery service platform that provides a broad range of advanced mobile services. These include:

- Gateway GPRS Support Node (GGSN)
- virtual private network (VPN) services

- a secure gateway
- a wide variety of tunneling technologies
- address translation functions
- comprehensive billing
- carrier-grade scalability and resiliency

The MS950 supports the packet data traffic processing needed between the public data network (PDN) and public land mobile network (PLMN) sides of the communications network (2.5G, 3G, and WLAN access environments).

The MS950 supports always-on access for mobile subscribers on the PLMN side with access to the Internet, VPNs, and corporate local area networks (LANs) while providing access on the PDN side to such wireless devices as mobile phones, personal digital assistants (PDAs), and laptops.

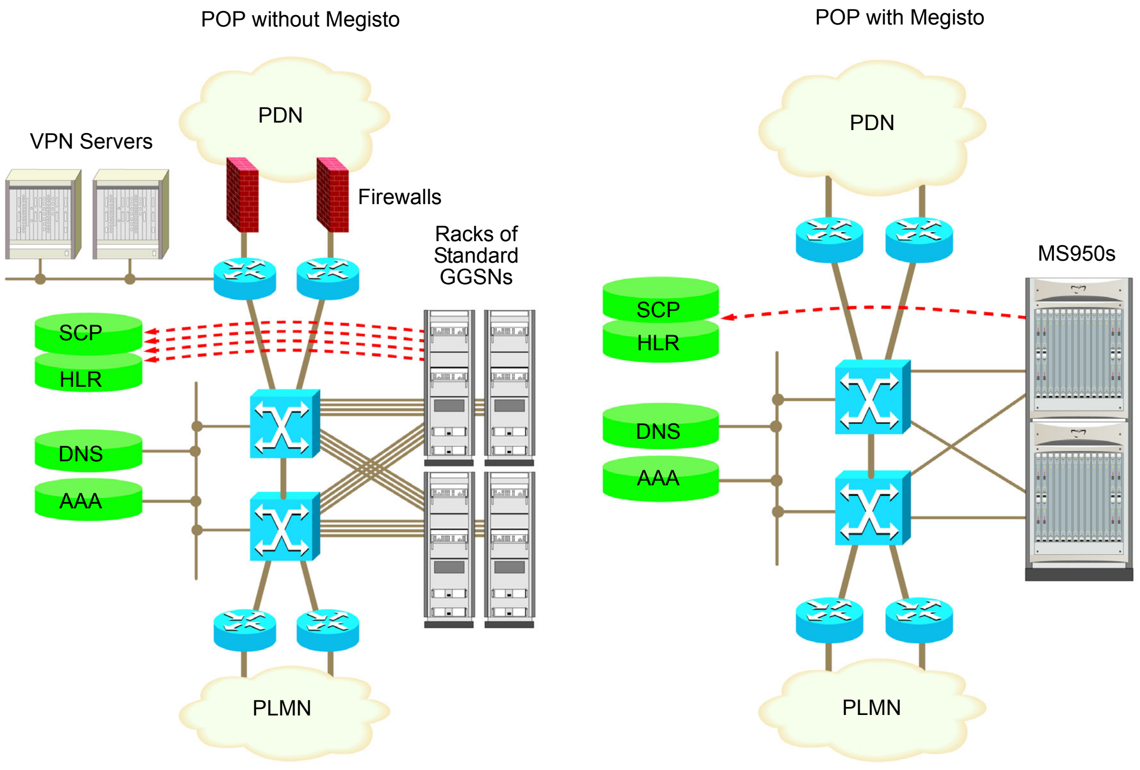


Note: The interworking functions between PDNs and PLMNs are assigned to the GGSN in General Packet Radio Services (GPRS) and Universal Mobile Telecommunications Service (UMTS).

Why the MS950?

The MS950 is purpose-built for multi-generation network functionality (2.5G, 3G, and WLAN access environments). Because it is more than a standard GGSN, the MS950 provides the functionality of multiple network nodes in one box.

For example, a point of presence (POP) today could contain VPN servers, firewalls, and multiple nodes in order to fulfill the duties of a GGSN. The MS950 removes the need for these additional boxes, thus reducing operational costs as well as providing easy configuration and integration with existing networks. It also provides a single point of administration because it is both highly scalable (requiring fewer similar boxes) and highly featured (requiring fewer dissimilar boxes).



Each MS950 can support up to 1,020,000 PDP contexts (170,000 per Service Card (6)), allowing reduction of nodes required to support subscribers.

The MS950 at Work

The MS950 can act as GGSN in a GPRS network, a Service Selection Node to communicate with an existing GGSN, or a CDMA Home Agent (HA). See “Operational Modes” on page 3-1 for a complete decsriptions of how the MS950 operates in each of these modes.

A complete system description of the MS950-ES is available in the *MS950-ES Installation and Maintenance Guide.*

The Megisto CLI

The Megisto CLI provides a mechanism for configuring the MS950 and the MS950-ES. It consists of a series of commands that, in combination, achieve all MS950 and MS950-ES operator configuration tasks.

Note: Hardware installation and initial configuration are discussed in the *MS950 Installation and Maintenance Guide* and the *MS950-ES Installation and Maintenance Guide.*

Configurable Items

The CLI is the enabling mechanism for configuring the MS950. The CLI allows you to:

- configure the MS950 via Telnet, RS-232C, and SSH
- perform basic file system operations and configuration
- configure interfaces
- set subscriber partitions
- configure MS950 charging parameters
- configure MS950-ES charging parameters
- configure IP services and routing functions
- configure tunnels and security parameters

- configure redundancy
- configure all services and network topologies

Unique Concepts

Subscriber Partitions

The MS950 hosts subscribers. A subscriber partition relates to a set of mobile subscribers that have been associated with an APN. Mobile subscribers build dynamic relationships with MS950s for the purpose of being served. These relationships are PDP contexts associated with the APNs. For example, an APN can represent a corporation that allows its employees mobile access through its corporate intranet. You must configure the MS950 to recognize the APN (as well as other data) and to execute a series of rules based on the subscriber profile before packet processing can begin. See “Subscriber Partitions” on page 19-1 for more information.

Interfaces

The MS950 features two types of interfaces: physical and virtual. Physical interfaces maybe connected to Gigabit Ethernet devices and to Fast Ethernet ports for OA&M connectivity. Virtual interfaces are logical entities that provide link and network layer functionality on service and control cards. See “Interfaces” on page 8-1 for more information.

Connecting Cards

The MS950 performs all Layer 3 processing on service cards while the Layer 2 processing is performed on line cards. A static connection between line cards and service cards must created prior to performing any other configuration tasks. See “Card Configuration” on page 6-1 for more information.

General Configuration Flow

The following steps provides a suggested flow of configuration.

1. Configure cards/redundancy.

Note: The fabric card must be configured before you can connect line cards to service cards.

2. Connect line cards to service cards.
3. Configure interfaces.

   At a minimum, it is recommended that you configure a management interface, a loopback interface for ms_id, a gigethernet interface, a fastethernet interface for Telnet, a tunnel interface for GTP traffic, and an IPSec tunnel interface if you plan to use IPSec.
4. Configure SNMP.
5. Configure time settings.
6. Configure users.
7. Configure charging.
8. Configure network security.
9. Configure subscribers.

Chapter 3: Operational Modes

In This Chapter

- GGSN
- CDMA Home-Agent
- Service Selection Node

Your MS950 can be configured to operate in one of three modes. The MS950 can act as GGSN in a GPRS network, a Service Selection Node to communicate with an existing GGSN, or a CDMA Home Agent (HA). The majority of the commands in the CLI work for GGSN operation. When the MS950 operates as a Service Selection Node or a CDMA HA, certain commands are no longer applicable. A few commands are reserved only for GGSN GTP configuration. When your MS950 acts as an SSN it can act as a RADIUS proxy or RADIUS broadcast. This chapter describes how to configure aspects of GGSN, Service Selection Node, and CDMA operation. Operation, parameters, and commands which do and do not apply to a particular mode of operation are marked.

Setting the Mode

You can configure the MS950's mode of operation and how it will act in that mode.

To set the actual mode of operation in superuser:

1. Enter the following at the command prompt:
   ```
   mode [ggsn | cdma-ha | ssn-native-ip |
      ssn-ip-ip]
   ```
2. Configure other desired system parameters in the sys-parmas command mode:
   ```
   gtp-sessions sessions
   ipsec-sessions sessions
   mip-enable [on | off]
   mip-sessions sessions
   ```

```
mip-subs number
ssn-radius-method [proxy | broadcast]
```

3. Reboot the system:

```
reload system
```

Example

The following example sets the mode for SSN and configures all system parameters.

```
MS# mode ssn-native-ip
MS# config sys-params
MS(config-sysparams)# gtp-sessions 300
MS(config-sysparams)# ipsec-sessions 300
MS(config-sysparams)# mip-sessions 300
MS(config-sysparams)# mip-subs 100
MS(config-sysparams)# mip-enable on
MS(config-sysparams)# ssn-radius-method proxy
```

GGSN

GGSN ~~CDMA~~ ~~SSN~~

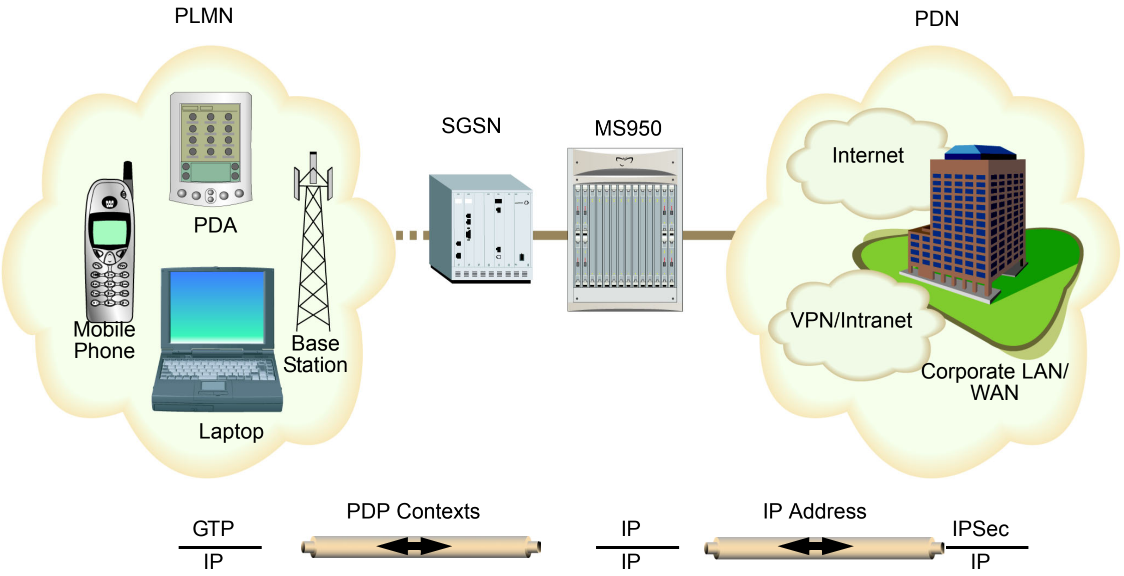
GPRS Tunneling Protocol (GTP) is a tunneling protocol that operates over UDP on interfaces between the SGSN and the MS950 in the GPRS/ UMTS environment. This interface is used for tunneling data between the core network and the PDN.

GTP provides the mechanism for forwarding data traffic within the GPRS backbone network. The function of GTP is essential to the MS950 operating as a GGSN.

The MS950 sets up, maintains, and clears packet data sessions related to mobile subscribers. It also applies service profiles that are created via subscription parameters. During such sessions, the MS950 forwards data from the PLMN to the PDN, and vice versa. Various traffic processing activities may occur on each of the packets while transversing the MS950. Such traffic processing may relate to security, quality of service (QoS) support, or IP forwarding between interfaces.

The MS950 is the interface node between the PLMN and the PDN. For each active subscriber, the MS950 administers at least one Packet Data Protocol (PDP) context. Traffic related to the PDP context is transported between Serving GPRS Support Nodes (SGSNs) and MS950s using tunnels.

On PDP traffic moving from the PLMN to the PDN, the MS950 terminates the GTP tunnels to decapsulate the original IP packets sent by the mobile subscriber. The IP packets are then forwarded into the Internet and to the desired destination, which is identified through the destination IP address.



On traffic moving from the PDN to the PLMN, the MS950 inspects the IP packets to guarantee compliance with PDP parameter requirements. The packets are then mapped into GTP tunnels according to the destination IP address of the mobile subscriber (the PDP address) and forwarded to the corresponding SGSN. The MS950 administers subscriber state information that includes:

- the PDP type and PDP address
- the GTP tunnel identifier for control signaling and packet data flow

- the related QoS parameters
- the type of services provided
- the current SGSN address of the user

The MS950 also supports charging and services that can be established on a per-subscriber basis.

The following procedure allows you to configure GTP parameters.

To configure GTP in administrator or superuser mode:

1. Enter the following at the command prompt to enter GTP commands:
   `configure gtp`
2. Enter the following at the command prompt to specify the number of times that the MS950 attempts to send a signaling request:
   `n3-requests` *`value`*
3. Enter the following at the command prompt to specify the time interval between each echo request message:
   `path-echo-interval` *`value`*
4. Enter the following at the command prompt to enable echo requests:
   `path-echo-request`
5. Enter the following at the command prompt to specify the number of seconds that the MS950 waits to respond to a signalling request message:
   `t3-response` *`value`*

Example

The following example sets the MS950 in config mode, tries 1025 times to send GTP signaling requests, waits 100 seconds before sending an echo-request, and waits 70 seconds before responding to a signaling request.

```
MS# configure gtp
MS(config-gtp)# n3-request 5
MS(config-gtp)# t3-response 5
MS(config-gtp)# path-echo-interval 60
MS(config-gtp)# path-echo-request
```

Deleting the GTP Group

You can delete all PDP-contexts with the **`delete gtp pdp-context`** command, or you can select specific PDP-contexts by specifying their IMSI with the **`delete gtp imsi`** command.

Example

```
MS# delete gtp pdp-context
MS# delete gtp imsi
```

Displaying GTP Information

You can display information about a variety of GTP settings using the following commands:

- **`show gtp params`**
- **`show gtp counters`**
- **`show gtp statistics`**
- **`show gtp status`**
- **`show gtp pdp-context`**
- **`show gtp imsi`**

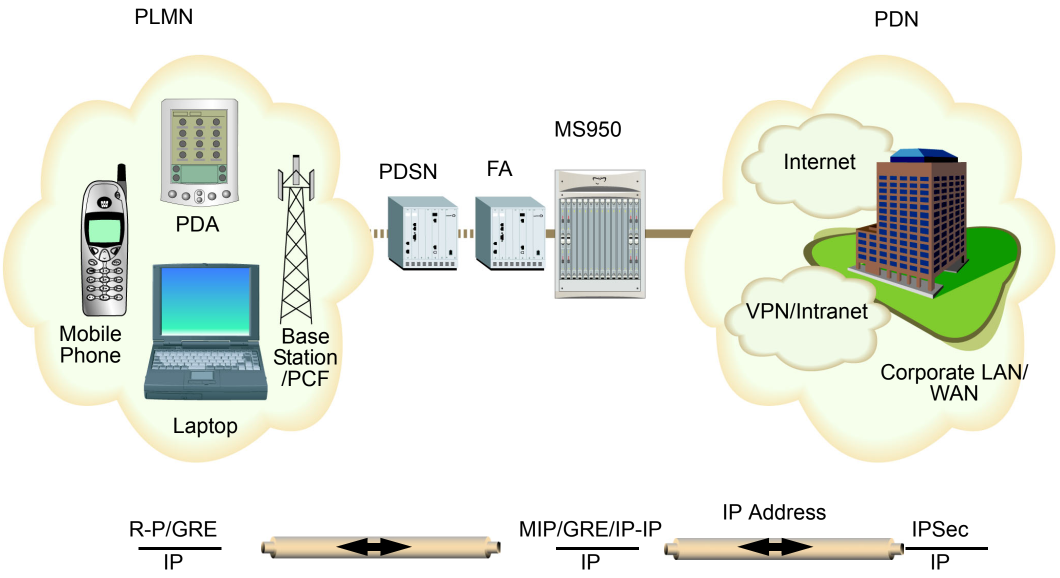
CDMA Home-Agent

CDMA ~~GGSN~~ ~~SSN~~

The MS950 supports subscriber-based authentication for GSM networks using the GTP protocol. In CDMA-based networks the MS950 acts as a Home Agent (HA) to support mobile node registration and packet forwarding functions. The Home Agent is the anchor point for mobile terminals for which Mobile IP services are provided. It supports and maintains mobile user registrations. Traffic sent to the terminal is routed via the Home Agent. With reverse tunneling, traffic from the terminal is also routed via the Home Agent.

The CDMA HA is used to offer advanced subscriber features like prepaid and differential billing support. Mobile IP is the protocol used on the access side for initiating these services. Subscribers are identified using NAI (user@realm). The “realm” part of the NAI is equivalent to an APN in GPRS. All CDMA realm configuration is performed under the APN command mode. APN should be considered equivalent to realm for configuration purposes.

Note: The MS950 operates exclusively as a Service Selector Node, GGSN, or CDMA HA.



To configure the MS950 for CDMA HA in administrator or superuser mode:

1. Enter the following at the command prompt:
   ```
   configure
   ```
2. Enter the following at the command prompt to configure the HA map:
   ```
   ha-map name
   ha-ip-addr address [spi spi] [shared-key key]
   fa-ip-addr address [spi spi] [shared-key key]
   ```
3. Configure the APN to use local authentication:
   ```
   authentication {local}
   ```
4. Enter the following at the command prompt to bind the HA map to the APN:
   ```
   bind ha-map name
   ```
5. If desired, enter the following at the command prompt to specify generic-subscriber-information:

```
generic-subscriber-info [mn-ha-spi spi] [mn-ha-
   sharedkey key]]
```

Example

The following example configures a CDMA HA map and configures the APN to use CDMA HA configuration.

```
MS# configure
MS(config)# ha-map hamap1
MS(config-map)# ha-ip-address 10.1.0.3 spi 123 shared-
   key xyz
MS(config-map)# fa-ip-address 10.1.0.3 spi 123 shared-
   key xyz
MS(config-map)# exit
MS(config)# subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# authentication local
MS(config-subs-apn)# bind ha-map hamap1
MS(config-subs-apn)# generic-subscriber-info mn-ha-spi
   123 mn-ha-sharedkey xyz
```

Displaying CDMA HA Information

You can display the current CDMA HA map via the **`show ha-map`** command.

Cll Commands That Do Not Apply

The following is a list of CLI commands that do not apply when the MS950 acts as a CDMA HA:

Whole Commands

- clear debug-gtp
- clear debug-gtpp
- delete gtp imsi
- delete gtp pdp-context
- show apn-pdp-statistics apn

- show apn-pdp-statistics context apn
- show apn-pdp-statistics context select
- show apn-pdp-statistics last-interval
- show apn-pdp-statistics select
- show charging charging-gateway
- show charging sgsn
- show gtp counters
- show gtp imsi
- show gtp params
- show gtp pdp-context
- show gtp statistics
- show gtp status
- show imsi-pdp-statistics context imsi
- show imsi-pdp-statistics context select
- show ms950-pdp-statistics control
- show ms950-pdp-statistics data
- show ms950-pdp-statistics sgsns control-address
- show ms950-pdp-statistics sgsns select
- show ms950-pdp-statistics signalling-count
- show pdp-statistics-interval
- configure charging gateway
- configure charging node
- configure charging profile charging-gateway
- configure charging sgsn
- configure pdp-statistics
- configure pdp-statistics interval
- configure gtp
- configure gtp n3-request
- configure gtp path-echo-interval
- configure gtp path-echo-request
- configure gtp qos-forwarding-method
- configure gtp t3-response
- debug gtp
- debug gtpp
- subscription-required

Charging Parameters

The following parameters of charging commands are not supported by MS950 while acting as a CDMA HA:

```
MS(config-charging-pro-cdr)#
```

- generation

  Parameters gtpp and both not supported by a CDMAHA.
- optional-ies

  Parameters pdp-type, pdp-address, apn-selection-mode and msisdn not supported by a CDMAHA.
- optional-extensions

  Parameters roaming-group and qos-negotiated not supported by a CDMAHA.

Mobile IP Parameters

The following parameters of MIP commands are not supported by MS950 while acting as a CDMA HA:

```
MS(config-mip)#
```

- home-agent

  The keep-alive option is not supported in CDMA HA mode.
- subscriber-info, clear mip counts, delete mip context, show mip context, show mip subscriber-info

  The type imsi and msisdn are not supported in CDMA HA mode.

SNMP Parameters

The following parameters of SNMP are not supported by MS950 while acting as a CDMA HA:

GTP and GTPP SNMP traps are not supported by a CDMAHA.

Service Selection Node

SSN ~~CDMA~~ ~~GGSN~~

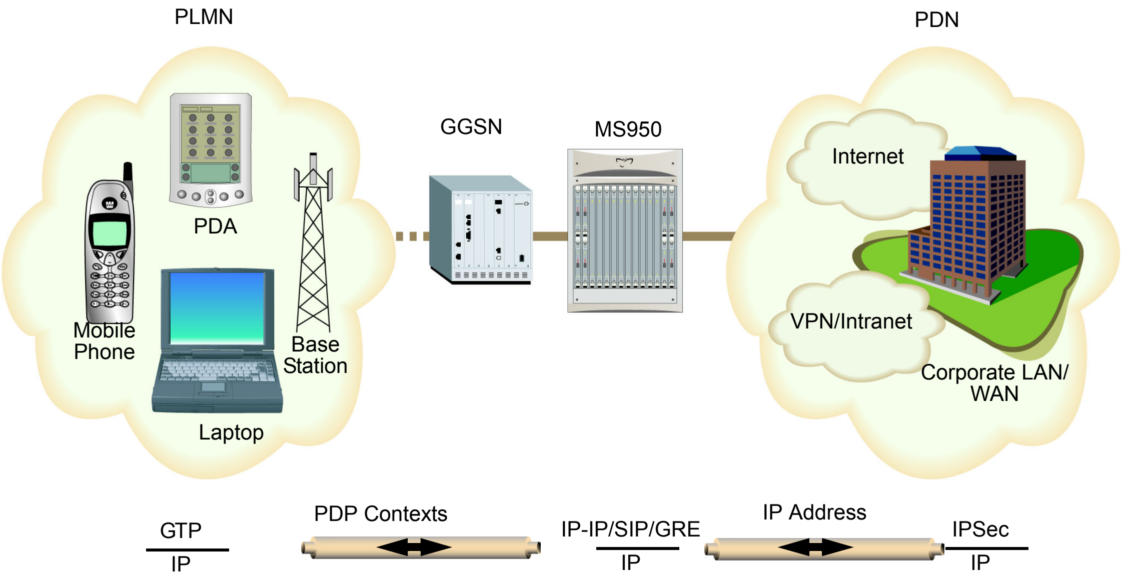
In some networks it is possible to deploy the MS950 as a subscriber-aware packet treatment platform without having to function as a GGSN, a Mobile IP Home Agent, or a PDSN. Examples of these include:

- deployment in situations in which there is an existing tunnel termination and session maintenance platform but without sophisticated subscriber-aware packet treatment capabilities
- deploymnet in a remote services network that does not provide any mobility or subscriber packet delivery infrastructure

The MS950 provides services by processing subscriber traffic. Therefore, in this solution, the network is configured such that all traffic from and to the tunnel termination box (a GGSN) is sent via the MS950. It should be noted that the third party GGSN (or tunnel termination device) in the networks shown above only terminate the access protocol (in this case GTP). All possible services such as VPNs and value-added services are provided by the MS950. There could be two modes of operation between the GGSN and the MS950:

- Co-located GGSN and MS950 with single port (single gige, one SC configuration): In this topology, the tunnel termination device is configured to forward all traffic out its Gi interface into inputs to the MS950.
- Remote Operation or co-located with multiple ports (multiple giges, multiple SCs): In situations in which the tunnel termination device is not co-located with the MS950 or there are multiple ports, traffic needs to be tunneled to the MS950 for subscriber-specific policy processing. The tunnel method of choice is GRE or IP-in-IP. There is one GRE or IP-in-IP tunnel from each Gi interface of the tunnel termination device to one port on the MS950. For VPN operation in which the external GGSN supports overlapping private addresses, a GRE or IP-in-IP tunnel is set up for each VPN. Both the GGSN and MS950 are configured to use a GRE or IP-in-IP tunnel for a VPN. All VPN traffic flows within this tunnel.

Note: The MS950 operates exclusively as a Service Selector Node, GGSN, or CDMA HA.



To configure The MS950 as a Service Selector in administrator or superuser mode:

1. Enter the following at the command prompt:
   `configure service-selector`
2. Enter the following at the command prompt to configure the RADIUS-client:
   `radius-client` *`name`* `[`**`key`** *`shared-secret`*`] [`**`ip-address`** *`address`*`] [`**`acct-message`** `[`**`drop`** `|` **`forward`**`}]`
3. Enter the following at the command prompt to create IP-IP policies:
   `ip-ip-policy` *`name`* `[`**`ggsn`** *`nas-ip-addr`*`] [`**`remote-endpoint`** *`address`*`] [`**`local-endpoint`** *`address`*`]`
4. Configure a tunnel interface with encapsulation set to IP-IP:
   `encapsulation` `{`**`ip-ip`**`}`
5. Configure a an APN ingress treatment type:
   `ingress-treatment` `{`**`simple-ip`** `|` **`gre`** *`tunnel-policy`*`|` **`ip-ip`** *`tunnel-policy`*`}`

Example

The following example configure the MS950 as a Service Selector.

```
MS# configure service-selector
MS(config-ssn)# radius-client name ggsn1 key
   testing123 ip-address 130.20.15.2
MS(config-ssn)# ip-ip-policy ippolocy1 ggsn 10.1.0.3
   remote-endpoint 10.15.67.8 local-endpoint
   130.20.15.15.2
MS(config-ssn)# exit all
MS# configure interface tunnel 14/0.1 name megisto-
   tunnel
MS(config-if-tun14/0.1)# encapsulation ipsec
MS(config-if-tun14/0.1)# exit all
MS# configure subscriber-partition user1
MS(config-subs)# access-point company1
MS(config-subs-apn)# ingress-treatment ip-ip ippol1
```

Displaying Service Selector Information

You can display the current Service Selector configuration via the **show radius-client** and **show ip-ip-policy** commands.

CIl Commands That Do Not Apply

The following is a list of CLI commands that do not apply when the MS950 acts as a Service Selection Node:

- clear debug-gtp
- clear debug-gtpp
- delete gtp imsi
- delete gtp pdp-context
- show apn-pdp-statistics apn
- show apn-pdp-statistics context apn
- show apn-pdp-statistics context select
- show apn-pdp-statistics last-interval
- show apn-pdp-statistics select
- show gtp counters
- show gtp imsi

- show gtp params
- show gtp pdp-context
- show gtp statistics
- show gtp status
- show imsi-pdp-statistics context imsi
- show imsi-pdp-statistics context select
- show ms950-pdp-statistics control
- show ms950-pdp-statistics data
- show ms950-pdp-statistics sgsns control-address
- show ms950-pdp-statistics sgsns select
- show ms950-pdp-statistics signalling-count
- configure pdp-statistics
- configure pdp-statistics interval
- configure gtp
- configure gtp n3-request
- configure gtp path-echo-interval
- configure gtp path-echo-request
- configure gtp qos-forwarding-method
- configure gtp t3-response

Chapter 4: Understanding the CLI User Interface

Most MS950 configuration tasks are performed via the CLI by an operator with one of three privileges: operator, administrator, or superuser. The prompt structure and entry of commands is similar to those of other commercial CLIs to provide ease-of-use. Instructions for using the CLI are contained in this chapter.

In This Chapter

Accessing the CLI

You can access the CLI via direct terminal connection, Telnet, and remote secure shell (SSH).

Initialization Script

When you bring up the MS950 for the first time or after the system has been wiped clean, an initialization script is presented. This script is detailed in the *MS950 Installation and Maintenance Guide* in detail and is summarized here.

The script first asks you to provide a system name. This is the name that appears in the prompt. It can be changed or configured without using this script via the **`snmp server`** command. See “SNMP” on page 16-1.

The second question asks you to provide the IP address and netmask of a Fast Ethernet port. This refers to the first (fei9/0) of the three ports. It is used for CLI access via Telnet. In lieu of using this script, you can configure this interface via the **fastethernet** command. See "Fast Ethernet Interfaces" on page 8-3.

RS-232

You can access the CLI via a terminal attached to the MS950 (RS-232 port (DB-9)). Connect the port as described in the *MS950 Installation and Maintenance Guide*. You can use any terminal emulation program for access. The terminal emulation settings are **19200, N, 8, 1**.

Telnet

You can establish a Telnet session to the CLI. You need to know the domain name or IP address of the first Fast Ethernet port as set in your initialization script or as configured in a Fast Ethernet interface. Your passwords and privilege level are established during initial setup. See the *MS950 Installation and Maintenance Guide*.

Other Access

You can also access the CLI via SSH. See "Configuring SSH" on page 13-3.

Operator Privileges

An operator can have one of three privilege levels:

- operator
- administrator
- superuser

Operator Mode

Operator mode provides display-level access to the MS950 file system. You can view folder contents and display status information but cannot make any changes to system configuration.

To perform operator operations:

1. Access the CLI via Telnet or serial port.
2. Enter your operator *username* and *password*.

   The username and password is set by the superuser. You are placed in operator mode as indicated by the `MS>` prompt.

Note: Throughout this guide the prompt is shown as **`MS`**. If you assigned an SNMP hostname via the **`snmp server`** command or assigned a system name via the initialization script, the configured hostname is displayed in the prompt.

Administrator Mode

Administrator (admin) mode allows you to modify configuration settings. You can add and change a variety of physical and virtual settings. You cannot modify user profiles.

To perform administrator operations:

1. Access the CLI via Telnet or serial port.
2. Enter your administrator *username* and *password*.

   The username and password is set by the superuser. You are placed in Administrator mode as indicated by the `MS#` prompt.

Note: Throughout this guide the prompt is shown as **`MS`**. If you assigned an SNMP hostname via the **`snmp server`** command or assigned a system name via the initialization script, the configured hostname is displayed in the prompt.

To perform administrator operations after logging in as operator:

1. Access the CLI via Telnet or serial port.
2. Enter your *username* and *password*.

   The username and password is set by the superuser. You are placed in Administrator mode as indicated by the `MS#` prompt.

   The changes you make in this mode are recorded in the configuration file.

Note: Throughout this guide the prompt is shown as **`MS`**. If you assigned an SNMP hostname via the **`snmp server`** command or assigned a system name via the initialization script, the configured hostname is displayed in the prompt.

Superuser Mode

Superuser mode allows you to modify configuration settings as well as modify user profiles. You can add and change a variety of physical and virtual settings.

Note: The first time you access the CLI you are placed in superuser mode. The default username and password is **`admin`**.

To perform superuser operations:

1. Access the CLI via Telnet or serial port.
2. Enter your Superuser *username* and *password*.

   The initial username and password was determined in your initial setup as described in the *MS950 Installation and Maintenance Guide*.

   You are placed in superuser mode as indicated by the **`MS#`** prompt.

Note: Throughout this guide the prompt is shown as **`MS`**. If you assigned an SNMP hostname via the **`snmp server`** command or assigned a system name via the initialization script, the configured hostname is displayed in the prompt.

Prompt Configuration and Structure

System prompts are in the form **`hostname(parent command)privilege_level`**. The mode expands to indicate sub-levels. For example, the prompt **`MS(config-subs-apn)#`** indicates that you are on the machine named MS, are in administrator (or superuser) mode, and are configuring the APN parameters for a subscriber partition.

Mode Prompt	Description	Example
>	Operator mode	MS>
#	Administrator	MS(config-sub-apn)#
#	Superuser - prompt is the same as Administrator mode	MS(config-sub-apn)#

Note: Throughout this guide the prompt is shown as **`MS`**. If you have assigned an SNMP hostname via the **`snmp server`** command or assigned a system name via the initialization script, the configured hostname will be displayed in the prompt.

Entering Configuration Commands

You must be in administrator or superuser mode to perform configuration tasks. To perform configuration tasks, type **`configure`** prior to the first configuration command in the group. For example, if you want to configure SNMP parameters, use **`configure snmp`**. You are placed in (config-snmp) from this point forward.

```
MS# configure snmp
MS(config-snmp)#
```

You may also enter **`configure`** alone and then enter the next-level command. For example:

```
MS# configure
MS(config)# snmp
MS(config-snmp)#
```

So long as you are entering SNMP commands, you do not need to type the words **`configure`** or **`snmp`** again (unless they are part of another command). You need to back out of the existing command structure using the **`exit`** or **`exit all`** commands to enter a new command structure.

You can type part of a command and press the **`tab`** key for command completion.

```
MS# con[tab]
MS# con[tab]figure
```

In most cases, the CLI recognizes the first two to three letters of a command.

History and Editing

You can navigate the command structure by entering commands or keystrokes. To go back up one level in the command structure type **`exit`**. To go back to the top level (for example, administrator (**`MS#`**)) type **`exit all`** or press **`ctrl-z`**. You can use the **`history`** command to list the most recent 30 commands entered. All hot keys are listed in the table below.

Key	Action
backspace	move left and delete the character
ctrl-a	move to the beginning of the line
ctrl-b or left arrow	move cursor left over characters without deleting the character
ctrl-d	delete the current character
ctrl-e	move to the end of the line
ctrl-f or right arrow	move cursor right over characters without deleting the character
ctrl-k	delete the text after the cursor
ctrl-n or down arrow	get the next command history
ctrl-p or up arrow	get prior command history
ctrl-t	transpose current and previous character
ctrl-u	delete all the text prior to the cursor
ctrl-w	delete the word prior to the cursor
ctrl-z	enter the command and return to root prompt
enter	execute the command and enter intermediate mode
esc-b	move back one word
esc-d	delete the remainder of the word
esc-f	move forward one word
tab	command completion. After you type the first few unique letter of the command, the rest of the command is typed for you.

Chapter 5: User Setup

You can add and delete users as well modify their privileges via superuser mode. A user is a person (an operator) who has access to the MS950 via Telnet or another method and can either view or modify system settings. You can set up to 100 user accounts, however, only 12 users can be on the MS950 at one time. Ten of these can be connected remotely via Telnet and 2 via direct serial connection. Users can have a variety of file and access privileges.

User accounts can be changed only by an account with superuser privilege. For an account with superuser privilege only the password can be changed. For all other users, once the user name is established, it cannot be modified. The superuser can change the password and access level for each user or completely delete the user, but the user name cannot be changed.

Note: The default login account "admin" has superuser privilege.

In This Chapter

Adding Users

As superuser, you can add users to the system at any time. Users can have operator or administrator privileges.

To add users in superuser mode:

1. Enter the following at the command prompt:
   `user`
2. Enter the following at the command prompt to add users:
   ```
   add name name level {operator | admin | superuser}
      {group name} [password-hash name]
   ```
   The prompt **`Enter new password`** appears.
3. Enter a password at the **`Enter new password`** prompt:
   The prompt **`Confirm new password`** appears.
4. Enter the same password that you entered in step 2 at the **`Confirm new password`** prompt.

Example

The following example adds a new user to the system.

```
MS# user
MS(user)# add john level operator group cdr-admin
Enter new password: ******
Confirm new password: ******
```

Deleting Users

As superuser, you can delete users from the system at any time.

To delete users in superuser mode:

1. Enter the following at the command prompt:
   `user`
2. To delete the user, enter the following at the command prompt:
   `delete` *`name`*

Example

The following example adds a new user to the system and then deletes user.

```
MS# user
MS(user)# add john level operator group cdr-admin
Enter new password: ******
Confirm new password: ******
MS(user)# delete john
```

Changing Privileges

When you add users, you also set user privileges. To change established user privileges and passwords, additional commands are needed.

To change a password, access, or group assignment in superuser mode:

1. Enter the following at the command prompt:
   user
2. Enter the following at the command prompt:
   ```
   update name [level {operator | admin | superuser}]
      [password] [password-hash name] [group name]
   ```
   The prompt **Enter new password** appears.

   Enter a password at the **Enter new password** prompt:

   The prompt **Confirm new password** appears.

Note: You can rename a group using the **group** command.

3. Enter the same password that you entered in step 2 at the **Confirm new password** prompt.

Example

The following example changes a user's password and privilege level.

```
MS# user
MS(user)# add john level operator group cdr-admin
Enter new password: ******
Confirm new password: ******
MS(user)# update john level admin group installer
```

Ending a Session

To end your user session use the **`logout`** command. This exits the current session and returns you to the login prompt.

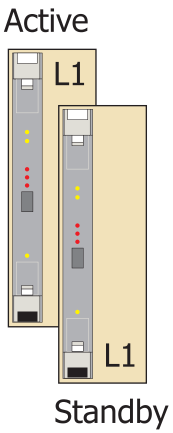
Displaying Users

You can display all created users via the **`show user`** command and all currently logged in users via the **`who`** command.

Chapter 6: Card Configuration

In This Chapter

- Configuring Cards
- Toggling Modes
- Connecting Cards



The MS950 has 18 slots for 2 fabric cards, 2 control cards, 6 service cards, and 8 line cards.

Each card can play one of two roles:

- primary (active)
- standby

Two or more cards of the same type (e.g., line cards with line cards) can be assigned a group. In a group, one card plays the standby role while the others are active.

A card cannot be made operational until it is configured with the **`card`** command. After this configuration, you can configure line card and service card connections (see “Connecting Line Cards” on page 6-3) and then interfaces.

Redundancy Groups

A redundancy group is a set of one or more cards in one functional group. If there are multiple cards in a redundancy group, there can be only one standby card. All other cards of the redundancy group must be configured to be active. The redundancy group configuration concept applies to service cards, line cards, and fabric cards. Control cards are delivered with factory-set redundancy; therefore, you cannot assign groups to them. Redundancy configuration is described in “Configuring Cards” on page 6-2.

You must go back to the original card configuration of line cards or service cards before you can reconfigure the cards in that redundancy group (e.g., for defining different redundancy groups).

Configuring Cards

You can configure the role of the card, switch over to another mode, and display the current card configuration. Prior to configuring your cards you must know the physical slot number of each card.

Note: A card can be removed from a redundancy group only if the connection (see “Connecting Line Cards” on page 6-3) for this card has first been deleted. The card can also be removed from a redundancy group only if it is not currently involved in a switchover/failover event. If so, you must first switch the traffic of the card so that the card is in its original redundancy mode then remove it from the redundancy group.

The following procedure sets the MS950 in config mode and sets redundancy options.

To configure cards in administrator or superuser mode:

1. Enter the following at the command prompt:
   ```
   configure card {line-card | service-card | fabric-
      card} slot_number
   ```
2. Enter the following at the command prompt to assign the card to a redundancy group:
   ```
   group group_name role {active | standby}
   ```
3. Enter the following at the command prompt to enable the card:
   ```
   no shutdown
   ```
4. Repeat steps 1, 2, and 3 for each card.

Note: After you configure cards, you can connect cards and then create interfaces.

Example

The following example configures the line card on slot 2. It assigns the card to group L4 and puts it in standby mode. It then configures a second card.

```
MS# configure card line-card 2
MS(config-card-slot2)# group l4 role standby
MS(config-card-slot2)# no shutdown
MS(config-card-slot2)# exit all
MS# configure card line-card 3
MS(config-card-slot3)# group l4 role active
MS(config-card-slot3)# no shutdown
```

Toggling Modes

You can toggle between standby and primary mode without reconfiguring your cards. This is a convenient way to meet a temporary need.

To toggle modes in administrator mode:

1. Enter the following at the command prompt:
   ```
   switchover [line-card | service-card | control-card |
      fabric-card] slot_number
   ```
2. Repeat step 1 for each card you wish to switchover.
3. Repeat step 1 when you wish to switch the card back to original configuration.

Example

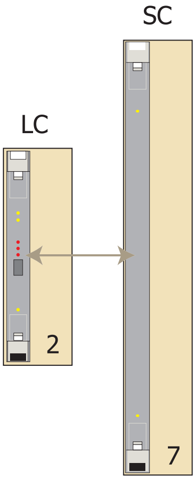
The following example toggles the mode for the line card in slot 2.

```
MS# switchover line-card 2
```

Connecting Line Cards

The MS950 performs all Layer 3 processing on service cards while it performs all Layer 2 processing on line cards. This design departs from

Card Configuration



the traditional line card or line card/forwarding engine approach for two reasons:

First, the MS950 is a purpose-built device that concentrates on providing fast, reliable, and scalable processing of GTP and IPSec traffic. GTP and IPSec (tunnel mode) traffic encapsulates IP datagrams, hence, all traffic is destined to the MS950. Highly scalable GTP and IPSec processing units can potentially receive traffic from any line card thus expanding processing capability.

Second, line card real estate is becoming increasingly inexpensive in today's industry with the advent of highly programmable chip technology. By separating the forwarding engine and specialized protocol processing portions from the basic line card functionality, line cards keep up with the bit rate demands of the industry.

You must statically associate a line card with a service card. This provides an Layer 2 interface to the service card. If the Layer 2 interface goes down for any reason, Layer 3 processing is unaffected. The static association is configured and can be modified via the CLI. This is useful in case of line card fault and can be done at time of switchover to a standby card.

The connecting of cards can be performed only after you have configured line cards, service cards, and fabric cards. See "Configuring Cards" on page 6-2. It can also be used to change the line card/service card association. You must connect each line card to a specific service card prior to configuring any interfaces.

To connect a line card to a service card in admin or superuser mode:

1. Configure line card, service cards, and fabric cards as shown in "Configuring Cards" on page 6-2.

Note: The fabric card must be configured before you can connect line cards to service cards.

2. Enter the following at the command prompt to connect a line card to a service card:

```
connect line-card slot_number service-card slot_number
```

3. Repeat step 2 for each line card.

Note: Interfaces can be configured only after you have configured cards and connected cards. You can connect cards only after cards have been configured.

Example

The following example configures the line card on slot 2, assigning it to group L4 in active mode. It then configures the service card on slot 5, assigning it to group S1 in active mode. The active fabric card is configured. Line card 2 and service card 5 are then connected.

```
MS# configure card line-card 2
MS(config-card-slot2)# group l4 role active
MS(config-card-slot2)# exit all
MS# configure card service-card 5
MS(config-card-slot5)# group s1 role active
MS(config-card-slot5)# exit
MS# configure card fabric-card 8
MS(config-card-slot8)# group f1 role active
MS(config-card-slot8)# exit all
MS(config)# connect line-card 2 service-card 5
```

Displaying Card Configuration

The configuration of cards is displayed via the **show connect** and **show card** commands.

Card Configuration

Chapter 7: The File System

The Megisto CLI provides many features common to most commercial command line interfaces (CLI). This chapter describes the MS950 file system and basic CLI commands.

Viewing the File system

The local file systems contain flash memory and RAM sufficient to retain system images, configuration files, and system log files. Although other directories may be visible, the following directories are user-accessible on the MS950:

Directory Name	Description
fs1:	A CompactFlash device. Configuration files and scripts may be copied here.
fs2:	A CompactFlash device or NFS. Used for storage of files or new releases.
system:	RAM storage created on boot. Contents not retained on reboot. Location for log and running configuration files.
system:/cdr	Location of call data records (CDRs).
fs1:/user0	Location of default configuration files, such as ssh.cfg and startup.cfg.
fs1:/user0/bulk	Location of bulk statistics.

You can view the contents of the file system using standard operating system commands. To view the content of a directory use `dir,` and to see the current working directory use `pwd`. To change directories use `cd`.

Navigating the File System

With the appropriate privilege, you can execute file management commands within the file system as well as create and modify a variety of system-level files important to the basic operation of the MS950.

Copying and Deleting Files

You can create and remove files in a file system using standard operating system commands. For example, to create directory structures use **`mkdir`** and to delete use **`rmdir`**. You can copy/FTP a file into the file system using **`copy`** and delete it using **`delete`**. Reformat a device (deleting the file system completely) using **`format`**. Delete the file system without reformatting the device using **`erase`**. Delete files and directories using the **`delete`** command and rename files via the **`rename`** command.

Note: Use of the commands, **`format`**, **`erase`**, **`rename`**, and **`delete`** on system files may affect system operation.

File Security

You can add or delete a user group from a local file’s user access list. After adding a user group to a file’s user group list, users in that group can read and write the file, unless the read-only parameter is applied.

After r group is removed from a file’s user access list, users no longer have read or write access. To remove only write access, you must first remove the group from the file’s group list and add it again specifying the read-only parameter.

You can also set the file creation masks that are used by various MS950 subsystems. These masks indicate the list of groups that are automatically given access to files created by a given subsystem. The current group lists used for each subsystem's mask can be viewed with the **`show groups`** command. The command operation on a given subsystem's group mask is similar to the command operation on a given filename. Adding a group to a subsystem causes the files that are created by that subsystem to become accessible to all users in that group. If the read-only parameter is supplied, then users in the added group are granted read access only on the files created by that subsystem.

Note: Adding a group to or removing a group from a given sub-system does not affect any existing files. It affects only files that are created after the command has been issued.

To set file permissions:

1. Enter the following at the command prompt to assign file permissions:

```
file-user-group {add | remove} {filename filename |
   sub-system subsystem} [groupname groupname] [read-
   only]
```

Example

The following example changes a user's file privilege level.

```
MS# file-user-group add filename fs1:/user0/cert/
   log.doc groupname security-admin read-only
```

CLI Scripts

Executing CLI Scripts

You can execute custom-created CLI scripts via the `exec` command. CLI scripts can reduce the amount of command entry needed for system configuration. All CLI scripts must placed in the **system:** folder via the `copy` command.

Example

The following script is a text file called cli_script.txt. It is executed in the order commands are entered in the file.

```
MS# exec -echo fs1:/user0/cli.txt
```

Creating CLI Scripts

CLI scripts are created in text files. Commands are entered into the file in the order in which they are to be executed. The script should not contain any commands that return data back to the console, such as show commands. All CLI debugging should be turned off prior to executing the script. If the script finds an error, such as debugging remaining on, the script stops at the point of error. All commands in the script should be concatenated so that that they start from the root of administrator mode (MS#). The appropriate **exit** or **exit all** command must be incorporated into the script. Complete configuration files can be executed as scripts.

Example

The following commands are contained in a text file called cli_script.txt.

```
configure
card line-card 2
group l2 role active
exit all
configure
card line-card 18
group l2 role active
exit all
configure
card service-card 14
group s1 role active
exit all
configure
card service-card 6
group s1 role active
exit all
configure
card fabric-card 8
group f1 role active
exit all
configure
card fabric-card 11
group f1 role standby
exit all
```

```
configure connect line-card 2 service-card 14
configure connect line-card 18 service-card 6
exit all
```

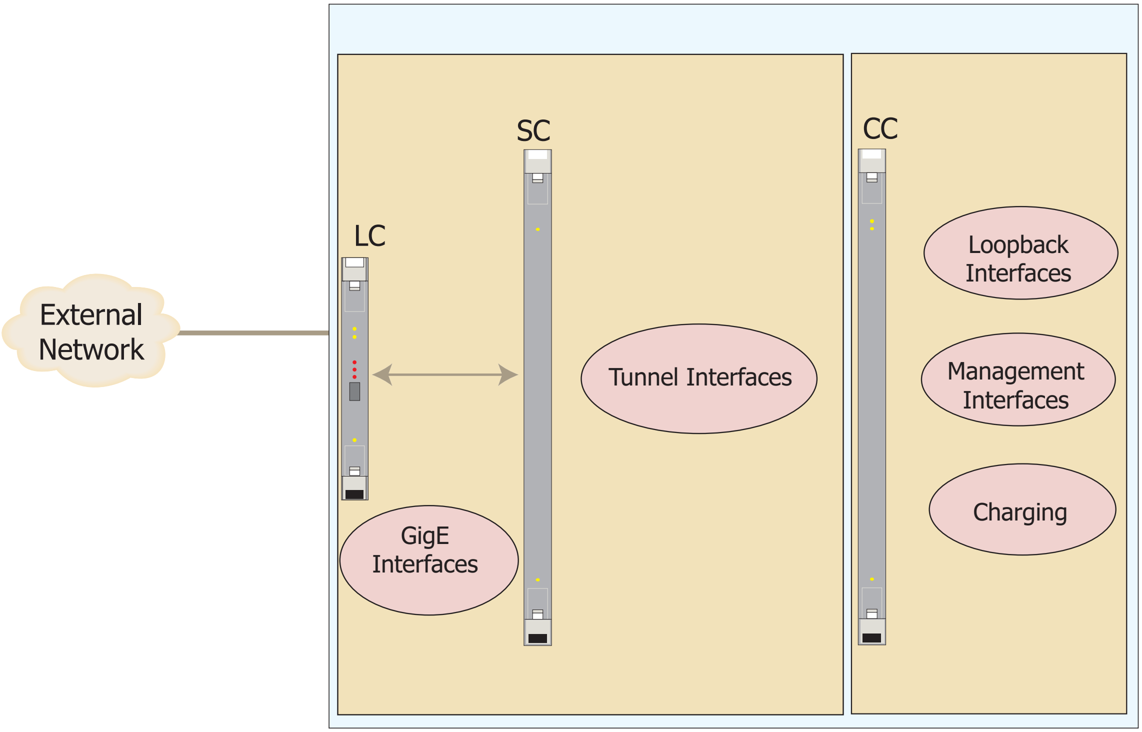
Configuration Files

You can view the current running configuration file using the **`show running-config`** command or the startup configuration file via **`show startup-config`**. Use the **`copy running-config to startup-config`** command to save the currently configured settings to the startup configuration file. The next configuration session will use those settings.

Note: The startup configuration file (startup.cfg) is always used on reboot. If you did not save your current session using the **`copy running-config`** command, the last saved settings are used.

Section II: Network Connection

The chapters in this section describe features that help place the MS950 in your network. It includes the setup of a variety of interfaces, routing information, IP services, charging parameters, GTP information, and network security.



Chapter 8: Interfaces

The MS950 features two types of interfaces: physical and virtual. Physical interfaces are connected to Gigabit Ethernet devices or to Fast Ethernet ports for OA&M connectivity. Virtual interfaces are logical entities that exist on service and control cards.

Note: Interfaces are created after you configure and connect cards. See "Configuring Cards" on page 6-2 and "Connecting Line Cards" on page 6-3.

Note: Interfaces are created in the down state (shutdown). They need to be unlocked via the **`no shutdown`** command to enable operation.

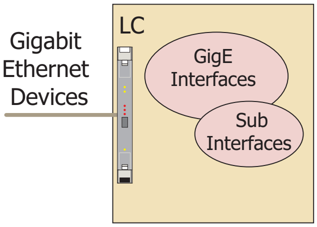
In This Chapter

- Physical Interfaces
- Virtual Tunnel Interfaces
- Virtual Management Interfaces
- Virtual Loopback Interfaces
- Displaying Interface Information
- Modifying Interfaces

Physical Interfaces

Physical interfaces provide physical connections to Gigabit Ethernet devices or Fast Ethernet ports.

Gigabit Ethernet Interfaces



Before you can configure Gigabit Ethernet interfaces, you need to know which slot the line cards for that interface populates (1-4 and 15-18) in your MS950 chassis. In addition, your router or switch must be set to auto-negotiate in order to communicate with the MS950 via Gigabit Ethernet interfaces.

To create Gigabit Ethernet interfaces from administrator mode:

1. Enter the following at the command prompt:

```
configure interface gigethernet slot_number/
   port_number [description] network [ran | internet |
   both]
```

2. Enter the following at the command prompt to assign the IP address:

   ```
   ip-address ip_address mask [secondary]
   ```

   This command assigns static IP addresses. The **secondary** keyword allows you to designate the address as a secondary IP address for the interface.

3. If desired, enter the following at the command prompt to change the amount of MTU bytes:

   ```
   mtu size
   ```

4. If desired, enter the following at the command prompt to specify an access list:

   ```
   access-group access_list_name {in | out}
   ```

   Access list parameters are set in “Creating Access Lists” on page 13-1.

5. If desired, enter the following at the command prompt to enable direct-broadcast:

   ```
   direct-broadcast
   ```

6. If desired, enter the following at the command prompt to enable the sending of ICMP unreachable messages:

   ```
   unreachable
   ```

7. If desired, enter the following at the command prompt to enable or disable ARP:

   ```
   arp
   ```

   Parameters for ARP are configured in “Configuring ARP” on page 10-1.

8. If desired, enter the following at the command prompt to enable encapsulation:

   ```
   encapsulation {dix | 802.3}
   ```

9. Enter the following at the command prompt to enable the interface:

   ```
   no shutdown
   ```

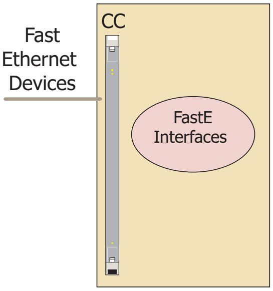
Example

The following example sets the MS950 in config mode, creates a Gigabit Ethernet interface on slot 1, and names it megisto-gig. It assigns an IP address and a secondary IP address. It also enables direct broadcast, modifies the amount of MTU bytes, enables ARP, and disables sending

ICMP unreachable messages. This interface operates for the RAN side of the Internet.

```
MS# configure interface gigethernet 1/0 megisto-int
   network ran
MS(config-if-gige1/0)# ip-address 192.168.40.2
   255.255.255.0
MS(config-if-gige1/0)# ip-address 10.0.0.1
   255.255.255.0 secondary
MS(config-if-gige1/0)# direct-broadcast
MS(config-if-gige1/0)# arp
MS(config-if-gige1/0)# mtu 1000
MS(config-if-gige1/0)# no unreachable
MS(config-if-gige1/0)# access-group acl25 in
MS(config-if-gige1/0)# encapsulation dix
MS(config-if-gige1/0)# no shutdown
```

Fast Ethernet Interfaces



Before you configure Fast Ethernet interfaces, you need to know which port your Fast Ethernet device will use on the control card (slot 9).

To create Fast Ethernet interfaces from administrator mode:

1. Enter the following at the command prompt:
   configure interface fastethernet *slot_number*/
      port_number [*description*]
2. Enter the following at the command prompt to assign the IP address:
   ip-address *ip_address mask* [**secondary**]

   This command assigns static IP addresses. The **secondary** keyword allows you to designate the address as a secondary IP address for the interface.
3. If desired, enter the following at the command prompt to change the amount of MTU bytes:
   mtu *size*
4. If desired, enter the following at the command prompt to specify an access list:
   access-group *access_list_name* {**in** | **out**}

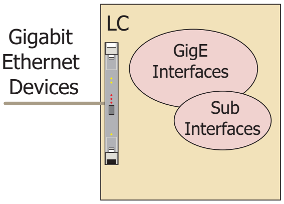
   Access list parameters are set in “Creating Access Lists” on page 13-1.
5. Enter the following at the command prompt to enable the interface:
   no shutdown

Example

The following example sets the MS950 in config mode, creates a fastethernet interface on slot 9 port 1 named fei9/1, and describes it as telnet. It then modifies the MTU setting and assigns an access list.

```
MS# configure interface fastethernet 9/1 telnet
MS(config-if-fei9/1)# ip-address 192.168.40.2
   255.255.255.0
MS(config-if-fei9/1)# ip-address 10.0.0.1
   255.255.255.0 secondary
MS(config-if-fei9/1)# mtu 1000
MS(config-if-fei9/1)# access-group acl25 in
MS(config-if-fei9/1)# no shutdown
```

Sub-interfaces



A sub-interface is a virtual instance of a physical interface. Configuring multiple virtual interfaces, or sub-interfaces, on a single physical interface allows greater flexibility and connectivity on the network. Sub-interfaces support VLANs. You must configure a sub-interfaces specifically for VLAN operation.

To create virtual sub-interfaces in administrator mode:

1. Enter the following at the command prompt:
   ```
   interface gigethernet slot_number/port_number.subif
      [description] network [ran | internet | both]
   ```

Note: If the sub-interface is intended for use with VPNs, the internet network must be used.

2. Enter the following at the command prompt:
   ```
   vlan number [vpn-name name]
   ```
   You can set up VLANs for sub-interfaces. In the case of Gigabit Ethernet physical interfaces you can assign an IEEE802.1q/p VLAN tag that identifies Layer 2 frames addressed to a particular sub-interface. The VPN-name parameter is used only when a VPN is needed for the APN.

Note: VLANs must be created prior to configuring the IP address of sub-interfaces.

3. Enter the following at the command prompt to assign the IP address:

```
ip-address ip_address mask [secondary]
```

This command assigns static IP addresses. The **secondary** keyword allows you to designate the address as a secondary IP address for the interface.

4. If desired, enter the following at the command prompt to change the amount of MTU bytes:

   ```
   mtu size
   ```

5. If desired, enter the following at the command prompt to specify an access list:

   ```
   access-group access_list_name {in | out}
   ```

   Access list parameters are set in “Creating Access Lists” on page 13-1.

6. If desired, enter the following at the command prompt to enable the sending of ICMP unreachable messages:

   ```
   unreachable
   ```

7. If desired, enter the following at the command prompt to enable or disable ARP:

   ```
   arp
   ```

   Parameters for ARP are configured in “Configuring ARP” on page 10-1.

8. If desired, enter the following at the command prompt to enable direct-broadcast:

   ```
   direct-broadcast
   ```

9. Enter the following at the command prompt to enable the interface:

   ```
   no shutdown
   ```

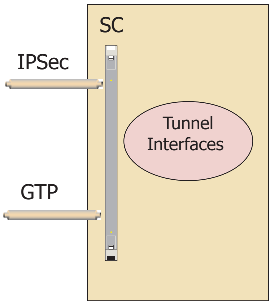
Example

The following example sets the MS950 in config mode, creates a sub-interface on slot 1 port 0 with a sub-interface-ID of 2, names it gige1/0.2, and describes it as megisto-sub. It connects to the Internet side of the network and configures additional interface options.

```
MS# configure interface gigethernet 1/0.2 megisto-sub
   network internet
MS(config-subif-gige1/0.2)# vlan 3
MS(config-subif-gige1/0.2)# ip-address 192.169.24.73
   255.255.255.0
MS(config-subif-gige1/0.2)# ip-address 192.168.40.3
   255.255.255.0 secondary
MS(config-subif-gige1/0.2)# mtu 1000
```

```
MS(config-subif-gige1/0.2)# arp
MS(config-subif-gige1/0.2)# direct-broadcast
MS(config-subif-gige1/0.2)# no unreachable
MS(config-subif-gige1/0.2)# access-group acl25 in
MS(config-subif-gige1/0.2)# no shutdown
```

Virtual Tunnel Interfaces



Tunnel interfaces are virtual interfaces used by tunneling mechanisms as end points for IP tunnels.

To create tunnel interfaces in administrator or superuser mode:

1. Enter the following at the command prompt:
   configure interface tunnel *slot_number*/
   port_number.instance [*description*]
2. Enter the following at the command prompt to assign the IP address:
   ip-address *ip_address mask* [**secondary**]

   This command assigns static IP addresses. The **secondary** keyword allows you to designate the address as a secondary IP address for the interface.
3. If desired, enter the following at the command prompt to change the amount of MTU bytes:
   mtu *size*
4. If desired, enter the following at the command prompt to specify the encapsulation mechanism of a tunnel interface:
   encapsulation {**gtp** | **ipsec**}

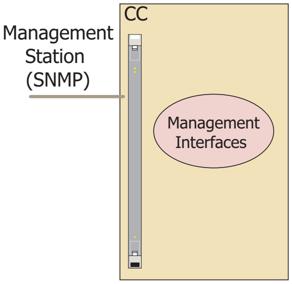
   GTP parameters are configured in “Configuring GTP” on page 11-1. IPSec parameters are configured in “Configuring IPSec and IKE” on page 21-2.
5. Enter the following at the command prompt to enable the interface:
   no shutdown

Example

The following example sets the MS950 in config mode, creates a tunnel interface on service card 16 with an index number of 1 named tun16/0.1, and describes it as megisto-tunnel. It then performs common virtual interface configuration tasks and enables GTP encapsulation.

```
MS# configure interface tunnel 16/0.1 megisto-tunnel
MS(config-if-tun16/0.1)# ip-address 192.168.40.2
   255.255.255.0
MS(config-if-tun16/0.1)# mtu 1000
MS(config-if-tun16/0.1)# encapsulation gtp
MS(config-if-tun16/0.1)# no shutdown
```

Virtual Management Interfaces



Management interfaces are virtual interfaces used in conjunction with sub-interfaces to receive or send MS950 management traffic. Management interfaces are located on the control card.

To create virtual management interfaces in administrator mode:

1. Enter the following at the command prompt:
   configure interface management *instance* [*description*]
2. Enter the following at the command prompt to assign the IP address:
   ip-address *ip_address mask* [**secondary**]

   This command assigns static IP addresses. The **secondary** keyword allows you to designate the address as a secondary IP address for the interface.
3. If desired, enter the following at the command prompt to change the amount of MTU bytes:
   mtu *size*
4. Enter the following at the command prompt to enable the interface:
   no shutdown

Example

The following example sets the MS950 in config mode, creates a management interface with a virtual instance of 32, and describes it as megisto-management.

```
MS# configure interface management 32 megisto-
   management
```

```
MS(config-if-mgmt2)# ip-address 192.168.40.2
   255.255.255.0
MS(config-if-mgmt2)# mtu 1000
MS(config-if-mgmt2)# no shutdown
```

Virtual Loopback Interfaces

Loopback interfaces are virtual interfaces used for data processing. Loopback interfaces are primarily located on service cards but can also be located on control cards.

To create loopback interfaces in administrator mode:

1. Enter the following at the command prompt:
   ```
   configure interface loopback slot_number/
      port_number.instance [description]
   ```
2. Enter the following at the command prompt to assign the IP address:
   ```
   ip-address ip_address mask [ms-id]
   ```
   This command assigns static IP addresses. Note that the ms-id parameter "is used only for loopback interfaces and to assign an ID to the MS950.
3. If desired, enter the following at the command prompt to change the amount of MTU bytes:
   ```
   mtu size
   ```
4. Enter the following at the command prompt to enable the interface:
   ```
   no shutdown
   ```

Example

The following example sets the MS950 in config mode, creates a loopback interface, and performs common virtual interfaces configuration tasks.

```
MS# configure interface loopback 17/0.145 megisto-loop
MS(config-if-lo17/0.145)# ip-address 192.168.40.2
   255.255.255.0 ms-id
MS(config-if-lo17/0.145)# mtu 1000
MS(config-if-lo17/0.145)# no shutdown
```

Displaying Interface Information

After interfaces have been created and configured, you can display their configuration information.You can display all interfaces using **`show interface all`** or just one type of interface using **`show interface`** *`interface_type`*. You can display detailed information about a specific interface with the **`show interface name`** command.

Modifying Interface Configuration

Use the **`interface`** commands to modify any existing interface as well as to create a new interface.

Chapter 9: Routing

The MS950 supports network reachability using static routes, RIP, router discovery, and default gateway parameters.

Configuring Static Routing

You can configure one or more static routes. A static route remains in the routing table until removed. When the MS950 receives an incoming packet, it checks the destination address and associates the address with the next-hop address and outgoing interface. When there is a network outage that causes the optimal route to become unavailable, the MS950 rediscovers the next-best optimal route. You may assign multiple routes from which the MS950 can select.

To add static routes and establish the default next-hop router in administrator mode:

1. Enter the following to enter the configure IP environment:
   `configure ip`
2. Enter the following at the command prompt to add a static-route:
   ```
   route ip_address network_mask
      ip_address [cost cost_number]
   ```
3. Repeat step 2 for each static route you wish to add.

Example

The first example below adds routes to the routing table and establishes the next-hop router IP address. The second adds a default route.

```
MS# configure ip
MS(config-ip)# route 128.89.1.0 255.255.255.0 4.0.0.1
MS(config-ip)# route 0.0.0.0 0.0.0.0 10.128.1.254
```

Display Routing Information

You can display routing information using show commands. You can show all routes via the **`show ip route`** command.

The routing table stores routes to directly attached devices, static IP routes, and routes configured in subscriber records.

Configuring RIP

RIP (Routing Information Protocol) is a widely used protocol for managing router information. You can configure a specific interface to use RIP or you can have all interfaces use RIP. RIP is considered an effective solution for small, homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network. The MS950 sends RIP messages, but does not hear RIP messages from external routers.

To configure RIP:

1. Enter the following at the command prompt to enter configuration mode:
   `configure rip`
2. Enter the following at the command prompt to configure the global RIP timer:
   `timer` *`seconds`*

Note: It is recommended that you do not change the value of the timer unless you know the specific desired value.

3. Enter the following at the command prompt to configure RIP authentication for an interface:

auth-type {**none** | **simple-password**} **interface-name** *name*

4. If simple-password is chosen, enter the following at the command prompt:
auth-key *key* **interface-name** *name*
5. Enter the following at the command prompt to enable (or disable) RIP:
status {**enable** | **disable**} **interface-name** *name*

Example

The following example configures a specific interface to use RIP.

```
MS# configure rip
MS(config-rip)# timer 45
MS(config-rip)# auth-type simple-password interface-
   name gigethernet2/0.1
MS(config-rip)# auth-key qwertyuiop interface-name
   gigethernet2/0.1
MS(config-rip)# status enable interface-name
   gigethernet2/0.1
```

Displaying RIP information

You can display the RIP table using the **show rip configuration** and **show rip statistics** commands.

Configuring OSPF

OSFP (Routing Information Protocol) is a widely used protocol for managing router information. In the MS950 its primary purpose is to inform adjacent routers of reachable addresses on the MS950. You can configure one OSPF instance per interface (via sub-interface). The use of OSPF on the MS950 is specifically for advertisement of reachable addresses and configuring OSPF on the system does not turn it in to a transit router.

To configure OSPF:

1. Enter the following at the command prompt to enter configuration mode:
configure ospf *address* | **all**

2. Enter the following at the command prompt to configure RIP authentication for an interface:
   `auth-type {none | simple-password}`
3. If simple-password is chosen, enter the following at the command prompt:
   `auth-key key`
4. Enter the following at the command prompt to specify the area type:
   `area-type {normal | stub}`
5. Enter the following at the command prompt to specify the cost:
   `cost cost`
6. Enter the following at the command prompt to specify the dead-interval:
   `dead-interval interval`
7. Enter the following at the command prompt to specify the hello-interval:
   `hello-interval interval`
8. Enter the following at the command prompt to specify the retransmit-interval:
   `retransmit-interval interval`
9. Enter the following at the command prompt to specify the transit-delay:
   `transit-delay interval`
10. Enter the following at the command prompt to enable (or disable) OSPF:
    `enable | disable`

Example

The following example configures a specific interface to use RIP.

```
MS# configure ospf
MS(config-ospf)# area-type stub
MS(config-ospf)# auth-type simple-password
MS(config-ospf)# auth-key qwertyuiop
MS(config-ospf)# cost 50
MS(config-ospf)# dead-interval 49
MS(config-ospf)# hello-interval 49
MS(config-ospf)# retransmit-interval 49
MS(config-ospf)# transit-delay 49
MS(config-ospf)# enable
```

Displaying OSFP information

You can display OSPF information via the following commands:

- show ospf area
- show ospf debug
- show ospf general
- show ospf intf
- show ospf links
- show ospf lsdb
- show ospf neighbor

Configuring the Default Gateway

The following procedure sets the default gateway. You can add multiple default gateways.

To set the default gateway in administrator mode:

1. Enter the following at the command prompt:
   `configure ip`
2. Enter the following at the command prompt to set the default-gateway:
   `default-gateway` *`ip_address`*

Example

The following example creates the default gateway.

```
MS# configure ip
MS(config-ip)# default-gateway 128.89.1.25
```

Displaying Default Gateway Information

You can display default gateway settings via the **`show ip default-gateway`** command.

Discovering Routers

Routers can be discovered for all interfaces or the specified interface.

To discover routers in administrator mode:

1. Enter the following at the command prompt:
   `configure ip`
2. Enter the following at the command prompt to enable router discovery:
   `router-discovery` `[`**`interface`** *`interface_name`*`]`

Example

The following example creates the default gateway.

```
MS# configure ip
MS(config-ip)# router-discovery gige1/0
```

Displaying Discovered Routers

The router discovery configuration is shown via the **`show ip router-discovery`** command. Discovered routers can be viewed via the **`show ip routes`** command.

Chapter 10: IP Services

You can configure domain name service (DNS) and address resolution protocol (ARP) for the MS950. These IP services apply to the MS950 as whole, independent of subscriber service configurations.

In This Chapter

- ARP
- DNS
- MIP

Configuring ARP

ARP is used to convert an Internet address into an Ethernet address. ARP operates between the IP and data-link layers. It performs the translation between 32-bit IP addresses and 48-bit hardware addresses (MAC addresses).

Configuring ARP

The following procedure adds an entry into the ARP table of a physical interface and flushes existing cache entries.

To configure ARP in administrator mode:

1. Enter the following at the command prompt:
   ```
   configure ip
   ```
2. Enter the following at the command prompt to add an ARP entry:
   ```
   arp destination ip_address hw-address
      mac_address interface-address
      interface_address
   ```
3. Enter the following at the command prompt to flush the existing ARP cache:
   ```
   arp flush interface-address
      interface_address
   ```

4. Enter the following at the command prompt to set the ARP timeout:
   arp timeout *timeout*
5. If desired, enable ARP on the desired interface. See “Physical Interfaces” on page 8-1.

Example

The following example adds an entry to the ARP table for the 4.0.0.1 interfaces and then flushes all entries for the same interface.

```
MS# configure ip arp destination 192.168.20.1 hw-
   address 0a:02:01:00:10:bc interface-address 4.0.0.1
MS(config-ip)# arp flush interface-address 4.0.0.1
MS(config-ip)# arp timeout 11
```

Displaying ARP Information

The **show arp** command displays the ARP table.

Configuring DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet’s global naming scheme, the DNS, accomplishes this task.

By default this service is enabled, however, you must assign DNS servers and assign the MS950 a DNS name. The MS950 uses DNS to resolve hostnames to IP addresses and to reverse map IP addresses to hostnames. The MS950 uses the domain name to identify the local domain and to complete domain name requests. Any IP host name that does not contain a domain name has the specified domain name appended to it for a DNS lookup.

Configuring DNS

The following procedure assigns DNS servers and assigns the DNS name.

To configure DNS in administrator or superuser mode:

1. Enter the following at the command prompt:
   `configure ip`
2. Enter the following at the command prompt to configure primary and secondary DNS servers:
   `dns server prim_ip [sec-ip ip_address]`
3. Enter the following at the command prompt to set the domain name of the MS950:
   `dns domain [name]`
4. Enter the following at the command prompt to enable domain lookup:
   `dns domain-lookup`

Example

The following example sets the MS950 in config mode, assigns the DNS server a primary and secondary IP address, gives the MS950 a DNS name megistodns, and enables DNS.

```
MS# configure ip
MS(config-ip)# dns server 192.168.20.1 sec-ip
   192.168.20.1
MS(config-ip# dns domain megistodns
MS(config-ip)# dns domain-lookup
```

Displaying DNS Information

You can display the current DNS server configuration and name using the **`show ip dns domain`** and **`show ip dns servers`** commands. The **`whois`** command displays information about a domain.

Mobile IP

A mobile device can be connected to the Internet via wire or wireless network interface; however, due to roaming, the device may change its network attachment each time it moves to a new link. Universal Mobility functionality enables seamless transition between access networks. The Universal Mobility feature allows you to deploy value-added services such as Multimedia Messaging Service (MMS) and the IP Multimedia Subsystem (IMS).

The Mobile Internet Protocol (Mobile IP) provides a reliable mechanism for associating subscriber identity with a point of attachment in the network and does so as the subscriber moves from one network to another. Mobile IP also provides the means to establish such tunnels as IP-in-IP, IP-in-UDP (User Datagram Protocol), and GRE (Generic Routing Encapsulation) in order to allow subscriber traffic to be identified within the core network of the mobile operator.

Mobile IP enables a mobile device to change its point of attachment to the Internet while keeping an unchanging IP address called its Home IP address. It does not require changes in the existing routing infrastructure and works well for mobility across homogeneous media and heterogeneous media.

Note: Types IMSI and MSISDN are not supported for CDMA HA.

To configure Mobile IP in administrator or superuser mode:

1. Enter the following at the command prompt:
   `configure mip`
2. Enter the following at the command prompt to configure the home-agent:
   home-agent {**enable** | **disable**} [**registration-lifetime** *seconds*] [**replay** *seconds*] [**registration-flags** *values*] [**holder-timer** *hours*] [**keep-alive** *seconds*]
3. Enter the following at the command prompt to create a policy map:
   policy-map *name* [**registration-lifetime** *seconds*] [**replay** *seconds*] [**registration-flags** *values*]
4. Enter the following at the command prompt to configure subscriber information:
   subscriber-info {**type imsi** *value*| **msisdn** *value*| **nai** *value*} [**enable** | **disable**]
5. Configure the tunnel interface encapsulation to use MIP and the APN to use the mip policy map. See “Virtual Tunnel Interfaces” on page 8-6
6. Configure the APN to use the MIP policy map.
   mip-policy-map *policy_name*
7. Enable UM service.
   `um-service`

Example

The following example sets a home agent, policy-map, and subscriber information for Mobile IP. It then enables UM services.

```
MS# configure mip
MS(config-mip)# home agent enable keep-alive 32
MS(config-mip)# policy-map mippol3 registration-
   lifetime 32
MS(config-mip)# subscriber-info type imsi 12345678
MS(config-mip)# exit all
MS# configure interface tunnel 16/0.1 megisto-tunnel
MS(config-if-tun16/0.1)# ip-address 192.168.40.2
   255.255.255.0
MS(config-if-tun16/0.1)# encapsulation mip
MS(config-if-tun16/0.1)# exit all
MS# configure subscriber-partition user1
MS(config-subs)# access-point company1
MS(config-subs-apn)# mip-policy-map mippol3
MS(config-subs-apn)# um-service
```

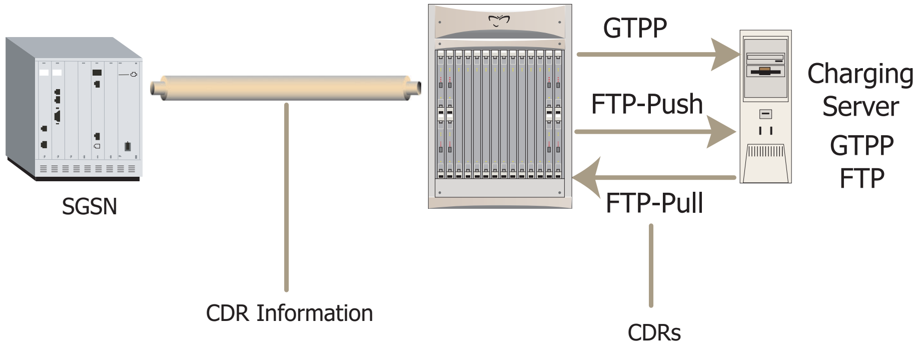
Displaying MIP Information

The following commands display information about MIP configuration:

- **`show mip globals`**
- **`show mip policy-map`**
- **`show mip context`**
- **`show mip subscriber-info`**

Chapter 11: Charging

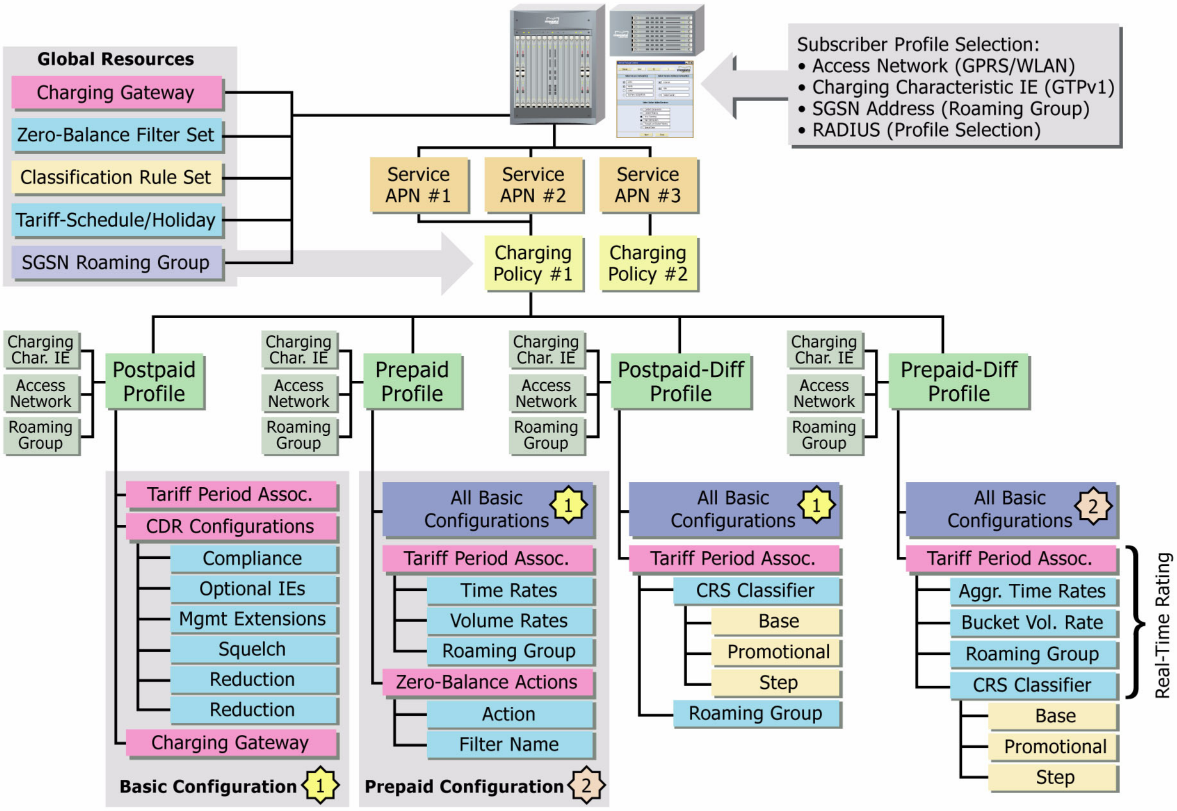
The MS950 is capable of communicating with a charging (also known as billing or accounting) server. It produces 3GPP-compliant ASN.1 charging data records (CDRs) that contain detailed subscriber information related to billing. You can configure content, event triggering, and transport of CDR data. The MS950 supports the transfer of CDRs to the server via GTPP, FTP-Push, or FTP-Pull. Only one of these transfer methods can be active at any given time. GTPP charging is modeled for 3GPP 32.015 and 32.215 as well as GSM 12.15. In addition to GTPP charging, you also can access a Remote Authentication Dial-In User Service (RADIUS) accounting server as described in “Configuring Default RADIUS Servers” on page 20-4 and “Configuring Subscriber RADIUS Addressing” on page 20-7.



In This Chapter

Charging Methods

The MS950 supports differential, prepaid, and postpaid charging methods. The configuration of general charging parameters (such as FTP-Push, FTP-Pull, GTPP, and CDRs) is applied to the selected charging method.



Prepaid charging uses a RADIUS Prepay System (RPS). Data volume is charged in the uplink and downlink directions separately. Time is charged per context. The number of credits charged varies per context, per tariff period, and per locale (that is, roaming versus local).

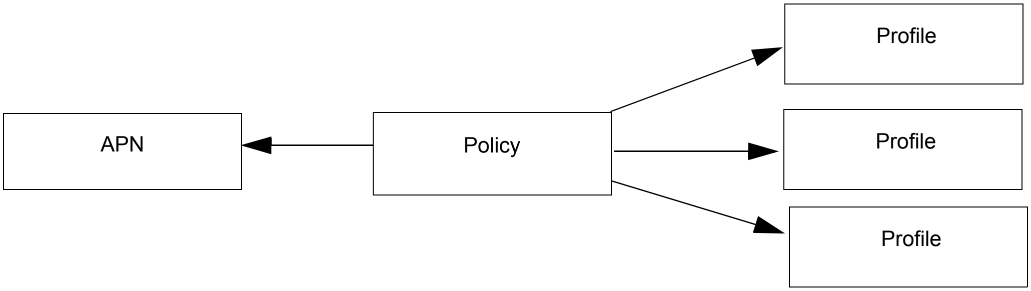
In a postpaid charging scenario, usage is reported to the telephone company that charges the subscriber. In the prepaid scenario, usage is reported to the telephone company and the ISP (and, in turn, to the RPS).

The intent of differential charging is to generate charging data for services. A packet is involved in service delivery if it matches the classification rule(s) used to define the service. There is a many-to-one relationship between service and charging bucket; many services may be aggregated into the same bucket.

All charging is configured in a similar manner: global charging attributes are created. Profiles then are created that consist of CDR specifications and rates (if desired). Policies are created that contain desired profiles and tariff schedules. Profiles are bound to policies; because policies also are bound to an APN, this configuration provides a variety of information available to a variety of APNs with a simple method of reference.

Configuring Policies

A charging policy defines the charging behavior for subscriber sessions hosted by the MS950. Any charging policy configured on the MS950 can be associated with an APN. The same policy can be used by more than one access point. The charging policy delegates charging behavior to charging profiles where the policy decisions are actually made. The charging policy is responsible for determining which profile applies to a subscriber session.



A policy designates the desired charging profile and charging unit. The policy contains a profile. Policies are bound to APNs.

To configure policies in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Enter the following at the command prompt to specify the policy name:
   `policy` *`name`*
3. If you are configuring prepaid or prepaid-differential (otherwise skip to the next step), enter the following at the command prompt to specify the charging-unit:
   ```
   charging-unit {time time_charging_unit} {uplink
      uplink_charging_unit} {downlink
      downlink_charging_unit}
   ```
4. Enter the following at the command prompt to specify the desired profiles:
   ```
   bind-profile name [charging-characteristics n | h | f
      | p | z] {roaming-group name} {access-network gprs
      | wlan | both}
   ```

Note: The profile must be created prior to calling it via this command. See “Configuring Profiles” on page 11-6.

5. Enter the following at the command prompt to specify the tariff schedule:
   `bind-schedule` *`name`*

Example

The following example sets the MS950 in charging mode and configures the charging policy.

```
MS# configure charging
MS(config-charging)# policy ppayPlanBPolicy
MS(config-charging-pol)# bind-profile wlan charging-
   characteristics n access-network wlan roaming-group
   roam1
MS(config-charging-pol)# charging-unit time 1800
   uplink 32 downlink 256
MS(config-charging-pol)# bind-tariff-schedule sched1
```

Tariff Schedules

Tariff schedules are independently created and bound to policies. The schedule defines the holiday calendar and tariff periods.

To configure tariff schedules in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Enter the following at the command prompt to create a tariff schedule:
   `tariff-schedule` *`name`*
3. Enter the following at the command prompt to specify the desired calendar:
   `bind-calendar` *`name`*
4. Enter the following at the command prompt to specify the tariff period:
   `bind-period` *`period_name`* {**`wkday`** | **`wkend1`** | **`wkend2`** | **`hol`** | **`eve`**} **`start-time`** *`start_time`* **`end-time`** *`end_time`*
5. Enter the following at the command prompt to specify the start day for weekend rates:
   `weekend-start` {**`fri`** | **`sat`**}

Example

The following example sets the MS950 in charging mode and configures the charging policy.

```
MS# configure charging
MS(config-charging)# bind-schedule sched1
MS(config-charging-tar)# bind-calendar hol1
MS(config-charging-tar)# weekend-start fri
MS(config-charging-tar)# period wkdayNight wkday
   start-time 00:00 end-time 07:59
```

Holiday Calendars

Holiday calendars specify the days on which to apply holiday rates. The name of the calendar is referenced in the tariff schedule.

To configure holiday calendars in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Enter the following at the command prompt to specify the policy name:
   `holiday-calendar` *`name`*
3. Enter the following at the command prompt to specify holiday eves:
   `eve` *`{MM/DD}`*
4. Enter the following at the command prompt to specify holidays:
   `hol` *`{MM/DD}`*

Example

The following example sets the MS950 in charging mode and configures the charging policy.

```
MS# configure charging
MS(config-charging)# holiday-calendar cal1
MS(config-charging-cal)# eve 12/24
MS(config-charging-cal)# hol 12/25
```

Configuring Profiles

Profiles contain detailed information about CDR generation, charging periods, and rates. The profiles are then bound to a policy, which, in turn, is bound to the APN. Four kinds of profiles are supported; a 3GPP Release 4–compliant postpaid charging profile, and Megisto proprietary prepaid, differential, and prepaid plus differential profiles.

CDRs contain subscriber usage data that may be used for billing. If GTPP is currently being used for data transfer, then CDRs are transferred directly to the server without being stored in a file. If FTP-Push or FTP-Pull is being used, then the CDRs are stored in files in the **`system:/cdr`** directory by default.

To configure profiles in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:

```
configure charging
```

2. Enter the following at the command prompt to create the profile:
   ```
   profile name post | prepay | differential | prepay-
      differential]
   ```
3. If you are configuring prepaid or prepaid-differential (otherwise skip to the next step), enter the following at the command prompt to determine a prepay zero balance action:
   ```
   prepay-zero-balance-action terminate | discard |
      filter | continue [filter name] [poll-interval
      seconds] [retries number]
   ```
4. Enter the following at the command prompt to specify CDRs settings:
   ```
   cdr
   ```
5. Configure the desired CDR settings as described in “CDRs” on page 11-8.
6. Enter the following at the command prompt to move back to the profile level:
   ```
   exit
   ```
7. Enter the following at the command prompt to specify period settings:
   ```
   bind-period
   ```
8. Configure the desired period settings as described in “Bind Periods” on page 11-10.

Example

The following example sets the MS950 in charging mode and configures a charging profile.

```
MS# configure charging
MS(config-charging)# profile prof1 prepay
MS(config-charging-pro)# prepay-zero-balance-action
   filter filter-name zbf1 poll-interval 180 retries 3
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# closure-thresh volume
   64000 time-limit 200 sgsn-limit 3 container-limit 4
MS(config-charging-pro-cdr)# compliance rel4 root-tag
   173
MS(config-charging-pro-cdr)# ftp-transport
MS(config-charging-pro-cdr)# optional-extensions
   policy-id on profile-id on
```

```
MS(config-charging-pro-cdr)# optional-ies msisdn on
   apn-selection-mode on node-id on local-sequence-
   number off
MS(config-charging-pro-cdr)# charging-gateway cg1
   priority 1
MS(config-charging-pro-cdr)# reduction
MS(config-charging-pro-cdr)# squelch
MS(config-charging-pro-cdr)# exit
MS(config-charging-pro)# bind-period wkdaypeak
MS(config-charging-pro-per)# time-rate rate 0 roaming-
   group slagroup5
MS(config-charging-pro-per)# volume-rate bucket 0
   uplink-rate 0 downlink-rate 0 roaming-group
   slagroup5
```

CDRs

To configure CDRs in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Enter the following at the command prompt to create the profile:
   profile *name* **post** | **prepay** | **differential** | **prepay-differential**]
3. Enter the following at the command prompt to specify CDRs settings:
   cdr
4. Enter the following at the command prompt to specify the thresholds to close CDRs and start transfer to the charging gateway:
   closure-thresh [**volume** *volume*] [**time-limit** *limit*] [**sgsn-limit** *limit*] [**container-limit** *limit*]
5. Enter the following at the command prompt to specify the ASN.1 root-tag and specification compliance:
   compliance rel97 | **rel99** | **rel14 [root-tag** *tag_number*]
6. If desired, enter the following at the command prompt to enable FTP for the profile:
   ftp-transport

Note: FTP-Push or FTP-Pull must be configured prior to enabling its use in the profile.

7. Enter the following at the command prompt to specify optional CDR information elements:

   ```
   options [msisdn on | off] [apn-selection-mode on |
      off] [node-id on | off] [local-sequence-number on |
      off]
   ```

8. Enter the following at the command prompt to specify optional CDR information elements:

   ```
   optional-extensions [policy-name on | off] [profile-
      name on | off] [access-network on | off] [roaming-
      group on | off] [nai on | off] [promotion-id on |
      off] [step-number on | off] [qos-negotiated on |
      off]
   ```

9. Enter the following at the command prompt to specify optional CDR information elements:

   ```
   optional-ies [network-initiated on | off] [apn on |
      off] [pdp-type on | off] [pdp-address on | off]
      [dynamic-address-flag on | off] [volume-list on |
      off] [diagnostics on | off] [extensions on | off]
      [msisdn on | off] [apn-selection-mode on | off]
      [node-id on | off] [local-sequence-number on | off]
      [charging-char-selection-mode on | off]
   ```

10. Enter the following at the command prompt to specify a RADIUS charging gateway:

    ```
    charging-gateway name priority priority
    ```

Note: Classification rules and rule sets must be configured prior to calling this command.

11. Enter the following at the command prompt to enable reduced-partial CDRs:

    ```
    reduction
    ```

12. Enter the following at the command prompt to enable squelching of reduced-partial CDRs:

    ```
    squelch
    ```

13. Enter the following at the command prompt move out of profile configuration:

    ```
    exit all
    ```

14. Enter the following at the command prompt move back into charging:

    ```
    configure charging
    ```

15. Enter the following at the command prompt to specify MS950 node identification used for charging (not at the profile):

    ```
    node {id string} {mcc number} {mnc number}
    ```

Note: The node ID can be the same as the DNS name for the MS950 but may contain a separate identifier.

Example

The following example sets the MS950 in charging mode and configures a charging profile.

```
MS# configure charging
MS(config-charging)# profile prof1 prepay
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# closure-thresh volume
   64000 time-limit 200 sgsn-limit 3 container-limit 4
MS(config-charging-pro-cdr)# compliance rel4 root-tag
   173
MS(config-charging-pro-cdr)# ftp-transport
MS(config-charging-pro-cdr)# generation gtpp
MS(config-charging-pro-cdr)# optional-extensions
   policy-id on profile-id on
MS(config-charging-pro-cdr)# optional-ies msisdn on
   apn-selection-mode on node-id on local-sequence-
   number off
MS(config-charging-pro-cdr)# charging-gateway cg1
   priority 1
MS(config-charging-pro-cdr)# reduction
MS(config-charging-pro-cdr)# squelch
MS(config-charging-pro-cdr)# exit all
MS# configure charging
MS(config-charging)# exit all
MS(config-charging)# node id www.megisto.com mcc 234
   mnc 456
```

Bind Periods

To configure periods in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Enter the following at the command prompt to create the profile:

```
profile name post | prepay | differential | prepay-
   differential]
```

3. Enter the following at the command prompt to create the period:

   ```
   bind-period name
   ```

4. If you are configuring prepaid or prepaid-differential (otherwise skip to the next step), enter the following at the command prompt to specify the time rate:

   ```
   time-rate time_rate {roaming-group group}
   ```

5. If you are configuring prepaid or prepaid-differential (otherwise skip to the next step), enter the following at the command prompt to specify volume rates:

   ```
   volume-rate bucket name {uplink uplink_rate} {downlink
      downlink_rate} {roaming-group group}
   ```

6. If you are configuring differential or prepaid-differential (otherwise skip to to the next step), enter the following at the command prompt to specify volume rates:

   ```
   classifier base base [step step] [promotion promotion]
   ```

Example

The following example sets the MS950 in charging mode and configures a charging profile.

```
MS# configure charging
MS(config-charging)# profile diff1
MS(config-charging-pro)# bind-period wkdaypeak
MS(config-charging-pro-per)# time-rate rate 0 roaming-
   group slagroup5
MS(config-charging-pro-per)# volume-rate bucket 0
   uplink-rate 0 downlink-rate 0 roaming-group
   slagroup5
MS(config-charging-pro-cdr)# classifier base crs1 step
   step0 promotion promo1
```

Charging Rules

Charging classification rules are used only for differential billing. The prepaid zero balance actions rules apply only to prepaid billing. Both are created at the charging level and then referenced in profiles.

To configure charging rules in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Enter the following at the command prompt to create specify charging packet classification rules:
   classification-rule *name* [**ip-address** *address*] [**netmask** *address*] [**protocol tcp** | **udp** | **icmp**] [**tos** *tos*] [**port** *port*]
3. Enter the following at the command prompt to create specify charging packet classification rule sets:
   classification-rule-set *name* {**id** *id*} [**type base** | **step** | **promotion**]
4. Enter the following at the command prompt to create specify charging packet classification rule sets:
   rule *name* {**bucket** *number*} [**index** *number*]
5. Enter the following at the command prompt to exit rule-set mode:
   exit
6. Enter the following at the command prompt to create specify zero balance actions:
   zero-balance-filter *name*
7. Enter the following at the command prompt to specify zero balance filter rules:
   allow id *id* [**ip-address** *ip_address*] [**netmask** *netmask*] [**protocol tcp** | **udp** | **icmp**] [**port** *port*]

Example

The following example sets the MS950 in charging mode and configures a charging profile.

```
MS# configure charging
MS(config-charging)# classification-rule name rule1
   ip-address 10.0.0.0 netmask 255.0.0.0
MS(config-charging)# classification-rule-set name crs1
   id 37 type base
MS(config-charging-crs)# rule rul5 bucket 5 index 17
MS(config-charging-crs)# exit
MS(config-charging)# zero-balance-filter zbf1
MS(config-charging-filter)# allow id 1 ip-address
   10.0.0.0 netmask 255.0.0.0
```

Differential Charging

Differential charging is postpaid charging plus classification rules. Charging classification rules determine the packet classification that is used to define, and to charge for, subscriber services. It specifies the initial conditions for instantiating a charging profile for a subscriber, and for changing the profile because of a change in access network, roaming state, tariff period, step charging level (usage crosses the step charging threshold), or policy. Prepaid plus differential incorporates all the prepaid and differential charging commands.

To configure differential charging options:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Configure charging rules as specified in “Charging Rules” on page 11-11.

   A classification rule and rule set must be configured. If this charging definition is prepaid plus differential, then you also must configure a zero-balance filter.
3. Configure a profile as specified in “Configuring Profiles” on page 11-6.

   The profile must contain a period with a classifier. If this charging definition is prepaid plus differential, then you also must configure the prepay zero balance action, time rate, and volume rate.
4. Configure the charging policy as specified in “Configuring Policies” on page 11-3.

   If this charging definition is prepaid plus differential, then you also must configure the charging unit.
5. Configure the APN to use the differential or prepaid plus differential charging policy. See “Creating Subscriber Partitions” on page 19-1.

Example

The following example configures prepaid plus differential charging.

```
MS# configure charging
MS(config-charging)# classification-rule name rule1
   ip-address 10.0.0.0 netmask 255.0.0.0
MS(config-charging)# classification-rule-set name crs1
   id 37 type base
MS(config-charging-crs)# rule rul5 bucket 5 index 17
MS(config-charging-crs)# exit
MS(config-charging)# zero-balance-filter zbf1
MS(config-charging-filter)# allow id 1 ip-address
   10.0.0.0 netmask 255.0.0.0
MS(config-charging)# profile prof1 prepay-diff
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# closure-thresh volume
   64000 time-limit 200 sgsn-limit 3 container-limit 4
MS(config-charging-pro-cdr)# compliance rel4 root-tag
   173
MS(config-charging-pro-cdr)# optional-extensions
   policy-id on profile-id on
MS(config-charging-pro-cdr)# optional-ies msisdn on
   apn-selection-mode on node-id on local-sequence-
   number off
MS(config-charging-pro-cdr)# charging-gateway cg1
   priority 1
MS(config-charging-pro-cdr)# classifier base crs1 step
   step0 promotion promo1
MS(config-charging-pro-cdr)# reduction
MS(config-charging-pro-cdr)# squelch
MS(config-charging-pro)# exit
MS(config-charging-pro)# bind-period wkdaypeak
MS(config-charging-pro-per)# time-rate rate 0 roaming-
   group slagroup5
MS(config-charging-pro-per)# volume-rate bucket 0
   uplink-rate 0 downlink-rate 0 roaming-group
   slagroup5
MS(config-charging-pro-per)# classifier base crs1 step
   step0 promotion promo1
MS(config-charging-pro-per)# exit
MS(config-charging-pro)# prepay-zero-balance-action
   filter filter-name zbf1 poll-interval 180 retries 3
MS(config-charging-pro)# exit
MS(config-charging)# holiday-calendar cal1
MS(config-charging-cal)# eve 12/24
MS(config-charging-cal)# hol 12/25
MS(config-charging)# policy ppayPlanBPolicy
MS(config-charging-pol)# tariff-schedule sched1
MS(config-charging-pol-tar)# bind-calendar hol1
MS(config-charging-pol-tar)# weekend-start fri
MS(config-charging-pol-tar)# bind-period wkdayNight
   wkday start-time 00:00 end-time 07:59
MS(config-charging-pol-tar)# exit
MS(config-charging-pol)# bind-profile prof1 access-
   network wlan
MS(config-charging-pol)# charging-unit time 1800
   uplink 32 downlink 256
MS(config-charging-pol)# bind-schedule sched1
MS(config-charging-pol)# exit all
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# charging-policy ppaydiffBPolicy
```

Configuring Prepaid Charging

Prepaid charging relies on RPS (along with RADIUS configuration) and is specific to an APN. The prepaid charging configuration is performed, and then the policy is bound to an APN. RPS is configured at the APN.

For prepaid service, the MS950 performs real-time session control and real-time tracking of bearer usage, applying customized charging policies to each session. The MS950 contains an optional extension shelf (MS950-ES) for application-aware charging for an array of applications and additional intelligent features.

To configure prepaid charging:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Configure Charging rules as specified in “Charging Rules” on page 11-11 for the zero-balance filter.
3. Configure a profile as specified in “Configuring Profiles” on page 11-6.

   The profile must contain a period with prepaid zero balance action, time rate, and volume rate.

4. Configure the charging policy as specified in “Configuring Policies” on page 11-3.

   You must configure the charging unit for prepaid charging.

5. Configure the APN to use the differential or prepaid plus differential charging policy and the **rps** command. See “RADIUS” on page 11-21.

Note: RADIUS must be configured for prepaid charging.

Example

The following example configures prepaid plus differential charging.

```
MS# configure charging
MS(config-charging)# zero-balance-filter zbf1
MS(config-charging-filter)# allow id 1 ip-address
   10.0.0.0 netmask 255.0.0.0
MS(config-charging)# profile prof2 prepay
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# closure-thresh volume
   64000 time-limit 200 sgsn-limit 3 container-limit 4
MS(config-charging-pro-cdr)# compliance rel4 root-tag
   173
MS(config-charging-pro-cdr)# generation radius
MS(config-charging-pro-cdr)# optional-extensions
   policy-id on profile-id on
MS(config-charging-pro-cdr)# optional-ies msisdn on
   apn-selection-mode on node-id on local-sequence-
   number off
MS(config-charging-pro-cdr)# charging-gateway cg1
   priority 1
MS(config-charging-pro-cdr)# reduction
MS(config-charging-pro-cdr)# squelch
MS(config-charging-pro)# exit
MS(config-charging-pro)# bind-period wkdaypeak
MS(config-charging-pro-per)# time-rate rate 0 roaming-
   group slagroup5
MS(config-charging-pro-per)# volume-rate bucket 0
   uplink-rate 0 downlink-rate 0 roaming-group
   slagroup5
MS(config-charging-pro-per)# exit
MS(config-charging-pro)# prepay-zero-balance-action
   filter filter-name zbf1 poll-interval 180 retries 3
MS(config-charging-pro)# exit
MS(config-charging)# holiday-calendar cal1
MS(config-charging-cal)# eve 12/24
MS(config-charging-cal)# hol 12/25
MS(config-charging)# policy prepay1
MS(config-charging-pol)# tariff-schedule sched1
MS(config-charging-pol-tar)# bind-calendar hol1
MS(config-charging-pol-tar)# weekend-start fri
MS(config-charging-pol-tar)# bind-period wkdayNight
   wkday start-time 00:00 end-time 07:59
MS(config-charging-pol-tar)# exit
MS(config-charging-pol)# bind-profile prof2 access-
   network wlan
MS(config-charging-pol)# charging-unit time 1800
   uplink 32 downlink 256
MS(config-charging-pol)# bind-schedule sched1
MS(config-charging-pol)# exit all
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# charging-policy prepay1
```

Note: Because prepaid billing utilizes RADIUS, the **radius-server**, **rps**, and **radius-service** commands must be configured either globally or for the specific APN.

Note: For data coming through SGSNs that have been configured via the **sgsn** command, local rates apply because the SGSN is considered part of the local network. If data comes through an SGSN outside the network, then roaming rates apply.

Configuring Postpaid Charging

Postpaid charging relies only on the charging mode selected (FTP-Push, FTP-Pull, or GTPP) and is specific to an APN. The postpaid charging configuration is performed, and then the policy is bound to an APN.

To configure postpaid charging:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Configure a profile as specified in “Configuring Profiles” on page 11-6.

The profile must contain no period because period parameters do not apply to postpaid.

3. Configure the charging policy as specified in “Configuring Policies” on page 11-3.
4. Configure the APN to use the differential or prepaid plus differential charging policy. See “Creating Subscriber Partitions” on page 19-1.

Example

The following example configures postpaid plus differential charging.

```
MS# configure charging
MS(config-charging)# profile prof3 postpaid
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# closure-thresh volume
   64000 time-limit 200 sgsn-limit 3 container-limit 4
MS(config-charging-pro-cdr)# compliance rel4 root-tag
   173
MS(config-charging-pro-cdr)# ftp-transport
MS(config-charging-pro-cdr)# generation gtpp
MS(config-charging-pro-cdr)# optional-extensions
   policy-id on profile-id on
MS(config-charging-pro-cdr)# optional-ies msisdn on
   apn-selection-mode on node-id on local-sequence-
   number off
MS(config-charging-pro-cdr)# charging-gateway cg1
   priority 1
MS(config-charging-pro-cdr)# reduction
MS(config-charging-pro-cdr)# squelch
MS(config-charging-pro)# exit
MS(config-charging)# holiday-calendar cal1
MS(config-charging-cal)# eve 12/24
MS(config-charging-cal)# hol 12/25
MS(config-charging)# policy postpay1
MS(config-charging-pol)# tariff-schedule sched1
MS(config-charging-pol-tar)# bind-calendar hol1
MS(config-charging-pol-tar)# weekend-start fri
MS(config-charging-pol-tar)# bind-period wkdayNight
   wkday start-time 00:00 end-time 07:59
MS(config-charging-pol-tar)# exit
MS(config-charging-pol)# bind-profile prof2 access-
   network wlan
```

```
MS(config-charging-pol)# bind-schedule sched1
MS(config-charging-pol)# exit all
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# charging-policy postpay1
```

Configuring Charging Transport

You can transport charging information via GTPP, FTP, or RADIUS.

GTPP

GTPP configuration is used when the GTPP protocol is to transport CDRs from the MS950 to the charging gateway. You can specify the GTPP charging gateway to be used for subscriber billing as well as the way that the MS950 communicates with that gateway. GTPP is typically used for postpaid and differential billing.

To configure GTPP charging in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Configure CDR Parameters as described in “CDRs” on page 11-8.
3. Enter the following at the command prompt to specify a the GTPP gateway:
   ```
   gateway name ip-address ip_address [port port]
      [timeout seconds] [retransmit times] [path-echo-
      interval seconds] [path-retransmit retries]
   ```

Example

The following example sets the MS950 in config mode, designates a charging gateway, specifies charging data transfer parameters, and enables GTPP transfer mode.

```
MS# configure charging
MS(config-charging)# gateway charge1 ip-address
   128.89.0.112 port 5001
```

FTP-Push

In FTP-Push mode, charging records are pushed from the MS950 to the the FTP charging server. FTP is typically used for postpaid and differential billing.

To configure FTP-Push transport in administrator or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   ```
   configure charging
   ```
2. Configure CDR Parameters as described in “CDRs” on page 11-8, making sure to enable FTP transport.
3. Enter the following at the command prompt to designate to FTP-Push information:
   ```
   ftp-push {ip ip_address} {dest-dir dir_name} {user
      user_name} {password password} [file-size bytes]
      {dir-size bytes] [push-interval minutes] [retry-
      interval seconds] [retransmit retries] [secondary]
      [source-dir dir_name]
   ```
4. Enter the following at the command prompt to enable Push mode:
   ```
   ftp-mode push
   ```

Example

The following example sets the MS950 in charging mode, creates an FTP user, and pushes FTP data for that user.

```
MS# configure
MS(config)# charging
MS(config-charging)# ftp-push ip 192.168.20.34 dest-
   dir /home/iv/cdr user iv password iv push-interval
   1 file-size 1000 dir-size 100000
MS(config-charging)# ftp-mode push
MS(config-charging)# profile prof3 postpaid
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# ftp-transport
```

FTP-Pull

In FTP-Pull mode, charging records are pulled from the MS950 by an FTP client. The log file that contains the information to pull has the naming convention 00000001.log to 99999999.log and is located in the directory **`system:/cdr`**. The current open file is named **`nnnnnnnn.tmp`**. FTP is typically used for postpaid and differential billing.

To configure FTP-Pull client transport information in admin or superuser mode:

1. Enter the following at the command prompt to enter charging configuration commands:
   ```
   configure charging
   ```
2. Configure CDR Parameters as described in “CDRs” on page 11-8, making sure to enable FTP-transport.
3. Enter the following at the command prompt to designate to push or pull FTP information:
   ```
   ftp-pull {source-dir dir_name} [file-size bytes] {dir-
      size bytes] [pull-interval minutes]
   ```
4. Enter the following at the command prompt to enable Push mode:
   ```
   ftp-mode push
   ```

Example

The following example sets the MS950 in charging mode, creates an FTP user, and pushes FTP data for that user.

```
MS# configure
MS(config)# charging
MS(config-charging)# ftp-pull source-dir system:/cdr
MS(config-charging)# ftp-mode pull
MS(config-charging)# profile prof3 postpaid
MS(config-charging-pro)# cdr
MS(config-charging-pro-cdr)# ftp-transport
```

RADIUS

RADIUS is the transport mechanism for all prepaid billing. RADIUS configuration can be done globally or at the APN. See “Configuring

Default RADIUS Servers" on page 20-4 or "Configuring Subscriber RADIUS Addressing" on page 20-7. In either case, the **rps** command must be configured to enable RADIUS billing.

To configure RADIUS transport in admin or superuser mode:

1. Configure RADIUS subscriber addressing as described in "Configuring Subscriber RADIUS Addressing" on page 20-7,
2. Create the subscriber partition as shown in "Creating Subscriber Partitions" on page 19-1.
3. Enter the following at the command prompt to configure the prepaid server.

```
rps [credit-reservation-timeout timeout] [default-
   interim interval] [low-credit-threshold balance]
```

Example

The following example configures RADIUS charging transport at the APN.

```
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# address-method radius
MS(config-subs-apn)# radius-server auth ip
   192.168.10.10 name funk key funky
MS(config-subs-apn)# radius-service auth
MS(config-subs-apn)# subscriber address-pool
   192.234.40.0 255.255.255.0 service-card 5
MS(config-subs-apn)# generic-user-info name johnh
   password secret
MS(config-subs-apn)# rps credit-reservation-timeout
   1800 default-interim 600 low-credit-threshold 100
```

Displaying Charging Parameters

You can display information about the current charging configuration via the following show commands:

- show charging-gateway
- show charging classification-rule

- show charging classification-rule-xref
- show charging classifier
- show charging ftp
- show charging holiday-calendar
- show charging policy
- show charging prepay rates
- show charging statistics
- show charging tariff schedules
- show charging unit
- show charging zero-balance-filter

Configuring Access Locations

You may designate which access locations are to be considered the local network or external network. A maximum of 20 SGSN or COA addresses can be configured to identify which subscribers are roaming. With regard to charging, calls through access-location in the local network are applied local rates while calls through access locations outside the local network are applied roaming rates.

To configure access locations in administrator or superuser mode:

1. Enter the following at the command prompt to enter configuration mode:
   configure
2. Enter the following at the command prompt to enter the SGSN address:
   access-location ip *ip_address* **mask** *netmask* **roaming-group** *roaming-group* [**type sgsn** | **coa**]

Example

The following example places the listed SGSN in the local network.

```
MS# configure charging
MS(config-charging)# access-location ip-address
   122.134.94.6 mask 255.255.255.255 type sgsn
   roaming-group slagroup5
```

Displaying Configured SGSNs

You can display configured SGSNs via the **`show sgsn`** command.

Chapter 12: Advanced Charging

The MS950-ES Expansion Shelf is a flexible expansion shelf for Megisto's MS950 platform that provides for the direct addition of both customized and third-party applications to the MS950 control and data planes. These applications include:

- Multimedia Messaging Service (MMS)
- Wireless Access Protocol (WAP)
- comprehensive billing
- carrier-grade scalability and resiliency

The Expansion shelf enhances the charging capabilities provided in the basic MS950 configuration. The MS950-ES is completely configurable via the MS950 CLI. This chapter describes only the charging features available in the MS950-ES. These features are available for differential billing. It is important to note that charging configuration in the previous chapter must be performed prior to or at the same time as ES configuration. The same command mode structures are need for some commands and some commands require additional modes.

In This Chapter

Configuring the ASE Blade

The heart of the MS950-ES is the ES-950-ASE Application Services Engine, a board that provides powerful, value-added services processing, including Layer 7 content and event-level charging.

The ase-node command configures the IP address and name for the ASE blade so that the MS950 can communicate with the MS950-ES.

To configure an ASE blade on the ES:

1. Enter the following command at the prompt:
   ```
   ase-node [ip-address address] id idname [i2r-ip-
      address address]
   ```
2. Enter the following command at the prompt:
   ```
   ase-load-balancer [r2i-vlan name] [i2r-vlan name]
   ```

Example

The following example configures the ASE blade.

```
MS# configure ase-node 192.168.51.1 workhorse
MS(config)# ase-load-balancer r2i-vlan vlan1 i2r-vlan
   vlan2
```

URI Content Charging

You can create content-based classification charging rules based on URI packet data. These rules isolate URI data and pass along charging information based on your specifications.

To configure URI content:

1. Enter the following at the command prompt to enter charging configuration commands:
   ```
   configure charging
   ```
2. Enter the following command at the prompt to create a URI set:
   ```
   uri-set uri-set-name [onnet]
   ```
3. Enter the following at the command prompt to add a URI to the set:
   ```
   uri name
   ```
4. Enter the following at the command prompt to add a URI shortcut to the set:
   ```
   shortcut uri_name
   ```
5. Enter the following at the command prompt to add a map of shortcut names to fully qualified or wildcarded URIs:
   ```
   uri-shortcut [shortcut-name] [uri]
   ```

6. Enter the following at the command prompt to create a URI policy
   ```
   uri-policy uri-policy-name
   ```
7. Enter the following at the command prompt to set default prepay rates for URI browsing;
   ```
   browse-default [credits | kilobyte]
   ```
8. Enter the following at the command prompt to configure volume-based charging for the specified URI-set:
   ```
   browse uri-set-name [credits | kilobyte]
   ```
9. Enter the following at the command prompt to configure event-based charging for URIs:
   ```
   event uri-set-name {credits | HTTP GET} [bearer-chg-
      failure]
   ```
10. Enter the following at the command prompt to specify the charging policy name:
    ```
    policy name
    ```
11. Enter the following at the command prompt to specify off URI redirection:
    ```
    recharge-portal [uri]
    ```
12. Enter the following at the command prompt to specify the interim for ase-accounting:
    ```
    ase-acct-interim [interval]
    ```
13. Enter the following at the command prompt to bind the URI settings to a profile:
    ```
    app-rates [roaming-group | default] [mms-policy] [uri-
       policy] [bearer_rate rate][default-tariff-period]
    ```

Example

The following example configures URI charging parameters.

```
MS# configure charging
MS(config-charging)# uri-set myUris onnet
MS(config-charging-uriset)# uri http://www.cnn.com/
   weather*
MS(config-charging-uriset)# uri-shortcut cnn
MS(config-charging-uriset)# exit
MS(config-charging)# uri-shortcut picassoLaVie http://
   www.clevelandart.org/museum/collect/highlights/
   high26.html
MS(config-charging)# uri-policy bronzePol
MS(config-charging-uripol)# browse-default 10
```

```
MS(config-charging-uripol)# browse redSet 1
MS(config-charging-uripol)# browse blueSet 10
MS(config-charging-uripol)# event littleSet 10
MS(config-charging-uripol)# event mediumSet 20
MS# configure charging policy goldPro
MS(config-charging-pol)# recharge-portal www.mobo.com/
   portal
MS(config-chg-pol)# ase-acct-interim 7200
MS(config-charging-pol)# exit
MS(config-charging)# profile goldPro period wkdayEve
MS(config-chg-pro-per)# app-rates roaming-group rmGrp0
   myMmsRates myUriRates bearer-rate 1
```

MMS Content Charging

You can create content-based classification charging rules based on MMS packet data. These rules isolate MMS data and pass along charging information based on your specifications.

To configure MMS content:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Enter the following command at the prompt to create an MMS rule:
   mms-address-prefix {**type** [**PLMN** | **SMTP** | **IPv4** | **ANY**]} [**prefix** [**PLMN prefix** | **Subnet** |**masklen**]] [**address-category** *category-name*]
3. Enter the following at the command prompt to add a URI to the set:
   uri *name*
4. Enter the following at the command prompt to add a URI shortcut to the set:
   shortcut *uri_name*
5. Enter the following at the command prompt to add a map of shortcut names to fully qualified or wildcarded URIs:
   uri-shortcut [*shortcut-name*] [*uri*]
6. Enter the following at the command prompt to create a MMS policy
   mms-policy *mms-policy-name*
7. Enter the following at the command prompt to configure slab or tier rating for MM based on size and content type:

```
mms-rate [type [slab | tier]] [direction [send |
   recieve]][content-type [text | image | audio |
   video | mixed | any]] [max-size sz] [credits cr]
   [address-category cname] [content-tag name]
```

8. Enter the following at the command prompt to obtain credit for each MM send:

   ```
   authorize-mm-charges
   ```

9. Enter the following at the command prompt to itemize MM recipient charges in RADIUS request messages:

   ```
   itemize-mm--recipient-charges
   ```

10. Enter the following at the command prompt to specify the aggregate content type:

    ```
    mm-aggregate-content tag_name [text | image | video |
       audio]
    ```

11. Enter the following at the command prompt :

    ```
    flagfall-charge [credits] [direction send| receive]
    ```

12. Enter the following at the command prompt :

    ```
    fixed-charge [credits] [direction send| receive]
    ```

13. Enter the following at the command prompt to bind the URI settings to a profile:

    ```
    app-rates [roaming-group | default] [mms-policy] [uri-
       policy] [bearer_rate rate][default-tariff-period]
    ```

Example

The following example configures MMS charging parameters.

```
MS# configure charging
MS(config-charging)# uri-set myUris onnet
MS(config-charging)# mms-address-prefix type PLMN
   prefix 6012 address-category local
MS(config-charging)# mms-address-prefix type PLMN
   prefix 6017 address-category local
MS(config-charging)# mms-address-prefix type PLMN
   prefix 60 address-category interop
MS(config-charging)# mms-policy bronzeMmsPol
MS(config-chg-mmspol)# mms-rate type slab direction
   send content-type any max-size 30 credits 30
   address-category local
MS(config-charging-mmspol)# authorize-mm-charges
```

```
MS(config-charging-mmspol)# itemize-mm-recipient-
   charges
MS(config-charging-mmspol)# mm-aggregate-content
   content1 image

MS(config-charging-mmspol)# exit
MS(config-chg-mmspol)# flagfall-charge 10000
MS(config-chg-mmspol)# fixed-charge 10000
MS(config-charging)# profile goldPro period wkdayEve
MS(config-chg-pro-per)# app-rates roaming-group rmGrp0
   myMmsRates myUriRates bearer-rate 1
```

Blocking Offnet Traffic

You can block IP traffic to off-net destinations. When off-net access is attempted, a control message is sent to the RADIUS accounting server that handles the user's accounting-request messages.

To block offnet traffic:

1. Enter the following at the command prompt to enter charging configuration commands:
   `configure charging`
2. Enter the following command at the prompt to block offnet traffic:
   `block-offnet`

Example

The following example blocks offnet traffic.

```
MS# configure charging profile goldPro
MS(config-charging-pro)# block-offnet
```

Step Charging and Promotions

Step charging specifies that at a particular interval there is an increase in charge. You can have dynamic tariff adjustment based on the subscriber’s time or volume usage. The tariff changes dynamically after a pre-defined threshold, which can be based on volume or time (e.g., volume receives a discount for traffic sent after the first 1 Mb of data usage, or usage receives a discount of 25 percent after the first hour). The system tracks usage and compares it with the specified threshold. When the threshold is reached, the tariff is switched.

Promotions specify a charge for a limited period of time. You can have dynamic tariff adjustment based on rewarding the subscriber with discounts or other charging incentives based on a desired activity. Similar to a step charge the system changes the tariff based on the specified promotion which overrides all other metering charging rules. For example, an operator might offer a day of free access to premium content services to subscribers that make online purchases.

Both step charging and promotions apply to prepaid and differential charging.

To set promotions or step charging:

1. Enter the following at the command prompt to enter charging configuration commands:
   configure charging
2. Enter the following at the command prompt to create the profile:
   profile *name* **post** | **prepay** | **differential** | **prepay-differential**]
3. Enter the following at the command prompt to specify period settings:
   bind-period
4. Enter the following at the command prompt to bind the step and/or promotion settings to a period:
   promo-time-rate [**rate** *rate*] [**roaming-group** *name*]
   step-time-rate [**rate** *rate*] [**roaming-group** *name*]

Example

```
MS# configure charging
MS(config-charging)# profile goldPro period wkdayEve
MS(config-charging-pro-per)# promo-time-rate rate 0
   roaming-group slaGroup5
MS(config-charging-pro-per)# step-time-rate rate 0
   roaming-group slaGroup5
```

Displaying Advanced Charging Parameters

You can display information about the current charging configuration via the following show commands:

- show charging mms-address-prefix
- show charging mms-policy
- show charging uri-policy
- show charging uri-set
- show charging uri-shortcut
- show charging wap-gateway

Chapter 13: Network Security

The MS950 provides all the security features expected of a GGSN as well as increased security capability. The MS950 provides secure data access via access lists and secure operator access via SSH. Specific subscriber security features are discussed in “Subscriber Security” on page 21-1.

In This Chapter

- Access Lists
- SSH

Creating Access Lists

IP access control lists (ACLs) filter traffic by controlling whether packets are forwarded or dropped on a particular interface. Each packet is examined against the filter rules that are configured in the access list.

Filter rules can be based on the IP source address, IP destination address, IP protocol, and for TCP or UDP packets, the source and destination ports.

The order that rules are added to access lists is significant. Packets are evaluated against the rules in the order that the rules were entered. Each packet is checked against each rule, in order, until a match is found. At that point, the associated action (permit or deny) is applied and no further filters are evaluated.

Access lists can be applied to physical (gigethernet or fastethernet) interfaces for either incoming or outgoing traffic. Only one access list can be applied per interface per direction.

Note: Access lists have an implicit "deny all" rule at the end of each list. You must keep in mind that, if you have set rules to deny only certain types of traffic, but you expect all other traffic to pass, then you should add a rule at the end of the list to explicitly allow traffic.

To configure global access lists in administrator or superuser mode:

1. Enter the following at the command prompt to configure an access list:
   ```
   access-list access_list_name src-ip number [src-mask
      netmask] dest-ip number [dest-mask netmask]
      protocol protocol sport number dport number {action
      deny | permit}
   ```
2. Bind the access list to Gigabit Ethernet interfaces via the `access-group` command. See "Gigabit Ethernet Interfaces" on page 8-1.

Access lists can also be used for subscriber security as described in "Configuring IPSec" on page 21-1.

Example

The following example creates an access list that denies traffic only from a particular network. The second rule is needed to allow any traffic not coming from the stopbadguys network to pass through. The access list is then bound to an interface.

```
MS# configure access-list stopbadguys src-ip
   192.168.20.0 src-mask 255.255.255.0 dest-ip *
   protocol * sport * dport * action deny
MS# configure access-list stopbadguys src-ip *src-mask
   dest-ip * protocol * sport * dport * action permit
MS# configure interface gigethernet 1/0 megisto-int
MS(config-if-gige1/0)# access-group stopbadguys in
```

Displaying Access Lists

Access lists are displayed via the `show access-list` command.

Configuring SSH

Secure Shell (SSH) provides a secure means of remote file transfer. The MS950 is shipped with a default SSH configuration stored in a configuration file. The default configuration allows both password and public key authentication but requires only password authentication. A default public/private key pair is used. It is highly recommended that the host key be changed.

To modify the default SSH configuration:

1. Download the text file `fs1:user0/etc/ssh2/ssh2.cnf`.

   Place the file in a location where it can be opened and modified.
2. Make the desired changes.
3. Save the file with the same name.
4. Place the file back into the same location.

To modify the default key pair:

1. Download the text files `fs1:user0/etc/ssh2/hostkey.pub` and `fs1:user0/etc/ssh2/hostkey.`

   Place the file in a location that it can be opened and modified.

   The file `hostkey.pub` contains the public hostkey. It is highly recommend that this key be changed. The `hostkey.pri` file contains the private host key.
2. Make the desired changes.

   To change the key, you need key generation software. SSH key generation software is available for download at www.ssh.com. This Website also contains extensive documentation on configuring the Secure Shell server.
3. Save the file with the same name.
4. Place the file back into the same location.

Displaying SSH information

You can display the current SSH configuration via the `show ssh` command.

Chapter 14: System Time Settings

In This Chapter

- NTP
- Setting Time and Date

The MS950 uses Network Time Protocol (NTP) for server time synchronization. You can set specific time and date data via the CLI.

System clock behavior is dependent on the state of configuration. Upon initialization, the Real Time Clock chip contains the current time if the clock has already been set and power has been off less than 30 days. If NTP is configured and is available, the clock comes under the control of NTP after initialization. If NTP is unavailable, the clock commands may be used to set the clock manually.

Configuring NTP

The MS950 uses NTP as specified in RFC1305 to obtain time information from time servers to synchronize internal timekeeping processes.

To configure NTP in administrator mode:

1. Enter the following at the command prompt to enter NTP commands:
   ```
   configure ip
   ```
2. Enter the following at the command prompt to configure NTP:
   ```
   ntp-server ip_address source
       interface_name [poll-interval
       minutes] [prefer] [version number]
   ```

Example

The following example assigns an NTP server.

```
MS# configure ip
MS(config-ip)# ntp-server source fei9/0 192.168.20.1
   version 4 prefer
```

Displaying NTP Information

You can display the current NTP servers using the **show ntp** command.

Setting Time and Date

You can set clock and calendar parameters to keep an accurate recording mechanism. These settings are appended to files at creation or modification. You can display the current clock settings using the **show clock** command.

Note: The order of entry for the following commands is important. When you are using a new or clean configuration, the commands must be entered in the order prescribed. On an existing configuration, the commands are accepted in any order.

To set time and date in administrator or superuser mode:

1. Enter the following at the command prompt to specify the time zone.:
   clock timezone *zone hour_offset* [**minute-offset** *minutes_offset*]
2. Enter the following at the command prompt to specify daylight savings time:
   clock summer-time start-date *date* **start-time** *time* **end-date** *date* **end-time** *time*
3. Enter the following at the command prompt to specify the current date and time:
   clock set [**date** *date*] [**time** *time*]

   The system calculates the UTC time based on the local time entered.

Example

The following example specifies the time and date for use by the system.

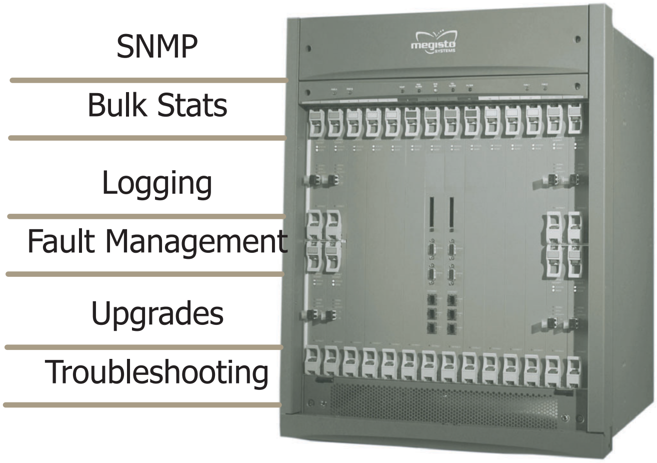
```
MS# clock timezone est -5
MS# clock summer-time start-date 05/20 start-time 23
   end-date 10/30 end-time 23
MS# clock set date 2001/09/03 time 04:12:01
```

Displaying Clock Information

You can display the current clock settings using the **show clock** command.

Section III: Management Configuration

The chapters in this section describe features that help you manage the system and its elements. Setup of SNMP, bulk statistics, and logging are provided.



Chapter 15: Software Release Management

The MS950 is shipped with default configuration files, including a default boot-image and a default configuration file.

The system obtains its configuration information from the **`system:/startup.cfg`** file upon reload (boot). All other system information is contained in the released software files such as boot-images. This chapter provides instructions on maintaining and upgrading system software and configuration files.

In This Chapter

Managing Software Releases

The MS950 contains system software that is updated from time to time. These release images can be updated for the entire system or a specific card.

It is important that you read the release notes for each new release because installation instructions for each release may differ. A typical release allows you to upgrade the entire system or a specific card.

The MS950 boots from the CompactFlash module fs1:/user0. The boot-images on each flash device must be designated as primary or secondary. When performing an upgrade, the new software should be loaded as the primary software and the last release as the secondary.

Depending on whether the release is backward-compatible, different scenarios may be used.

System-level Upgrades

System-level reloads upgrade the entire system. They can be done immediately or at a scheduled time. They can be used for any type of software upgrade that applies to all of the cards.

Note: The **`reload system`** command is also used for a cold boot of the system.

To perform a system upgrade in administrator or superuser mode:

1. Enter the following at the command prompt to copy the desired new files into fs1:/user0:
   `copy` *`IP`*`:/`*`filename`* **`fs1:/user0/`***`directory/filename`*
2. Enter the following at the command prompt to specify the primary and secondary boot image files:
   `boot-image` *`file_name`* **`secondary`** *`file_name`*
3. Enter the following at the command prompt to specify a boot image reload schedule:
   `reload system` `[`**`at`** *`time`*`] [`*`month`*`] [`*`day`*`]`
4. Enter the following at the command prompt to commit to the new release:
   `boot-image` *`file_name`*

   The file name in this case is the name of the new release file. You can go back to the old version of the software using the same command with the filename of the previous release name. It may be useful to do a **`show boot-image`** to identify the correct filenames.

Example

The following example copies the new release into fs1:/user0 and specifies it as the primary boot image. It then immediately reloads the entire system. Updates are done as the system reboots.

```
MS# copy fs2:/image/MS0102016.bin fs1:/user0/image/
   MS0102016.bin
MS# boot-image fs1:/user0/image/MS0102016.bin
   secondary fs1:/user0/image/MS0102015.bin
MS# reload system
System boots....show boot-image, if desired
MS# boot-image fs1:/user0/image/MS0102016.bin
```

Card-level Upgrades

Card-level upgrades are applied to a single card. They can be performed immediately or at a scheduled time. The new release must be backward-compatible with the current running release as indicated in the release notes.

To perform a card upgrade in administrator or superuser mode:

1. Enter the following at the command prompt to copy the desired new files into fs1:/user0:
   `copy IP:/filename fs1:/user0/release`
2. Enter the following at the command prompt to specify the primary and secondary boot image files:
   `boot-image file_name secondary file_name`
3. Enter the following at the command prompt to specify a card to upgrade:
   `upgrade card slot_number [at time] [month] [day]`

   It is recommended that you upgrade standby cards, one at a time. Wait for the hot standby card to activate. Next, upgrade the cards that were active.
4. After all cards are upgraded, enter the following at the command prompt to commit to the upgrade:
   `boot-image file_name`

   The file name in this case is the name of the new release file. You can go back to the old version of the software using the same command with the filename of the previous release name.

Example

The following example specifies copies the new release into fs1/user0 and specifies it as the primary boot image. The MS950 has 2 control cards (slot 10 is standby, 9 is active) and 3 service cards (slot 7 is standby, 5 and 6 are active) to be upgraded.

```
MS# copy fs2:/image/MS0102016.bin fs1:/user0/image/
   MS0102016.bin
MS# boot-image fs1:/user0/image/MS0102016.bin
   secondary fs1:/user0/image/MS0102015.bin
MS# upgrade card 10
MS# upgrade card 7
Wait for the hot standby card 10 to activate....
```

```
MS# upgrade card 9
MS# upgrade card 5
Wait for the hot standby card 7 to activate....
MS# upgrade card 6
Wait for the hot standby card 5 to activate....
MS# boot-image fs1:/user0/image/MS0102016.bin
```

Displaying Release information

The release status of a file can be viewed via the **`show release-info`** command. Primary and secondary boot-image names are shown via the **`show boot-image`** command. Upgrade and reload schedules are shown via the **`show reload`** and **`show upgrade`** commands.

Chapter 16: System Management

The MS950 has several tools that allow you to manage the system as well as gather information on system performance.

SNMP

SNMP is used to monitor such system elements as environment, health, and statistics. This application Layer 7 protocol facilitates the exchange of information between network devices and is part of the TCP/IP protocol suite. SNMP lets you manage network performance, find and resolve network problems, and plan for network growth.

SNMP consists of three parts: the agent, the manager, and the MIB. Agents gather data from variables in the MIB database and then send traps (notifications) to the manager (a management station). The management station can send get or get-next requests on variables in the MIB to the agent, while the agent sends traps to the management station.

You can specify an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the MS950. Standard MIBs as well as the Megisto-specific MIBs are located on the CD in the *build_MIBs* directory.

Note: GTP and GTPP SNMP traps are not supported when the MS950 acts a CDMA HA.

Configuring SNMP

The following procedure sets SNMP parameters.

To configure SNMP in administrator or superuser mode:

1. Enter the following at the command prompt to begin SNMP configuration:
   configure snmp
2. Enter the following at the command prompt to configure the server:
   server contact *syscontact*] [**location** *syslocation*]
   [**hostname** *hostname*]
3. Enter the following at the command prompt to define SNMP get community string:
   community get *string*
4. Enter the following at the command prompt to define SNMP set community string:
   community set *string*
5. Enter the following at the command prompt to define SNMP trap community string:
   community trap *string*
6. Enter the following at the command prompt to enable or disable the traps that the MS950 sends:
   trap *trap_id* | **all** {**enable** | **disable**}
7. Enter the following at the command prompt to enter the source address used for traps:
   trap-source *ip_address*
8. Enter the following at the command prompt to configure which SNMP notifications are sent:
   notifications information | **notice** | **warning** |
   disabled
9. Enter the following at the command prompt to configure the SNMP trap target:
   target *target_ip_address* [**port** *port_number*]

Note: The target_ip_address must be set in order for traps to be sent.

Example

The following example provides SNMP server contact information and sets the desired community strings. It then sets the target, trap source, and maximum packet size to be transmitted.

```
MS# configure snmp
MS(config-snmp)# server contact joemegisto@megisto.com
   location centuryblvd hostname MS950
MS950(config-snmp)# community get private
MS950(config-snmp)# community set public
MS950(config-snmp)# community trap private
MS950(config-snmp)# trap-source 190.11.123.44
MS950(config-snmp)# trap chassis-pdu-b-Failure enable
MS950(config-snmp)# notification warning
MS950(config-snmp)# target 128.89.1.112 port 163
```

Displaying SNMP Information

You can display information about the current SNMP configuration via the **show snmp** command.

Logging

The logging commands list configuration events and system error messages, such as interface status, security alerts, environmental conditions, debugging output, and CPU process overloads in files. Likewise, any captured application debug output sessions in a real-time scenario use this facility to log messages. The log messages stay in the system log for a pre-configured interval. Log messages may also be displayed at a console terminal (local or remote) or sent to a network management station via a syslog client application.

To create logs in administrator or superuser mode:

1. Enter the following at the command prompt:
   configure
2. Enter the desired version of the syslog local command at the command prompt to configure local logs:
   syslog local

```
syslog local [type {memory | console | file}]
no syslog local
```

3. Enter the desired version of the syslog host command at the command prompt to configure host logs:

```
syslog host
syslog host {ip-addr ip_address} [port port_num]
syslog host {level {alert | critical | error | warning
   | notice | info | debug}}
syslog host {facility {kern | user | mail | daemon |
   auth1 | syslog | printer | news | uucp | audit |
   clock2 | local0 | local1 | local2 | local3 | local4
   | local5 | local6 | local7}}
no syslog host
```

Example

The following example specifies all log parameters for the host at the specified address.

```
MS# configure syslog host ip 192.178.66.764 port 1200
   level info
```

Displaying logging information

You can display logs using the **show syslog** command. You can clear a local-log using the **clear local-log** command.

Fault Management

Alarms are activated in the system whenever specified faults occur. As an administrator or superuser, you can clear alarms using the **clear alarm** commands. You can view alarms using the **show alarm** command.

Chapter 17: Statistics

The MS950 has several tools that allow you to gather information about system performance.

In This Chapter

- Statistic show commands
- Configuring System statistics
- Bulk Statistics

GGSN System Statistics

GGSN ~~CDMA~~ ~~SSN~~

You can monitor system-level statistics via a variety of show commands that reveal detail traffic-related information upon request.

To configure system statistics:

1. Enter the following at the command prompt:
   `configure interval minutes` *`minutes`*

Note: This command is applicable to MIP.

2. Enter **`exit all`** to get to the top-level prompt.
3. Enter any of the following show commands to view statistical information (see the *MS950 CLI Reference Guide* for exact syntax):
   - show apn-pdp-statistics apn
   - show apn-pdp-statistics select
   - show apn-pdp-statistics last-interval
   - show apn-pdp-statistics context apn
   - show apn-pdp-statistics context select
   - show imsi-pdp-statistics context imsi
   - show imsi-pdp-statistics context select,
   - show ms950-pdp-statistics control
   - show ms950-pdp-statistics data
   - show ms950-pdp-statistics signalling-count
   - show ms950-pdp-statistics sgsns
   - show ms950-pdp-statistics sgsns select
   - show interval

Example

The following example configures the pdp-statistics interval generation and displays specific statistics for win.megisto.com.

```
MS# configure interval minutes 25
MS(config)# exit all
MS# show apn-pdp-statistics select c1 1 c2 3 c3 100 c4
   win.megisto.com

Number of   Number of   %     Access Point Name
PDP         PDP         Total
Contexts    Contexts    Calls
Active      Failed
======================================================
1           3           100   win.megisto.com
```

MIP Statistics

You can monitor MIP traffic via the following show commands.

To configure system statistics:

1. Enter the following at the command prompt: **`configure interval minutes`** *`minutes`*
2. Enter **`exit all`** to get to the top-level prompt.
3. Enter any of the following show commands to view statistical information (see the *MS950 CLI Reference Guide* for exact syntax):
   - show stats apn-mip-statistics apn
   - show stats apn-mip-statistics select
   - show stats apn-mip-statistics last-interval
   - show stats ms950-mip-statistics control
   - show nai-mip-statistics data

Example

The following example configures the pdp-statistics interval generation and displays specific statistics for win.megisto.com.

```
MS# configure interval minutes 25
```

```
MS(config)# exit all
MS# show stats apn-mip-statistics select c1 1 c2 3 c3
   100 c4 win.megisto.com
```

Bulk Statistics

Bulk statistics provide a mechanism for monitoring use of system resources including global system resources (e.g., CPU), interfaces and sub-interfaces, and IPSec security associations. It does this by allowing the user to apply schema definitions to the system resources. Bulk statistics collection also provides a means of collecting accounting information for permanent flows. This differs from RADIUS, which is used for reporting accounting information for transient sessions. It is also useful for collecting statistics in networks with large numbers of devices in which SNMP polling becomes impractical. All of the information collected is stored in data collection files, which are periodically transferred to a collector station.

Creating a Schema Definition File

The data that is collected into the collection file is determined through the use of a "schema". Each schema is like a "printf" statement; it has a format string that specifies the format of the data through the use of conversion characters, followed by a list of variables that correspond to the conversion characters. Each schema is bound to an interface or other system resource via the CLI.

Schema definition (from the schema definitions file):

```
schema-def schema1 "gige: inPkts %u outPkts %u\n",
   ifInPkts, ifOutPkts
```

There are three conversion characters for all schema: %u for unsigned long integers, %d for integers, and %s for strings. They operate in the same manner as in the standard C library “printf” function.

The schema definitions are contained in a file called **`schema_def.txt`**, located in **`fs1:/user0/bulk`**. This file is created upon boot. You can edit this file and then re-load it using the **bulk params** command. Also, an alternate file name can be provided with the same command.

Schema Definition File Syntax

The schema definition file follows a specific syntax. An example of the file is shown below:

```
# sample schema definition file, schema_def.txt
schema-def global "host: %s cpu %d\n", hostname,
   cpu5min
schema-def gige_if "%s: %d/%d inPkts %u outPkts %u\n",
   description, slot, port, ifInPkts, ifOutPkts
schema-def gige_subif "%s: %d/%d.%d inPkts %u outPkts
   %u\n", description, slot, port, instance, ifInPkts,
   ifOutPkts
schema-def gtptun "%s: %d/%d.%d inPkts %u outPkts
   %u\n", description, slot, port, instance, ifInPkts,
   ifOutPkts
schema-def ipsectun "%s: %d/%d.%d inPkts %u outPkts
   %u\n", description, slot, port, instance, ifInPkts,
   ifOutPkts
```

Schema Definition File Syntax Rules

- Lines that are blank, or that begin with a “#”, are ignored.
- White space is ignored.
- All schema definition lines must begin with “schema-def”, followed by the name of the schema.
- The format string must follow the name of the schema definition, and it must begin and end with double quotes(").
- The the format string and the variables that immediately follow it must be separated by commas.
- Each schema definition must fit on one line; it may not be broken across multiple lines.

Schema Variable Names and Conversion Characteristics

The following are valid (% values) for use in the schema definitions file.

System (Global)	Interface and Sub-interface	IPSec Security Associations
Hostname %s	description %s	description %s
Date %s	slot %d	slot %d
timeofday %s	port %d	port %d
Sysuptime %u	ifInOctets %u	instance %d
Cpu5min %d	ifInPkts %u	ifInOctets %u
Cpu1min %d	ifInDiscards %u	ifInPkts %u
Cpu5sec %d	ifOutOctets %u	ifInDiscards %u
	ifOutPkts %u	ifOutOctets %u
	ifOutDiscards %u	ifOutPkts %u
		ifOutDiscards %u
		inDecryptErrors %u
		inAuthErrors %u
		inReplayErrors %u
		inOtherErrors %u

Configuring Bulk Statistics

Once the schema definitions file has been created or modified, you can configure bulk statistics output.

Note: The default schema definitions file is created by the system when it initializes.

To configure bulk statistics in admin or superuser mode:

1. Enter the following at the command prompt to enter bulk configuration commands:
   ```
   configure bulk
   ```
2. Enter the following at the command prompt to setup information about the collector station:
   ```
   collector {ip-address ip_address} [user name]
       [password password] [secondary]
   ```

3. Enter the following at the command prompt to map a schema to an interface:

   ```
   map {schema name} {interface name | remote-gateway
      ip_address | system}
   ```

4. Enter the following at the command prompt to set up the parameters for the bulk stats server:

   ```
   params [local-path path_name] [sampling-interval
      minutes] [transfer-interval minutes] [retention-
      period hours] [transfer-method [ftp]] [remote-path
      path_name] [file-usage max_size] [schema-file
      file_name]
   ```

5. If desired, enter the following at the command prompt to force immediate transfer of bulk stats to the collector station:

   ```
   force-transfer
   ```

6. Enter the following at the command prompt to enable bulk statistics:

   ```
   no shutdown
   ```

Example

The following example sets up the bulk statistics collector station, maps a schema to an interface, and sets parameters for the bulk server.

```
MS# configure bulk
MS(config-bulk)# collector ip-address 124.234.20.2
MS(config-bulk)# map schema gige-if interface gige2/0
MS(config-bulk)# map schema gige-if interface gige2/
   0.1
MS(config-bulk)# map schema ipsectun remote-gateway
   192.234.24.2
MS(config-bulk)# params local-path path1 sampling-
   interval 22 transfer method ftp schema-file schema1
MS(config-bulk)# no shutdown
```

Displaying Bulk Stats Information

You can display information about your bulk statistics setup using the following commands:

- `show bulk maps`
- `show bulk params`

- `show bulk schema`

Chapter 18: Troubleshooting

The CLI provides a variety of mechanisms for troubleshooting data transmission. Debug commands allows you to monitor applications states. For example, you can watch a transaction of a particular TCP connection between a MS950 and another host or you can monitor GTP control plane activity and interactions with other processes for IP address assignment.

You can view protocol statistics, buffer content, and queue content at any time using a series of show commands. You can use show commands to test general connectivity. In addition, the commands provide problem traceability through their comprehensive diagnostics.

In This Chapter

Displaying Information

Most features in the CLI have show commands that display the active configuration on a per-feature basis. Show commands help monitor installation behavior and normal network behavior, as well as isolate problem areas. Show commands are listed in the same location as the feature in this manual and are described in detail in the *MS950 CLI Reference Guide*.

Debugging

The Debug and Trace feature on the MS950, in the form of **`debug`** commands, can be used to turn on and off debugging-related information for a specified sub-system. These commands assist in the isolation of protocol and configuration problems. All debug information is forwarded to Syslog, and get displayed as per the options set in Syslog. You must configure logging prior to enabling debugging. The **`syslog`** commands designate where debugging output is displayed. See “Logging” on page 16-3. In addition, debug information can be written to CompactFlash for later retrieval. All debug commands are listed the *MS950 CLI Reference Guide*.

When viewed on the console, individual traces may appear truncated if they exceed the Syslog-defined maximum size limit of 512 bytes. For such cases, it is recommended that traces also be dumped to the CompactFlash file system. On the CompactFlash, each sub-system may generate 5 Mb of data in the form of 10 files each of size 0.5 Mb. Each sub-system has its own directory on the CompactFlash file system. For example, debug files related to GTP can be located under **`/ata1/DBGT/GTP`** and they are named `gtp.00` through `gtp.10`. Similarly, debug files related to GTPP can be located under **`/ata1/DBGT/GTPP`** and they are named `gtpp.00` through `gtpp.10`. In addition, each file also contains a timestamp at the beginning. When the size of the debug information reaches 5 Mb, the oldest file is deleted and a new file is created to store data.

GTP, GTPP, and IPSec Debugging

The **`debug gtp`** command can be used to troubleshoot potential GTP-related communication problems between the MS950 and SGSNs. This command can also be used to collect debug information for a specific IMSI and NSAPI.

Similarly, the **`debug gtpp`** command can be used to troubleshoot potential GTPP-related communication problems between the MS950 and charging gateways. This command can also be used to collect debug information for a specific charging gateway functions.

The **`debug ipsec`** command can be used to troubleshoot potential IPSec-related communication problems between the MS950 and remote security gateways. This command can also be used to collect debug information for a specific tunnel.

Note: At times, these commands may generate a significant amount of data, therefore it is advised to use them only as needed.

Depending upon the requirements, a variety of debug information can be collected. The following keywords indicate the different levels of debug information that are supported.

Keyword	Description
Events	Protocol FSM state transitions and general trace information.
Messages	Brief description of protocol messages sent and received (no hex dump).
Packets	Received and sent messages protocol header hex dump.
Payload	Received and sent messages complete hex dump (header + data).
Verbose	All of the above.

Example

The following example enables debugging for GTP.

```
MS# debug gtp
```

The following example enables events-level debugging for all GTP contexts.

```
MS# debug gtp events context all
```

The following example enables events-level debugging only for the GTP context identified by IMSI= 123456789123456 and NSAPI= 6.

```
MS# debug gtp events context imsi 123456789123456
   nsapi 6
```

The following example turns on the file-system logging option for GTP.

```
MS# debug gtp logging
```

The following example temporarily disables all debugging related to GTP with the intention of re-enabling it later.

```
MS# no debug gtp
```

The following example disables GTPP debugging for the CGF identified by the IP address 10.11.12.13, and cleans up occupied resources.

```
MS# no debug gtpp context ip-addr 10.11.12.13
```

The following example disables all GTPP debugging and cleans up occupied resources.

```
MS# clear debug-gtpp
```

The following example disables all IPSec debugging and cleans up occupied resources.

```
MS# clear debug-ipsec
```

Diagnostics

You can use diagnostic commands to evaluate how data is traveling through the MS950. The **show on-line statistics** command show diagnostics about the cards. You can enable statistics with the **on-line statistics** command and clear them with the **clear on-line-statistics** command.

Testing Connectivity

Ping and Traceroute

The **ping** and **traceroute** commands allow you to test connectivity either by verifying IP reachability or by tracing IP route routes.

```
ping {ip_address | hostname} [number-of-packets value]
    [interface name] [src ip_address] [pattern
    hex_pattern] [size bytes] [timeout seconds] [apn
    apn]
traceroute {ip_address} [df] [maxttl ttl] [minttl ttl]
    [size bytes] [count number] [timeout seconds] [port
    number] [src src_ip] [interface name] [apn apn]
```

Example

```
MS# traceroute 4.0.0.1 size 1024
MS# ping 4.0.0.1 size 1024
```

Resetting the System

You can reset the system using the **`reload system`** and **`reload card`** commands. These perform either a system- or card-level cold boot that may be immediate or scheduled. The **`reload system`** command is also used for software upgrades.

Example

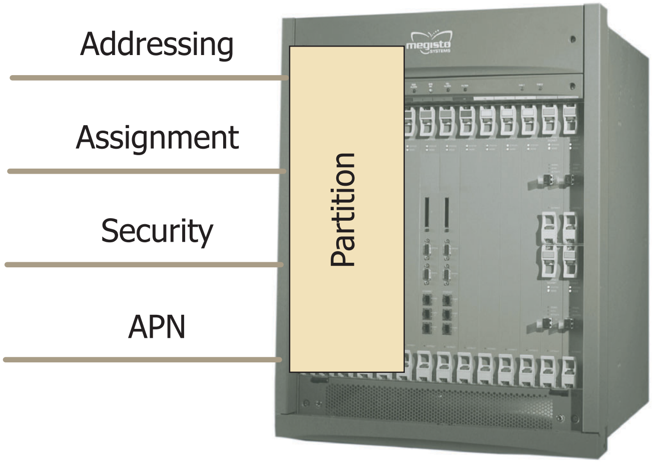
The following example schedules a card reload at the specified time and date.

```
MS# reload card 3 jun 23 at 23:00
```

Troubleshooting

Section IV: Subscriber Services

The chapters in this section provide information on how to configure subscriber access and addressing.



Chapter 19: Subscriber Partitions

The MS950 hosts subscribers. Subscribers are the end users of the data transmitted to and from the MS950. A subscriber partition relates to a set of subscribers that are associated with an APN and designates a physical area of the MS950 used for that subscriber's access to information. Subscribers communicate with the MS950 via PDP-contexts (associated with the APNs). Each subscriber partition has an access point and addressing scheme that identifies it and provides its method of access. All subscriber-specific information is configured in the subscriber partition.

This chapter describes the creation and configuration of the subscriber partition. Subscriber addressing can be performed at a global level or at the partition level. All subscriber addressing is discussed in “Subscriber Addressing Mechanisms” on page 20-6.

Creating Subscriber Partitions

Subscriber partitions set subscriber access based on the subscriber's APN and access mode. In general, the following flow can be followed.

To configure subscriber partitions in administrator or superuser mode:

1. Enter the following at the command prompt to name the partition:
   ```
   configure subscriber-partition name
   ```

2. Enter the following at the command prompt to set the APN name:
   access-point *name* [**vpn**]
3. Enter the following at the command prompt to specify authentication parameters:
   authentication none | **radius** | **local**
4. Enter the following at the command prompt to bind a charging policy to the access point:
   charging-policy *policy_name*
5. If desired, enter the following at the command prompt to enable subscription verification:
   subscription-required
6. Configure addressing mechanisms. See “Subscriber Addressing Mechanisms” on page 20-6.

Note: If a prepaid billing charging policy is selected, the **radius-server, rps,** and **radius-service** commands must be configured either globally or for the specific APN. RADIUS addressing must be configured, as must the RPS. See “RADIUS” on page 11-21.

7. Configure partition assignments. See “Configuring Partition Assignment” on page 19-3.
8. Enter the following at the command prompt to enable the partition:
   no shutdown.

Example

The following example sets the MS950 in config mode, creates a subscriber partition named megistosystems, names the access point, and sets the GPRS access mode to transparent. It then configures the partition assignment, configures a local pool, prescribes a charging policy, and assigns an IPSec treatment type.

```
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# authentication none
MS(config-subs-apn)# address-method local-pool
MS(config-subs-apn)# subscriber-address-pool
   192.234.40.1 255.255.255.0 service-card 5
MS(config-subs-apn)# charging-policy ppayPlanBPolicy
MS(config-subs-apn)# subscription-required
MS(config-subs-apn)# treatment-type ipsec
MS(config-subs-apn)# ipsec-policy-map map1
MS(config-subs)# exit
MS(config-subs)# no shutdown
```

Wildcard APNs

The Wildcard APN feature lets you provision a single APN throughout the network. Subscribers that use this APN can be redirected to a different APN, one that is provisioned only on the MS950. This redirection is accomplished independently of the MS950 through subscriber policies on an external RADIUS server.

The following *must* be set for the MS950 to support Wildcard APN:

- The Wildcard APN must be configured to use RADIUS authentication via the **`authentication`** command.
- The RADIUS server must be configured to return the redirected APN in the callback-id field of the access-accept message.

At the time of call setup, the mobile subscriber signals the MS950 with the Wildcard APN. You can choose to override the mobile subscriber's signaled username/password by enabling the override flag of the subscriber partition on the MS950 via the **`generic-user-info`** command. If the override flag is set, then the MS950 attempts authentication using the generic-user-info username and password that was configured on the MS950. See "Configuring Subscriber RADIUS Addressing" on page 20-7 for more information on subscriber RADIUS addressing.

Configuring Partition Assignment

In addition to configuring addressing mechanisms and access points for a subscriber partition, you can provide a security scheme and a treatment type.

To configure partition assignments in administrator or superuser mode:

1. Create the subscriber partition and APN as shown in "Creating Subscriber Partitions" on page 19-1.
2. Enter the following at the command prompt to specify a treatment type:

```
treatment-type {simple-ip| vlanvpn vlanname| ipsec
   policy_name}
```

For VLANVPNs, a sub-interface configured for VLANs must exist. See "Sub-interfaces" on page 8-4. The VPN name is designated in the **vlan** command.

For IPSec, an IPSec policy must exist. See "Configuring IPSec and IKE" on page 21-2.

Example

The following example sets the MS950 in config mode, places you in the subscriber partition named megistosystems, creates an APN, sets the treatment type to IPSec, and assigns an IPSec policy map.

```
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# treatment-type ipsec policy1
```

Displaying Subscriber Information

You can display information about the subscriber partition via the **show subscriber-partition** command.

Subscriber Packet Redirection

You can specify to redirect packet data traffic of subscribers who match a profile and filter to a different destination address than those listed in the destination address of the packet.

To configure redirection in administrator or superuser mode:

1. Enter the following at the command prompt:
   ```
   configure redirect-rule-set name [ip-address
      ip_address] [netmask netmask] [protocol tcp | udp |
      icmp | number] [port port] nexthop ip_address
   ```
2. Enter the following commands at the command prompt to enter the desired APN:
   ```
   subscriber-partition name
   ```

```
access-point name [vpn]
```

3. Enter the following at the command prompt to bind the rule set:

```
bind-redirect name
```

Example

The following example redirects packet traffic for a subscriber.

```
MS# configure
MS(config)# redirect-rule-set rule1 10.10.10.2
   255.255.0.0 protocol tcp 205.123.54.0
MS(config)# subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# bind rule1
```

Displaying Packet Redirection

You can display information about the subscriber partition via the **show redirect-rule-set** command.

Chapter 20: Addressing Mechanisms

The MS950 supports several mechanisms to determine the address allocation method for mobile subscribers. This includes DHCP, address pools, and RADIUS.

Mobile subscribers may obtain their IP addresses either statically or dynamically. In the case of static IP address assignment, the mobile subscribers are pre-programmed with IP addresses that they use when they log on to the MS950, but the MS950 does not assign them their IP addresses. This static IP address is the address that the MS950 uses to identify the mobile device. In the case of dynamic address assignment, the MS950 assigns IP addresses using either local pools, DHCP, or RADIUS.

In This Chapter

Subscriber Address Pools

For each addressing mechanism, an address pool must exist. In any subscriber-pool, if a host address instead of a network address is specified for the *ip_address* parameter, this address is marked as reserved and the MS950 never allocates it. You can use this host address as the client address in the **`radius-server`** and **`push-server`** commands.

In the case of DHCP, three addresses are marked as reserved: the all ones (1), the all zeroes (0), and the host address (entered as the *ip_address* parameter). The host address would be used as a giaddr when talking to the DHCP server. You must bind this address to a loopback address (interface) for all non-VPN cases so that the responses from the DHCP server get back to the MS950.

Example

In the following example, the address pool ranges from 10.0.128.0 to 10.0.207.255. The addresses 10.0.128.0 and 10.0.207.255 are marked as reserved. The address 10.0.128.1 is also marked as reserved because the operator specifies an address with non-zero host bits. The first address available for assignment for the subscriber is 10.0.128.2.

`subscriber-address-pool` *`ip_address netmask`* {**`service-card`** *`slot_number`*}

```
MS# subscriber-address-pool 10.0.128.1 255.255.192.0
service-card 5
```

If this command were changed to

```
MS# subscriber-address-pool 10.0.128.99 255.255.192.0
service-card 5
```

then 10.0.128.99 would be marked as reserved instead of 10.0.128.1, as shown in the previous example. The address allocation would start from 10.0.128.1, go up to 10.0.128.98, skip over 10.0.128.99, and continue from 10.0.128.100.

Default Addressing Mechanisms

DHCP, local pools, and RADIUS addressing can be assigned for use by default. Unless a subscriber partition specifies an addressing mechanism, the default assignment is used.

Configuring DHCP

You can set dynamic address allocation at the system level or at the subscriber partition level (via an APN). The MS950 can assign IP addresses to subscribers using DHCP in proxy mode. The arrival of a PDP-context creation message triggers a DHCP request to a server. The following procedure provides the commands at the system level. See "Configuring Subscriber DHCP Addressing" on page 20-6 for information on DHCP at the subscriber partition level.

To configure default DHCP settings in administrator or superuser mode:

1. Create a loopback interface to be used by the local pool. See "Virtual Loopback Interfaces" on page 8-8.

   The IP address used for this interface must be one of the addresses in the subscriber pool created in step 4.
2. Enter the following at the command prompt:
   configure ip
3. Enter the following at the command prompt to assign the DHCP server:
   dhcp-server *prim_ip_address* [*prim_server_name*] [**sec-ip** *sec_ip_address*] [**sec-name** *sec_server_name*]
4. Enter the following at the command prompt to create a DHCP address pool:
   subscriber-address-pool *ip_address netmask* {**service-card** *slot_number*} {**type dhcp**}

Example

The following example configures default DHCP addressing for the MS950.

```
MS# configure interface loopback 9/0.10 name dhcploop
MS#(config-if-lo9/0.10)# ip-address 172.24.1.1
   255.255.255.0
MS(config-if-lo19/0.10)# exit all
MS# configure ip
MS(config-ip)# dhcp-server 192.168.10.10 DHCP_PRIMARY
   sec-ip 4.0.0.2 sec-name wsp-megisto-dhcp
MS(config-ip)# subscriber-address-pool 172.24.1.1
   255.255.0.0 service-card 14 type dhcp
```

Displaying DHCP Information

You can display DHCP settings via the **show dhcp-server** command.

Configuring Default Local or Static Address Pools

Local address pools are stored on service cards. The MS950 can be configured with local address pools out of which it assigns addresses to the mobile stations. These pools are assigned to subscribers when they access the MS950. If the subscriber already has an IP address, static pools are used.

To configure default local or static address pools in administrator or superuser mode:

1. Enter the following at the command prompt:
   ```
   configure ip
   ```
2. Enter the following at the command prompt:
   ```
   subscriber-address-pool ip_address netmask {service-
      card slotnumber} {type {local | static}}
   ```

Example

The following example sets the MS950 in config mode and assigns an address pool.

```
MS# configure ip
MS(config-ip)# subscriber address-pool 192.234.40.0
   255.255.255.0 service-card 5 type local
```

Displaying Local Address Pools

You can display a table of all address pools or specific information about an individual pool using the **`show subscriber-address-pool`** command.

Configuring Default RADIUS Servers

RADIUS is a client/server solution for remote security management. RADIUS is the de facto industry standard for user authentication, authorization, and accounting (AAA). It provides a distributed security solution and eliminates the need for special hardware while providing access to a variety of state-of-the-art security solutions. The distributed security architecture provided by RADIUS separates user authentication and authorization from the communications process and creates a central location for user authentication data. Communication servers, such as the MS950, act as RADIUS clients. The MS950 sends authentication requests to the RADIUS server and acts on responses sent back by the server. It is recommended that you configure the RADIUS authentication and accounting servers to be the same.

Note: RADIUS uses the MS-ID loopback interface. It must exist for RADIUS to work properly.

To configure default RADIUS servers in administrator or superuser mode:

1. Enter the following at the command prompt:
   `configure ip`
2. Enter the following at the command prompt:
   `subscriber-address-pool` *`ip_address netmask`* {**`service-card`** *`slotnumber`*} (**`type`** {**`radius`**}}
3. Enter the following at the command prompt to configure AAA parameters:
   `configure aaa`
4. Enter the following at the command prompt to specify a RADIUS server host:
   `radius--server` [**`auth`** | **`acct`**] {**`ip`** *`ip_address`*} [**`name`** *`name`*] [**`key`** *`key_string`*] [**`auth-port`** *`port`*] [**`acct-port`** *`port`*] [**`secondary`**] [**`timeout`** *`seconds`*] [**`retransmit`** *`retries`*] [**`interim`** *`seconds`*] [**`no-forwarding`**] [**`client-address ms-id`** | **`mgmt-id`** |*`ip_address`*]

Note: RADIUS accounting is enabled when the **`radius-server acct`** command is issued. If it has been turned off via the **`no radius-service`** {**`acct`**} command, you may enable it using the **`radius-service`** {**`acct`**}.

Example

The following example sets the MS950 in config mode, specifies RADIUS server authentication, and enables RADIUS service.

```
MS# configure ip
MS(config-ip)# subscriber address-pool 192.234.40.0
   255.255.255.0 service-card 5 type radius
MS(config-ip)# exit all
```

```
MS# configure aaa
MS(config-aaa)# radius-server auth ip 192.168.10.10
   name funk key funky
MS(config-aaa)# radius-service auth
```

Displaying RADIUS Information

You can display the current RADIUS server status using the **show radius-server** command.

Subscriber Addressing Mechanisms

For each APN, you can assign an addresing scheme. Subscriber-level addressing always overrides default addressing.

Configuring Subscriber DHCP Addressing

You can assign a specific DHCP server to a specific subscriber partition. This supersedes the global DHCP server.

To configure an APN-specific DHCP in administrator or superuser mode:

1. Create a loopback interface to be used by the local pool. See “Virtual Loopback Interfaces” on page 8-8.

   The IP address used for this interface must be one of the address in the subscriber pool created in step 5.
2. Create the subscriber partition as shown in “Creating Subscriber Partitions” on page 19-1.
3. Enter the following at the command prompt to specify a dynamic address allocation method:
   address-method dhcp-proxy-client
4. Enter the following at the command prompt to specify a primary and optionally a secondary DHCP server to allocate IP:
   dhcp-server *prim_ip_address* [*prim_server_name*] [**sec-ip** *sec_ip_address*] [**sec-name** *sec_server_name*] [**tunneling**]

Note: Use of this command overrides any global setting for DHCP.

5. Enter the following at the command prompt:

```
subscriber-address-pool ip_address netmask {service-
   card slot_number}
```

Example

The following example sets the MS950 in config mode, places you in the subscriber-partition named megistosystems, selects the address method dhcp-proxy-client, and creates an address pool for the APN.

```
MS# configure interface loopback 9/0.10 name dhcploop
MS#(config-if-lo9/0.10)# ip-address 172.24.1.1
   255.255.255.0
MS(config-if-lo19/0.10)# exit all
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# address-method dhcp-proxy-client
MS(config-subs-apn)# dhcp-server 192.168.10.10
   dhcp_primary
MS(config-subs-apn)# subscriber-address-pool
   172.24.1.1 255.255.0.0 service-card 14
```

Configuring Subscriber RADIUS Addressing

You can assign a specific RADIUS server to a specific subscriber partition. This supersedes the global RADIUS server.

Note: RADIUS uses the MS-ID loopback interface. This interface must exist for RADIUS to work properly.

To configure an APN-specific RADIUS in administrator or superuser mode:

1. Create the subscriber partition as shown in “Creating Subscriber Partitions” on page 19-1.
2. Enter the following at the command prompt to specify a dynamic address allocation method:
   `address-method radius-client`
3. Enter the following at the command prompt to specify RADIUS parameters:

```
radius-server [auth | acct] {ip ip_address} [name
   name] [key key_string] [auth-port port] [acct-port
   port] [secondary] [timeout seconds] [retransmit
   retries] [interim seconds] [no-forwarding] [client-
   address ms-id | mgmt-id |ip_address] [tunneling]
```

Note: RADIUS accounting is enabled when the **radius-server acct** command is issued. If it has been turned off via the **no radius-service** {**acct**} command, you may enable it using the **radius-service** {**acct**}.

Note: Use of this command overrides any global setting for RADIUS.

4. Enter the following at the command prompt:

```
subscriber-address-pool ip_address netmask {service-
   card slot_number}
```

5. If desired, enter the following at the command prompt to specify generic user information for the partition:

```
generic-user-info name name password password
    [override]
```

Note: The override value is used for wildcard APNs only.

Note: If prepaid charging is desired, the **rps** command must be configured. See “Configuring Prepaid Charging” on page 11-15.

Example

The following example sets the MS950 in config mode, places you in the subscriber-partition named megistosystems, and selects the address method radius-client.

```
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# address-method radius
MS(config-subs-apn)# radius-server auth ip
   192.168.10.10 name funk key funky
MS(config-subs-apn)# radius-service auth
MS(config-subs-apn)# subscriber address-pool
   192.234.40.0 255.255.255.0 service-card 5
MS(config-subs-apn)# generic-user-info name johnh
   password secret
```

Configuring Subscriber Local or Static Pool Addressing

You can assign a specific local pool server to a specific subscriber partition. This supersedes the global local or static pool.

To configure addressing mechanisms in administrator or superuser mode:

1. Create the subscriber partition as shown in “Creating Subscriber Partitions” on page 19-1.
2. Enter the following at the command prompt to specify a dynamic address allocation method:
   address-method {**local-pool** | **static**}
3. Enter the following at the command prompt:
   subscriber-address-pool *ip_address netmask* {**service-card** *slot_number*}

Note: Use of this command overrides any global setting for IP addressing.

4. If desired, enter the following at the command prompt to configure a DNS server specific to this APN:
   dns-server *ip_address* [**sec-ip** *ip_address*]
5. If desired, enter the following at the command prompt to configure a NETBIOS server specific to this APN:
   netbios-server *ip_address* [**sec-ip** *ip_address*]

Example

The following example sets the MS950 in config mode, places you in the subscriber-partition named megistosystems, selects the address method local-pool, specifies a pool, and configures DNS and NETBIOS servers.

```
MS# configure subscriber-partition megistosystems
MS(config-subs)# access-point megisto-engineering.gprs
MS(config-subs-apn)# address-method local-pool
MS(config-subs-apn)# subscriber address-pool
   192.234.40.0 255.255.255.0 service-card 5
MS(config-subs-apn)# dns-server 128.89.1.112 sec-ip
   4.0.0.2
MS(config-subs-apn)# netbios-server 128.89.20.112 sec-
   ip 192.234.68.2
```

Chapter 21: Subscriber Security

The MS950 provides network-level security as described in “Network Security” on page 13-1. This chapter discusses security specific to subscribers.

In This Chapter

- IPSec
- IKE
- Certificates

Configuring IPSec

IPSec is a set of protocols used to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement mobile intranets (also known as VPNs).

Two stations that want to communicate with one another establish a security association (SA) by exchanging security keys. SAs specify security parameters like the IPSec protocol used; the authentication and encryption algorithm; the keys themselves; the lifetime of the keys; and the lifetime of the entire SA.

An SA can be a simple connection between any two hosts or VPN gateways, or it can be a link between a host and a security gateway. Key exchange, defined in IKE, is normally a two-step process: a first to transfer security parameters and a second to transfer data. In the first phase, the partners establish an SA and decide on security parameters: encryption and hashing algorithms, authentication method, and the group of the Diffie-Hellman algorithm (the method used to calculate a shared secret (some piece of information known to each party but not to the general public)) to use. Once the parties agree on the parameters, they set up a second SA for data transfer.

Configuring IPSec and IKE

To configure IPSec in administrator or superuser mode:

1. Enter the following at the command prompt to enter IPSec commands:
   `configure ipsec`
2. Enter the following at the command prompt to configure the IKE policy:
   ```
   ike-policy policy_name enc alg hash alg auth mech dh-
      group group [lifetime seconds seconds]
   ```
3. Enter the following at the command prompt to set the policy map:
   ```
   policy-map name access-list listid end-point endpoint
      ike-policy names [pre-shared string] transform-set
      name pfs {enable | disable}
   ```
   The IPSec policy map is bound to a subscriber partition via the **`ipsec-policy-map`** command. See “Configuring Partition Assignment” on page 19-3.
4. Enter the following at the command prompt to set transform properties:
   ```
   transform name protocol esp mode tunnel enc alg hash
      alg
   ```
5. Enter the following at the command prompt to assign transform sets:
   ```
   transform-set name transforms transforms lifetime
      lifetime seconds seconds
   ```
6. Assign these parameters to a specific partition as described in “Configuring Partition Assignment” on page 19-3.

Example

The following example links the IKE policies to a transform set, tunnel, and access list.

```
MS# configure ipsec
MS(config-ipsec)# ike-policy vpn1_ike1 enc 3des hash
   sha1 auth rsa-sig dh-group modp-1024 lifetime
   seconds 100000
MS(config-ipsec)# policy-map vpn_map access-list
   vpn1_acl end-point 192.168.41.3 ike-policy
   vpn1_ike1,vpn1_ike2 transform-set vpn1_TS pfs
   enable
MS(config-ipsec)# transform vpn1_trans1 protocol esp
   mode tunnel enc 3des hash sha1
```

```
MS(config-ipsec)# transform-set vpn1_TS transforms
   vpn1_trans1,vpn1_trans2 lifetime seconds 100000
```

Displaying IPSec and IKE

A variety of shows commands are available for IPSec and IKE configuration, including:

- `show ipsec policy-map`
- `show ipsec stats`
- `show ipsec sa`
- `show ipsec hw-engine`
- `show ipsec ike sa`
- `show ipsec transform`
- `show ipsec transform-set`

Creating Digital Certificates

A digital certificate is an electronic “credit card” that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder’s public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Configuring Manual Certificates

Prior to configuring manual certificates on the MS950, you must generate the required keys and certificate. There are several commercial and non-commercial tools that have been developed for use in the generation of public and private keying material and certificate signing requests. It is recommended that you check the release of MS950 in use for the method prescribed for the current release.

To generate the required keys and certificate:

1. Generate the public and private key pairs in privacy enhanced mail (PEM) format or BER format.

2. Generate a certificate signing request (CSR) with the public key for the CA.
3. Copy the files into fs1:/user0:

```
MS# copy host:mscert.der fs1:/user0/mscert.der
Do you want to copy source file host:mscert.der
to destination file fs1:/user0/mscert.der ?(yes|no)yes
```

   Once the certificate information has been created, you can configure the way that it is used.

4. Enter the following at the command prompt to enter IPSec commands:

```
configure ipsec
```

5. Enter the following at the command prompt to specify CA or local certificate parameters:

```
certificate ca cert-name name certificate-file
   filename
certificate local cert-name name certificate-file
   filename private-key-file filename
```

Example

The following example creates certificates.

```
MS# configure ipsec
MS(config-ipsec)# certificate ca cert-name vpn1_cert
   certificate-file fs1:/user0/cacert.der
MS(config-ipsec)# certificate local cert-name vpn_key
   certificate-file fs1:/user0/pgncert.der private-
   key-file fs1:/user0/pgnpriv.der
```

Configuring Certificates via SCEP

You can use public key infrastructure (PKI) to generate and enroll certificates. In this case, you do not perform any manual configuration steps.

Note: Make sure DNS is properly configured prior to configuring certificates.

To configure PKI SCEP protocol based certificates:

1. Enter the following at the command prompt to begin entering PKI configuration:

```
configure pki
```

2. Enter the following at the command prompt to specify SCEP configuration:

   ```
   scep-config ca-name name ca-address address passcode
      passcode [crl-address address] [retry-count count]
      [retry-timer timer]
   ```

3. Enter the following at the command prompt to view the retrieved CA:

   ```
   fingerprint view
   ```

4. Enter the following at the command prompt to accept or reject the retrieved CA:

   ```
   fingerprint accept | reject
   ```

5. If the CA was accepted, enter the following at the command prompt to enroll it:

   ```
   enroll local-subject name
   ```

Example

The following example retrieves a CA, views the CA, accepts it, and enrolls it.

```
MS# configure pki
MS(config-pki)#scep-config ca-name test-ca1.ssh.com
   ca-address http://pki.ssh.com:8080/scep/ passcode
   ssh retry-count 10 retry-timer 120
MS(config-pki-scep-config)# fingerprint view
CA Certificate Fingerprint : 9b9651bb 290dc9e0
   75c8030d 0d92606c
MS(config-pki-scep-config)# fingerprint accept
MS(config-pki-scep-config)# enroll local-subject
   "C=US,O=MegistoRock,OU=Lab,CN=Candi" Current CA and
   Local identity certificates (if any) will be
   deleted, proceed (yes|no) : yes
```

Displaying Digital Certificates

You can display information about all or specified digital certificates via the **`show ipsec cert-file`** command. To view certificates use **`show ipsec certificate`**.

You can display information about certificates retrieved via PKI with the **`show pki enrollment-status`** and **`show pki scep-config`** commands.

Index