

NN10279-111

Multimedia Communication Portfolio

Multimedia Communication Server 5100

Accounting Module Basics

MCS 5100 2.0 Standard (02.02) February 2004



Overview

How this chapter is organized

This chapter is organized as follows:

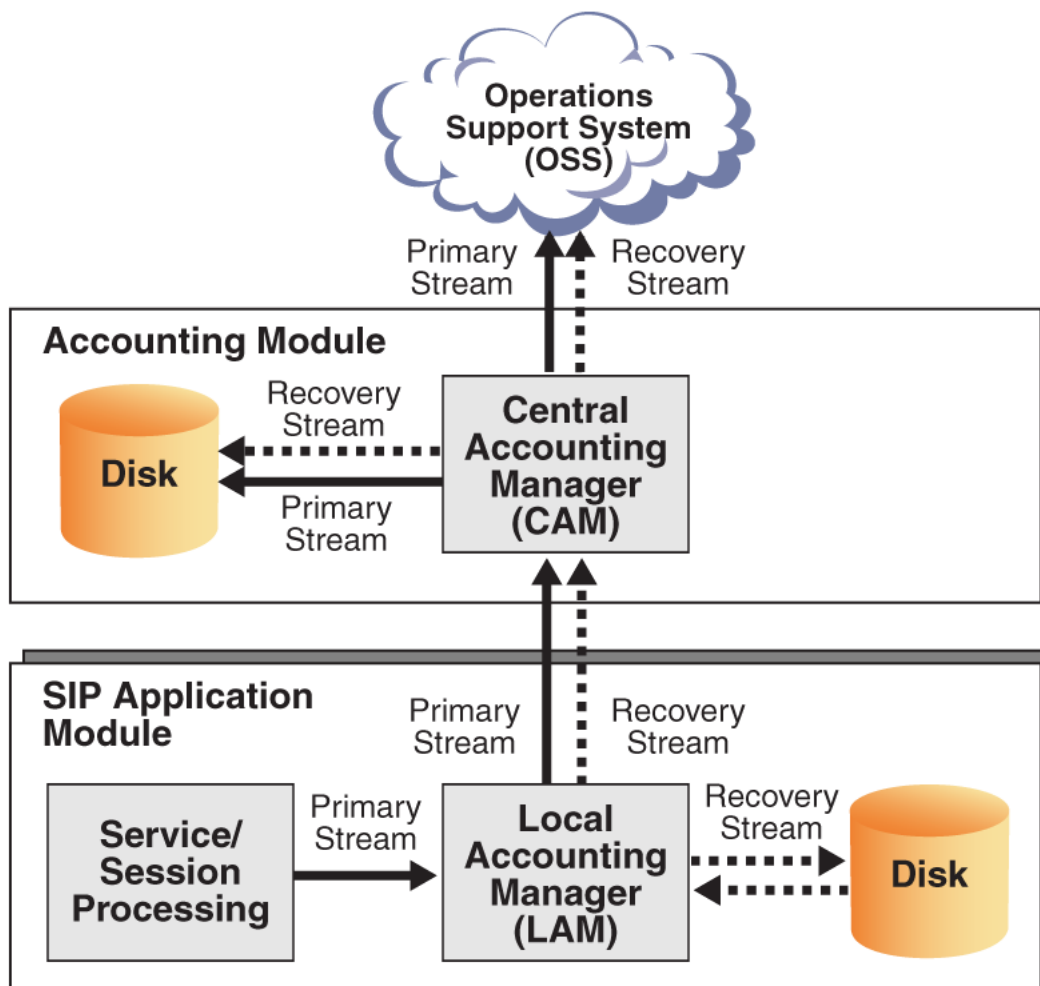
- [Functional description on page 3](#)
 - [Local Accounting Manager \(LAM\) on page 4](#)
 - [Central Accounting Manager \(CAM\) on page 5](#)
 - [Accounting terminology on page 7](#)
- [Architecture on page 9](#)
 - [Non-redundant architecture on page 10](#)
 - [Redundant architecture on page 10](#)
- [Hardware on page 12](#)
- [Software on page 12](#)
- [Tools and utilities on page 13](#)

Functional description

The Accounting Module provides a framework that enables the transport of accounting information from the network to a customer's back-end billing system. The accounting system is comprised of two logically distinct entities:

- Local Accounting Manager (LAM), included within the SIP Application Module, and
- Central Accounting Manager (CAM), included within the Accounting Module.

[Figure 1, Accounting overview, on page 4](#) shows the general layout of the accounting system and how accounting data flows through the network.

Figure 1 Accounting overview

The following sections provide a high-level overview of the LAM and CAM.

Local Accounting Manager (LAM)

The primary function of the LAM is to collect, as specific events occur, raw accounting data from active sessions on the SIP Application Module and transport it to the CAM. The LAM transports blocks of raw accounting data to the CAM by way of two accounting streams—a primary stream (transportation of accounting data in near real-time) and a recovery stream (transportation of accounting data is not in near real-time). These streams are noted within [Figure 1, Accounting overview, on page 4](#).

When an active session passes accounting data to the LAM, it is packaged with available accounting data from other sessions into a

block of data. This block of accounting data is transported to the CAM through the primary stream. If the primary stream cannot transmit the accounting data quickly enough to the CAM (due to either communications problems or an exceedingly high traffic spike), then the LAM begins to store blocks of accounting data locally on disk. Once the communication path from the LAM to the CAM has been restored, transportation of the accounting data on the primary stream is resumed. At the same time, the recovery stream begins transporting the stored blocks of data on the LAM to the CAM as a low priority background task.

To ensure that no data is lost from the LAM to the CAM, the LAM retains a copy of all data sent to the CAM until it receives confirmation that the data has been successfully processed by the CAM. During extraneous periods of congestion, or extended communications outages, the LAM is able to store up to 24 hours worth of contiguous accounting data to local file storage.

**CAUTION**

The storage mechanism on the LAM is intended only as an emergency backup provision.

Central Accounting Manager (CAM)

The CAM is responsible for receiving the raw accounting data from the LAM, reformatting it, and saving the reformatted information onto the local file storage. After each block of received data is formatted and stored to disk, the CAM sends an acknowledgement to the LAM to indicate that the received data was successfully processed.

When the CAM receives a block of accounting data from the LAM, it reformats the raw data received into Internet Protocol Detail Record/Extensible Markup Language (IPDR/XML) accounting records. Based on the stream where the raw accounting data was received (primary or secondary), these formatted records are stored to a file within different directories on disk. For more information on these directories and the location of accounting files, please refer to [CAM output file directory on page 48](#). The CAM can be configured to compress the accounting files containing the accounting records for

optimum storage. In order to provide data integrity, the CAM never deletes accounting records.

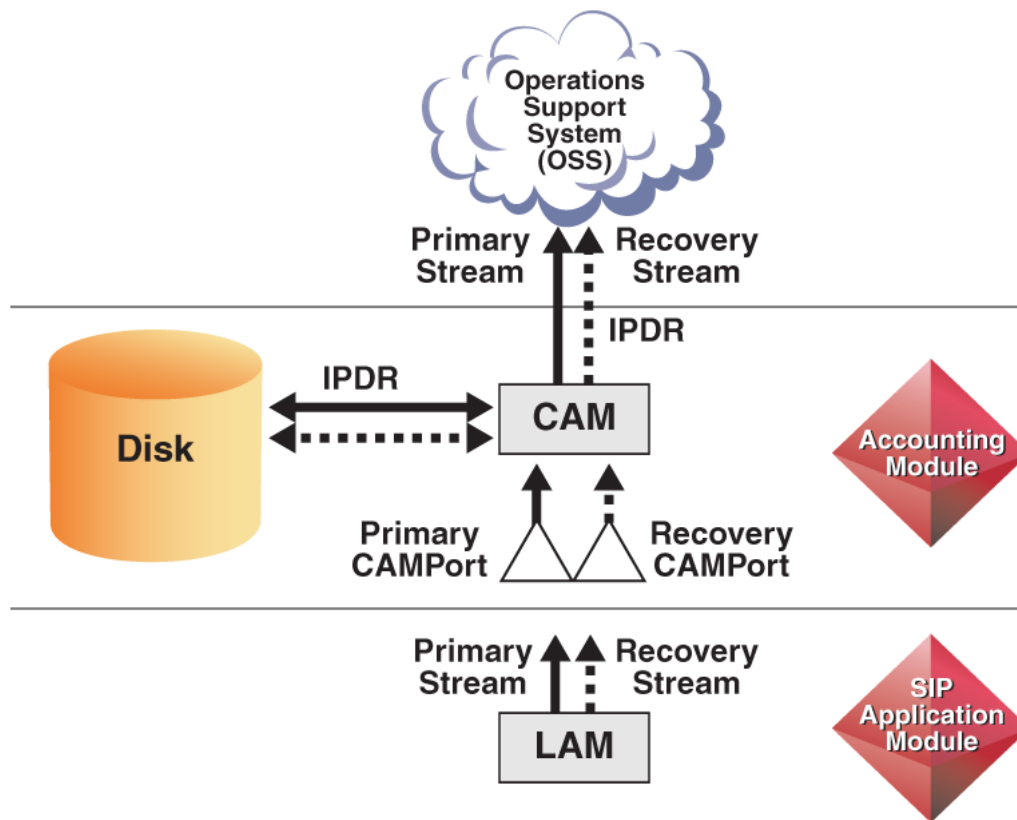
**CAUTION****Monitor the alarms.**

It is the responsibility of the customer to remove old accounting files to make room for new accounting data. There are threshold alarms that notify the user when running out of disk space.

The accounting records may also be optionally directed toward a downstream Operations Support System (OSS) through configuration of a near real-time TCP/IP connection and/or FTP connection (FTP push or FTP pull).

[Figure 2. CAM interfaces, on page 6](#) provides a graphical explanation of the CAM interfaces.

Figure 2 CAM interfaces



As mentioned previously, the accounting data received from the LAM on the primary stream is formatted, written to the local file storage of the CAM, and optionally sent to a downstream OSS. When the formatted accounting data is sent to the downstream OSS, it is considered to be a continuation of the primary stream. The same concept is true for the recovery stream.

Note: The primary and recovery stream accounting data being sent to the OSS is the same data which was received on these streams from the LAM. The primary and recovery streams to the OSS are not based on any communications loss to the OSS, but are always based on a communications loss between the LAM and the CAM.

The CAM can simultaneously receive accounting data from multiple LAMs. For each connected LAM, the CAM supports reception of both a primary and a recovery accounting data stream.



CAUTION

There is one LAM per SIP Application Module. It is recommended that the network is configured so that every LAM in the network deliver its data to the CAM.

Accounting terminology

Recording Units

As the LAM collects accounting data for events that occur during sessions, it stores the raw accounting data in Recording Units (RUs).

RU Blocks

At the same time that the LAM collects new RUs, it also places queued RUs into RU Blocks to send to the CAM.

Data Transport Protocol

A socket-based TCP/IP communication protocol is used for transmitting collected accounting data from the LAM in the SIP Application Module to the CAM in the Accounting Module. It also provides the appropriate acknowledgement of receipt of the data from the CAM back to the LAM. Both the primary and recovery stream use this protocol in order to transfer and confirm the transmission of the accounting data from the LAM to the CAM.

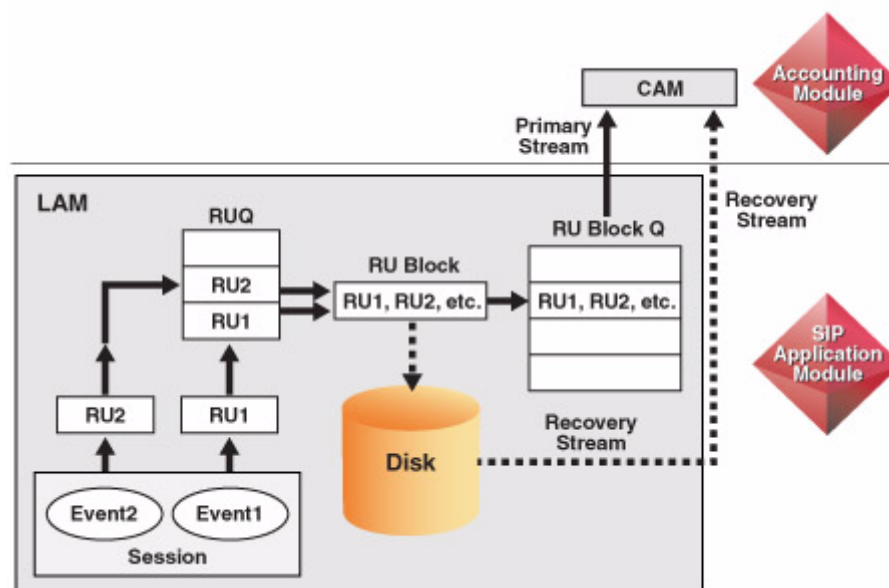
In the case of a communication loss between the LAM and the CAM, corresponding alarm and Operational Measurement (OM) information is captured. For more information regarding these alarms and OMs, please refer to *MCS 5100 System Management Console User Guide*.

Service/Session Processing

Service/Session processing collects raw accounting data in the SIP Application Module as specified service events occur during a SIP session (i.e. multimedia call). This raw accounting data is passed in the form of Recording Units (RUs) to the LAM for transport to the CAM. The LAM places the RUs into RU Blocks and transports the RU Blocks to the CAM. This near real-time data transfer constitutes the primary accounting stream from the LAM to the CAM.

[Figure 3, LAM flow, on page 8](#) provides a graphical explanation of the LAM internal workings.

Figure 3 LAM flow



If there is a loss of communication between the LAM and the CAM or an exceedingly high traffic spike, then RU Blocks are stored locally to disk on the server where the SIP Application Module resides. Once communication between the LAM and the CAM is restored, the LAM resumes sending the RU Blocks along the primary stream. Simultaneously, the RU Blocks that were previously saved to the local file storage during the outage are sent along the recovery stream. The recovery stream to the CAM has a lower priority than the primary stream.

After the CAM acknowledges successful processing (receipt, translation and storage) of an RU Block, the LAM removes the corresponding copy of the RU Block at the LAM. This applies to both the primary and recovery streams.

Local file storage

When there is a communication loss from the LAM to the CAM and the local file storage that stores the RU Blocks is exceeded, a `diskAccessFailure` alarm is raised and all subsequent RUs are discarded.

When the local file storage for the CAM is exceeded, a `diskAccessFailure` alarm is raised and the CAM does not send an acknowledgement of the data to the LAM. Due to this non-acknowledgement, the LAM stores this accounting data to its local file storage until the situation is resolved or the LAM's local file storage is depleted.

There are two configurable alarm thresholds on the LAM and the CAM to warn of the onset of local file storage becoming full. These thresholds determine the conditions for when the following alarms are raised on the appropriate component:

- `DiskMonMajor` alarm - indicates when the local file storage is getting low.
- `DiskMonCritical` alarm - indicates when the local file storage is severely depleted.

In addition to the alarms discussed above, performance metrics are also updated regarding the ability to save accounting data to local file storage. These metrics are shown within the Operational Measurements (OMs) for the LAM and CAM as follows:

- LAM Operational Measurements
 - `percentageusedisk`
 - `diskaccessfailurecount`
- CAM Operational Measurements
 - `campercentdiskuse`
 - `amdiskfailurecount`

For more information regarding these alarms and OMs, please refer to *MCS 5100 System Management Console User Guide*.

Architecture

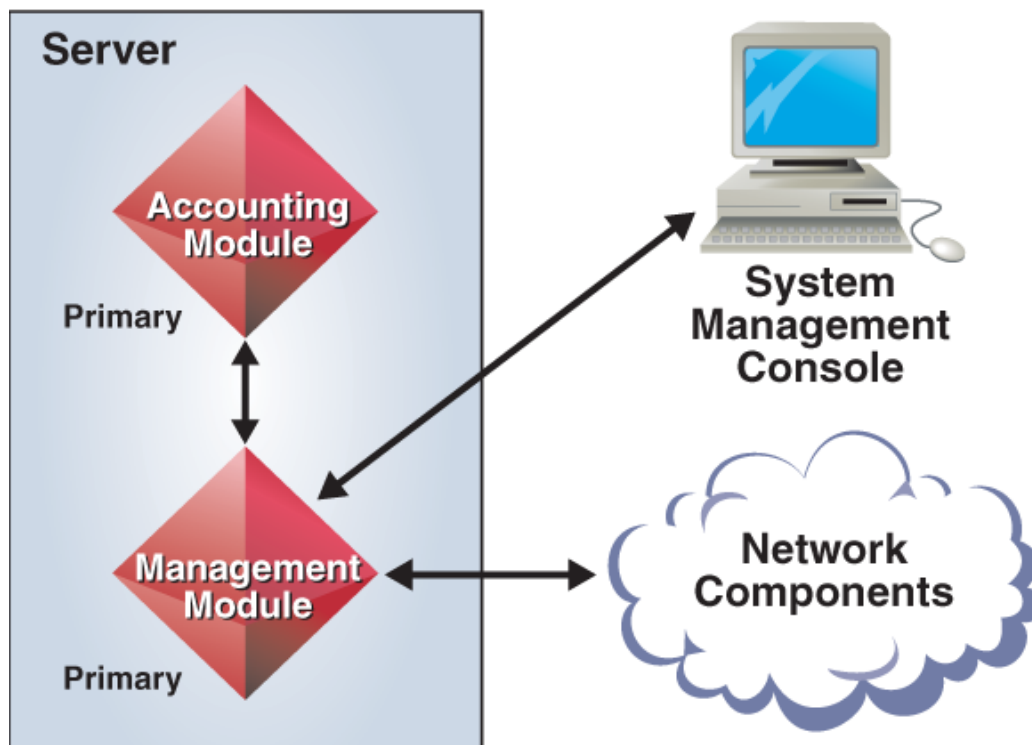
Depending on whether redundancy is required within the network, there are two different ways to architect the Accounting Module functionality.

Non-redundant architecture

In a non-redundant architecture, the Accounting Module is deployed on a single server. In this architecture, there is no failover of the Accounting Module since there is no secondary Accounting Module.

In addition, the same server is configured to host the Management Module component. A graphical representation of a non-redundant architecture can be found in [Figure 4. Non-redundant configuration, on page 10.](#)

Figure 4 Non-redundant configuration



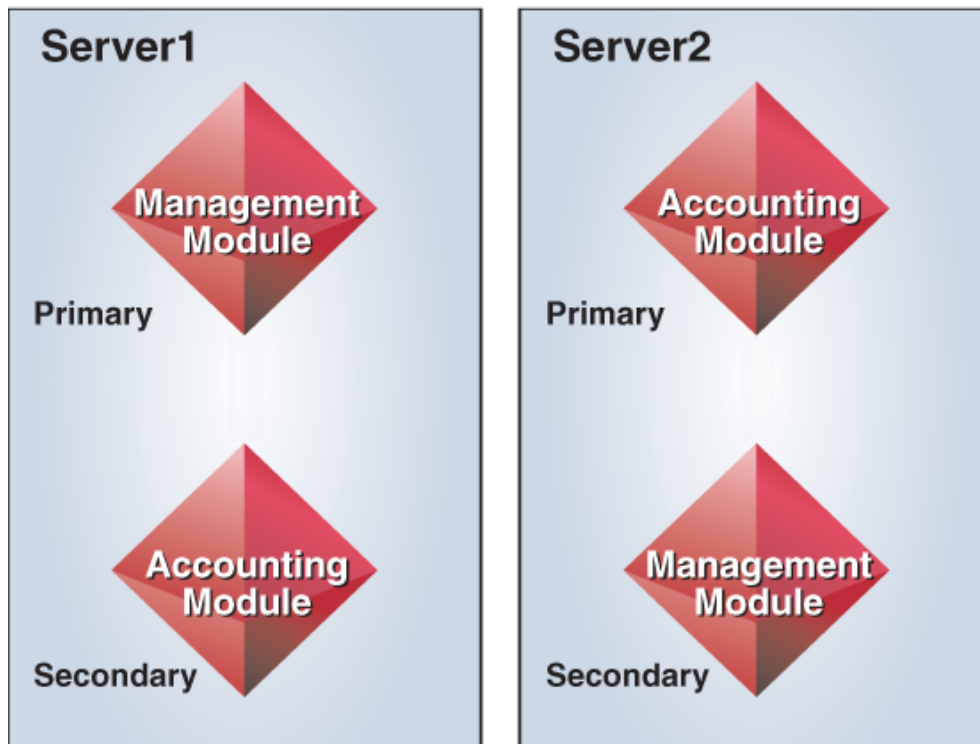
Redundant architecture

In a redundant architecture, the Accounting Module is deployed similarly as it is in a non-redundant architecture, except with two servers. In this architecture, one instance of the Accounting Module resides on one server and acts as the primary instance; while another instance resides on a second server and acts as the secondary instance.

In addition, these two servers also host two instances of the Management Module. In order to balance the load between these two components on each of the servers, the secondary instance of one component always resides on the server hosting the primary instance

of the other component. Please refer to [Figure 5, Redundant configuration, on page 11](#) for a graphical representation.

Figure 5 Redundant configuration



Hardware

The Accounting Module is deployed on either of the following hardware servers detailed in [Table 1, Hardware details, on page 12](#).

Table 1 Hardware details

Hardware	Details
Sun Netra* t 1400 or Sun Netra* t 1405 	The server has the following hardware features: • 4 440 Mhz CPUs • 4 GB RAM • 4 36 GB Disks • 10x Internal DVD-ROM drive • 20 GB 4mm DDS-4 Internal Tape Drive • 1 Quad Fast Ethernet (QFE) PCI card • 1 Netra* t alarm card • Universal Sliding Rack Mount Kit • t 1400 model is DC-powered; t 1405 model is AC-powered
Sun Fire* v100 	The server has the following hardware features: • UltraSparc Ili 550 Mhz Processor • 512 KB On-Chip L2 cache • 1 GB RAM (4 @ 256 MB DIMMS) • 2 40 GB IDE disk drives @ 7200 RPM • 24X CD-ROM drive • 2 10/100BASE-T Ethernet ports • 2 USB ports • 2 RS-232C/RS-423 serial ports • Universal Sliding Rack Mount Kit

Software

Information on updating the Accounting Module to a new maintenance release is covered in [Upgrades on page 15](#).

Tools and utilities

Both the CAM and LAM are configured through the System Management Console which is the interface to the Management Module. For more information regarding the System Management Console, please refer to *MCS 5100 System Management Console User Guide*.

CAM properties are configured within the Central Accounting Manager tab for the Accounting Module using the System Management Console. LAM properties are configured within the Local Accounting Manager tab for the SIP Application Module within the System Management Console.



Upgrades

How this chapter is organized

This chapter is organized as follows:

- [Functional description on page 15](#)
- [Tools and utilities on page 15](#)
- [OAM&P strategy on page 16](#)
- [Task flows on page 16](#)
 - [Updating the Accounting Module component in a non-redundant architecture on page 16](#)
 - [Updating the Accounting Module component in a redundant architecture on page 20](#)

Functional description

This chapter documents upgrade tasks that can be performed when upgrading to a maintenance release. For information on upgrading to a full release, please refer to *MCS 5100 Installation, Commissioning, and Upgrade Guide*.

Tools and utilities

Maintenance updates (both upgrades and downgrades) to the Accounting Module are performed through the use of the System Management Console. Please refer to *MCS 5100 System Management Console User Guide* for more information.

The update operation on the System Management Console allows administrators to either upgrade the Accounting Module component to future maintenance releases, or downgrade the Accounting Module component to a previous maintenance release.

OAM&P strategy

The update operation has the following characteristics:

- does not impact stable calls.
- introduces new functionality.

Note: If an upgrade fails before or during the initial stages of the upgrade, a rollback to the previous load is performed. A notification of the failure appears within the System Management Console. If a component upgrade fails after the initial stages of the upgrade, it does not roll back automatically. A dialog box appears stating the upgrade failed and prompts the administrator to determine whether a rollback should be performed.

Task flows

Updating the Accounting Module component in a non-redundant architecture

As part of the update operation, the Accounting Module is temporarily shutdown. When the Accounting Module is shutdown, the LAM and the CAM lose communication. Due to this communication loss, the LAM begins storing blocks of accounting data to local file storage. When the updated Accounting Module returns to active status and communication is restored, the LAM transports the stored blocks of data to the CAM through the recovery stream. For more information, please refer to [Local Accounting Manager \(LAM\) on page 4](#).

Maintenance updates should be performed as described in the following procedure:

Note 1: The LAM is updated along with the SIP Application Module. Please refer to the *MCS 5100 SIP Application Module Basics* for more information on updating the SIP Application Module component.

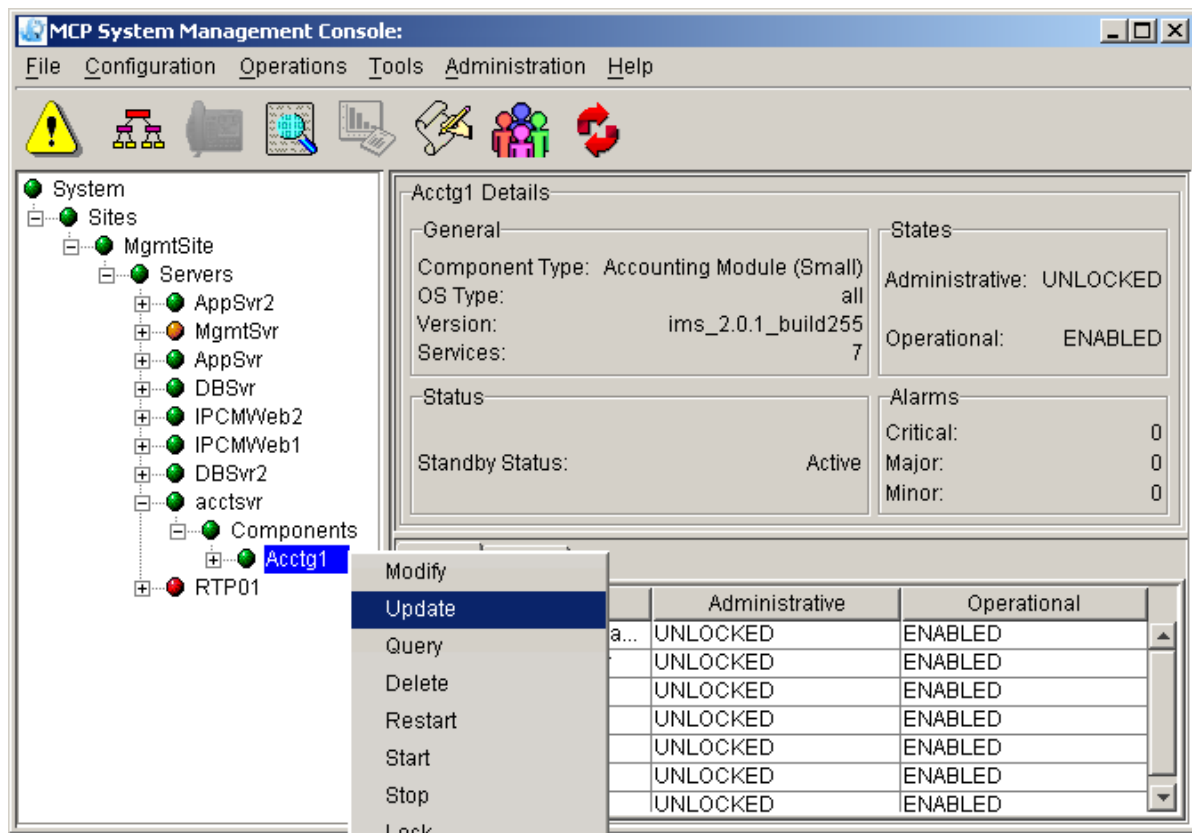
Note 2: Updates (both upgrades and downgrades) to network components must be performed in a specific order. Please refer to *MCS 5100 Basics* for further information.

From the System Management Console

- 1 In the System tree, right-click on the appropriate Accounting Module component.

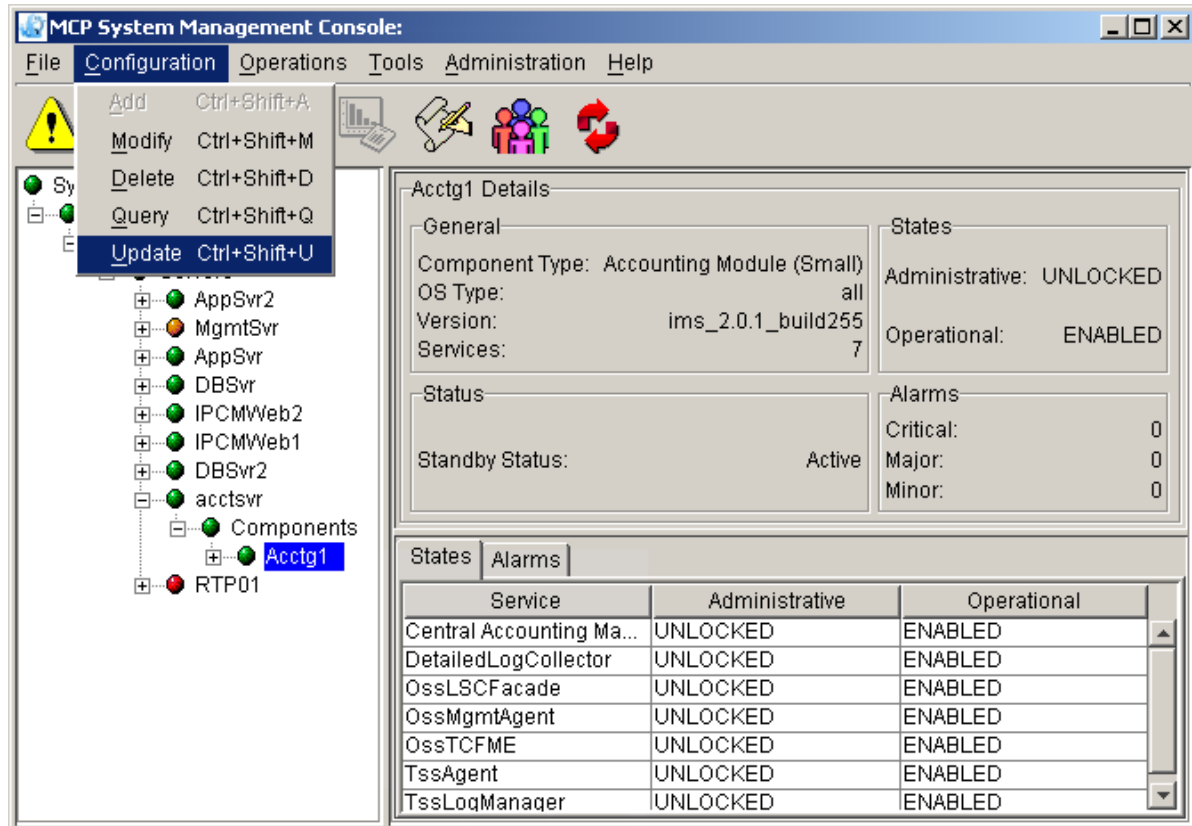
- 2 From the pop-up menu, select the **Update** command.

Figure 6 Update from the pop-up menu



You can also launch the update command from the pull-down Configuration menu.

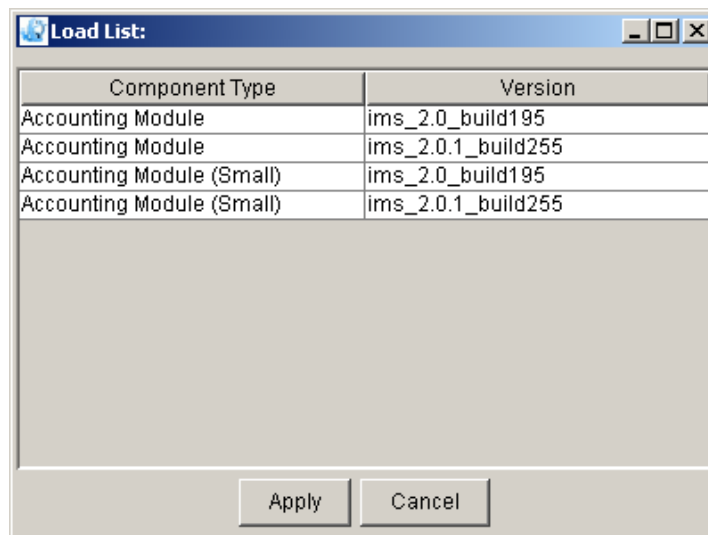
Figure 7 Update from the Configuration menu



3 After **Update** is selected, the following window appears:

Figure 8 Retrieving Load list window

- 4 The Load List window appears. The window only shows software loads intended for the Accounting Module component type, since this is the component type being updated.

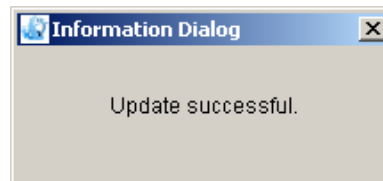
Figure 9 Load list for updating

- 5 Select the load version that should be used to update the Accounting Module. Click on the **Apply** button.
- 6 The System Management Console displays the Accounting Module configuration window with the CAM configuration properties. If required, modify any configuration properties. For a description of these properties, please refer to [Table 2.](#)

[Configuration properties of the CAM, on page 36](#). Click on the **Apply** button.

- 7 A window showing the progress of the update appears. Once the update has completed, the following window appears showing that the Accounting Module component was successfully updated.

Figure 10 Successful update dialog box



Updating the Accounting Module component in a redundant architecture

To prevent service interruption, the following steps should be performed, in order, when updating the Accounting Module component in a redundant architecture:

- 1 Ensure that both Accounting Modules are working under normal operating conditions (i.e. the primary Accounting Module is the active instance while the secondary Accounting Module is the cold standby instance).
- 2 Update the secondary instance of the Accounting Module. This procedure is the same as updating the Accounting Module component in a non-redundant architecture. Please refer to the procedure found in [Updating the Accounting Module component in a non-redundant architecture on page 16](#).
- 3 Perform a manual failover so that the secondary instance of the Accounting Module becomes the active instance and the primary instance goes into a cold standby state. Please refer to the procedure found in [Failover to the secondary Accounting Module on page 24](#) for the manual failover procedure.
- 4 Update the primary instance of the Accounting Module. Please refer to the procedure found in [Updating the Accounting Module component in a non-redundant architecture on page 16](#).
- 5 Perform a manual failover so that the primary instance of the Accounting Module goes back to being the active instance and the secondary instance goes into a cold standby state. Please refer to the procedure found in [Failover back to the primary Accounting Module on page 25](#) for the manual failover procedure.



Fault management

How this chapter is organized

This chapter is organized as follows:

- [Network fault management strategy on page 21](#)
- [Failure strategy within a non-redundant architecture on page 21](#)
- [Failure strategy within a redundant architecture on page 21](#)
 - [Failover to the secondary Accounting Module on page 24](#)
 - [Failover back to the primary Accounting Module on page 25](#)

Network fault management strategy

The system handles network fault management through alarms and logs. Accounting alarms and logs occur on both the Local Accounting Manager and the Central Accounting Manager. Both CAM and LAM alarms and logs are viewed from the System Management Console. Please refer to *MCS 5100 System Management Console User Guide* for detailed information relating to alarms and logs.

Failure strategy within a non-redundant architecture

In a non-redundant architecture, there is only one instance of the Accounting Module component present on a single server. If any failure occurs, it is recommended that your next level of support be contacted.

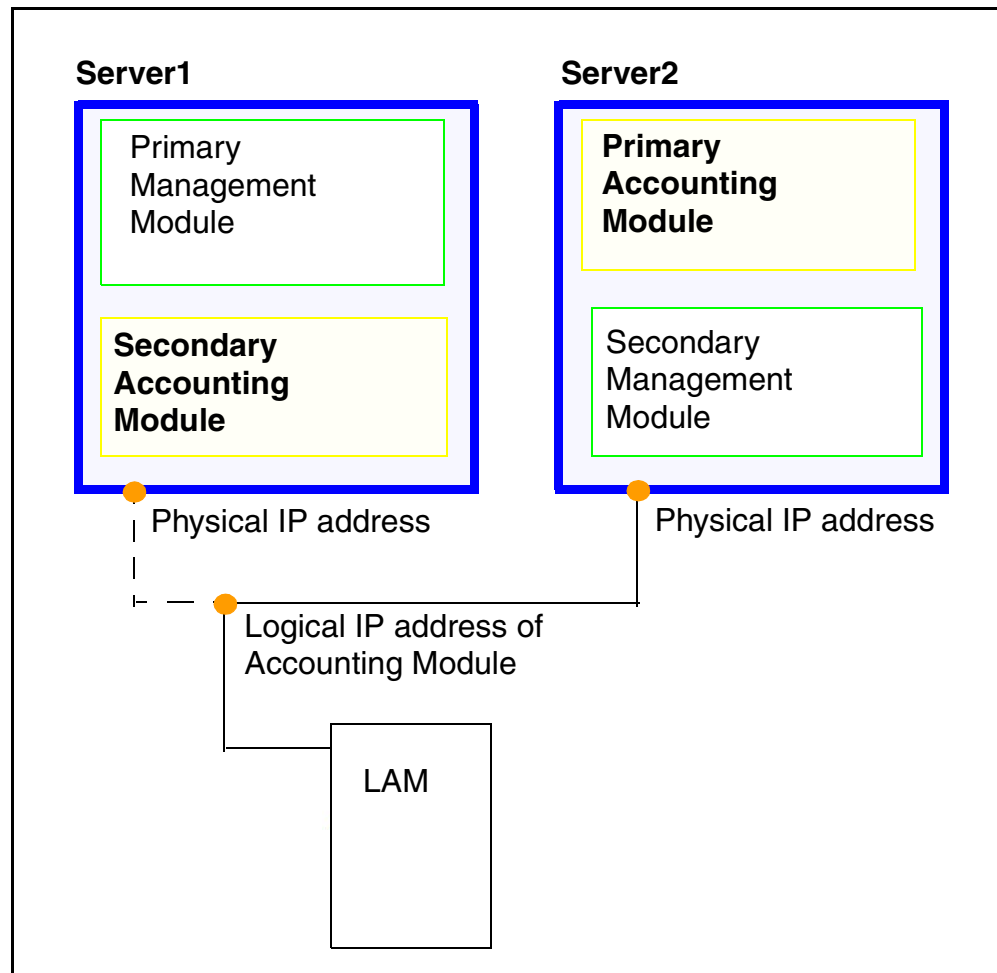
Failure strategy within a redundant architecture

In a redundant architecture, there are two instances of the Accounting Module component present on two separate servers: one is designated as the primary instance, and the other is designated as the secondary instance. Additionally, these two servers are also configured to host two instances of the Management Module. For more information, please refer to [Redundant architecture on page 10](#).

Having two instances of the Accounting Module and Management Module components ensures the high availability of these two fundamental system components. If the server containing the primary

Accounting Module fails, a manual failover allows the transfer of Accounting Module activity to the secondary instance waiting on the server containing the primary Management Module. Similarly, if the server containing the primary Management Module fails, a manual failover allows the transfer of Management Module activity to the secondary instance on the server containing the primary Accounting Module.

Both servers running the two instances of the Accounting Module have their own physical IP address. However, in order to provide a failover mechanism for the Accounting Module that is transparent to the LAM (i.e. with no configuration changes), the concept of a logical IP address is used. The LAM is configured to connect to a logical IP address which is associated with the active instance of the CAM. This logical IP address identifies the active instance of the Accounting Module and is independent of a physical server, actually migrating from one physical server to the other as conditions dictate. During a manual failover, the logical IP address is updated in order to identify the currently active instance after failover occurs. A logical view of this arrangement is shown in [Figure 11, Redundancy of Accounting Module - logical view, on page 23](#).

Figure 11 Redundancy of Accounting Module - logical view

If the primary instance of the Accounting Module component goes down, the LAM implicitly loses its connection to the CAM. In this case, the LAM begins queuing accounting data and (if the problem persists) storing accounting data to its local file storage. To resolve this fault, an administrator needs to perform a manual failover to the secondary instance of the Accounting Module (installed on another server). The manual failover process involves the following:

- stopping the primary instance of the Accounting Module
- releasing the associated logical IP address from the primary instance
- stopping the secondary instance of the Accounting Module
- assigning the logical IP address to be the secondary instance
- restarting the secondary instance of the Accounting Module

Failure of the Central Accounting Manager (CAM) will typically be indicated by alarms. There may also be alarms from one or more Local Accounting Managers (LAMs) executing on the SIP Application Module component.

Failover to the secondary Accounting Module

Failover for the Accounting Module component is a manual process that should take only minutes to execute.

ATTENTION

For any failure, contact your next level of support to debug the root cause of the failure.

From the administrator workstation

To stop the primary Accounting Module:

- 1 If possible, establish a remote login session to the server hosting the primary instance of the Accounting Module. Login in as **sysadmin**.

Note: If it is not possible to establish a remote login session to the server, you still need to run the failover script as soon as connectivity to the server is possible.

- 2 type: **cd /IMS/acctmgr/bin**

- 3 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl stop acctmgr**

This will ensure that the Accounting Module is placed in cold standby mode. If the process is still running it will be shut down, the logical IP will be unassigned and the process will be restarted. Since it is now in cold standby mode it will not receive data.

To start the secondary Accounting Module:

- 4 Establish a remote login session to the server hosting the secondary Accounting Module. Login in as **sysadmin**.

- 5 type: **cd /IMS/acctmgr/bin**

- 6 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine and the Accounting Module process restarted.

Impacts and recovery

The Accounting Module component is no longer running on the preferred server. If the active Accounting Module and the active Management Module are running on the same server, it may result in degraded capacity of the Accounting Module. To avoid any capacity problems, a failover back to the primary Accounting Module should be performed as soon as the primary instance is available.

When the primary Accounting Module is manually failed over to the secondary instance, raw accounting data currently being processed on the primary instance will be stored persistently to disk (either on the server hosting the primary Accounting Module or the server hosting the SIP Application Module). If formatting was completed prior to the failover, the record will appear in the accounting file on the server where the primary Accounting Module was deployed. If the raw accounting data was not formatted, the CAM would not have sent an acknowledgement to the LAM. Thus, the LAM would store the raw accounting data on the server where the SIP Application Module was deployed. For more information on the acknowledgement and backup storage on the LAM, please refer to [Service/Session Processing on page 8](#).

**CAUTION**

When a manual failover occurs, the accounting file is not closed. In this situation, the accounting file extension is marked as “.incomplete” to indicate that the IPDRDoc.End element (including its attributes) and closing IPDRDoc information will need to be added manually to the accounting file before processing.

During a manual failover, the accounting files previously stored on the primary instance will remain on the server hosting that instance. No accounting files are transferred between the Accounting Module instances, or their servers, as part of the manual failover process.

Failover back to the primary Accounting Module

Restoring the primary Accounting Module to active status is a similar process as that described in the last section. The main difference is that no failure has occurred and the failover is being performed in order to

return the instances of the Accounting Module back to their normal, preferred states.

**CAUTION**

This action will interrupt the communication link between the CAM and the LAM, temporarily forcing the LAM into a failure recovery mode of operation.

From the administrator workstation**To stop the secondary Accounting Module:**

- 1 Establish a remote login session to the server hosting the secondary instance of the Accounting Module. Login in as **sysadmin**.
- 2 type: **cd /IMS/acctmgr/bin**
- 3 Use the sudo command to execute the failover script using the following syntax:

type: **sudo Failover.pl stop acctmgr**

The process will be shut down, the logical IP will be unassigned and the process will be restarted. It is now in cold standby mode and it will not receive data.

To start the primary Accounting Module:

- 4 Establish a remote login session to the server hosting the primary Accounting Module. Login in as **sysadmin**.
- 5 type: **cd /IMS/acctmgr/bin**
- 6 Use the sudo command to execute the Failover script using the following syntax:

type: **sudo Failover.pl start acctmgr**

The process will be stopped, the logical IP will be assigned for this machine, and the Accounting Module process restarted.

Accessing accounting data on the Cold Standby Accounting Module

There should not be any changes to FTP access to accounting files on the Accounting Module component when it is running in cold standby mode.

Impacts and recovery

Since the process for restoring the primary Accounting Module component is similar to the manual failover, it has the same impact to the raw accounting data being processed on the secondary Accounting Module. For the details of these impacts, refer to [Impacts and recovery on page 25](#).



Configuration management

How this chapter is organized

This chapter is organized as follows:

- [Tools and utilities on page 29](#)
- [OAM&P strategy on page 29](#)
- [Task flows on page 31](#)
 - [Adding the Accounting Module component on page 31](#)
 - [Querying or modifying Accounting Module configuration properties on page 40](#)
 - [Configuring the LAM on the SIP Application Module on page 42](#)

Tools and utilities

Deployment and configuration of the Accounting Module is performed through the use of the System Management Console. Please refer to *MCS 5100 System Management Console User Guide* for more information.

The add operation on the System Management Console allows administrators to initially deploy and configure the Accounting Module component. The query operation is used for viewing configuration property values. The modify operation is used for changing the values of configuration properties any time after initial deployment.

OAM&P strategy

The accounting system is configured during the deployment of the Accounting Module (CAM) and SIP Application Module (LAM) components.

Accounting Module properties are configured under the Central Accounting Manager tab on the Accounting Module within the System Management Console and cannot be modified in real-time.

The CAM is configured for:

- Data Transport Protocol
 - CAM IP address
 - Primary CAM port
 - Recovery CAM port
- file management
 - file rotation size
 - file rotation time
 - file compression
- disk full condition
 - disk monitor major threshold
 - disk monitor critical threshold
- TCP/IP transport to OSS
 - TCP/IP enabled
 - TCP/IP address
 - TCP/IP primary host port
 - TCP/IP recovery host port
- FTP transport to OSS
 - FTP push enabled
 - primary FTP directory
 - recovery FTP directory
 - remote FTP node ID
 - FTP user ID
 - FTP user password

Local Accounting Manager properties are configured under the Local Accounting Manager tab for the SIP Application Module within the System Management Console and cannot be modified in real-time. For further information, refer to the *MCS5100 SIP Application Module Basics*.

The LAM is configured for:

- file management
 - file rotation size
 - file rotation time
- disk full conditions
 - disk monitor major threshold
 - disk monitor critical threshold

Task flows

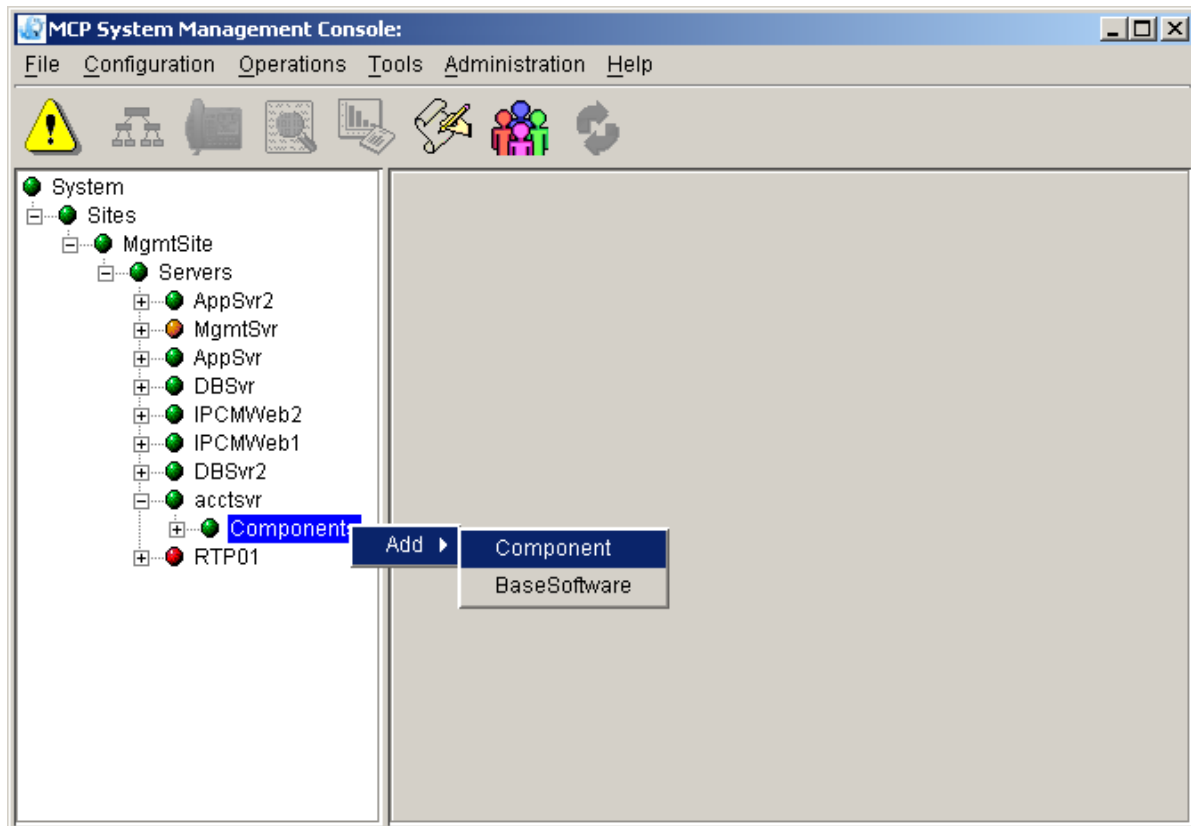
The following sections provide procedures on configuring the Accounting Module component and LAM portion of the SIP Application Module component. To perform these procedures, the administrator should login to the System Management Console. For detailed procedures on logging into the System Management Console, please refer to *MCS 5100 System Management Console User Guide*.

Adding the Accounting Module component

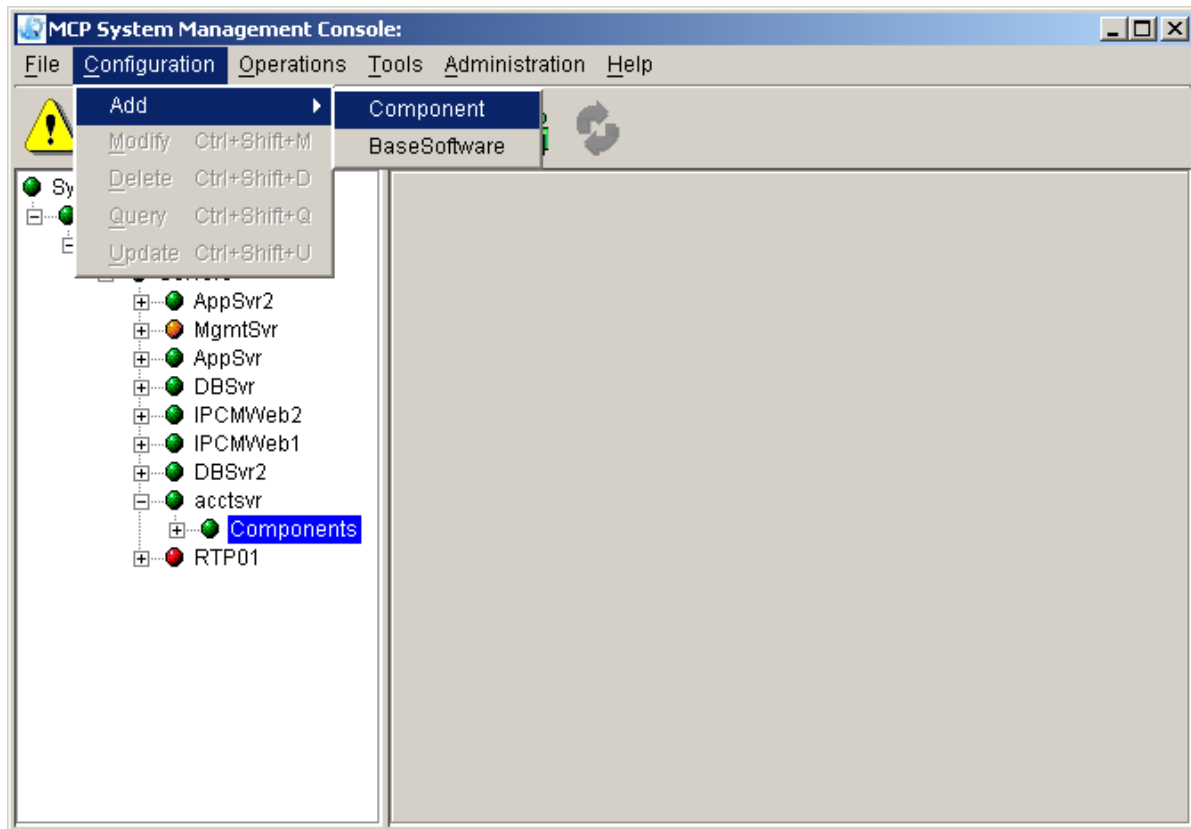
This procedure assumes that the server on which the Accounting Module component will be added has already been configured. For example, [Figure 12, Add from the pop-up menu](#) shows the Accounting Module component being deployed onto a previously configured server, named “AcctSvr1”.

From the System Management Console

- 1 In the System tree, right-click **Components** under the appropriate server where the Accounting Module is to be deployed.
- 2 From the pop-up menu, select **Add > Component** command.

Figure 12 Add from the pop-up menu

You can also launch the add from the pull-down Configuration menu.

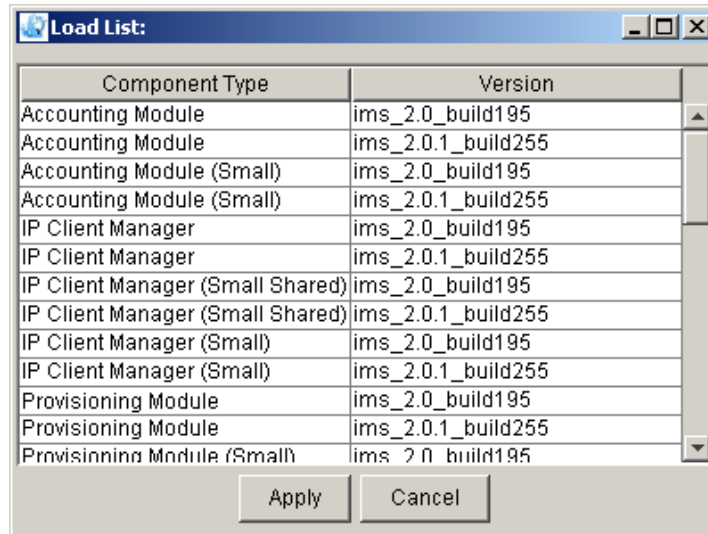
Figure 13 Add from the Configuration menu

- 3 After **Add > Component** is selected, the following window appears:

Figure 14 Retrieving Load list window

- 4 The Load List window appears with all available component loads (except for those components already deployed to the server).

Figure 15 Load list for adding



- 5 Select the desired software load version for the Accounting Module. Click on the **Apply** button.
- 6 You will be prompted to configure the Accounting Module through the Central Accounting Manager tab and properties. For a description of these properties, please refer to [Configuration properties of the CAM on page 36](#).

Figure 16 CAM configuration tab

Central Accounting Manager

* CAM IP Address : 0.0.0.0

* Primary CAM Port : 17667

* Recovery CAM Port : 17668

* File Rotation Size : 100000

* File Rotation Time : 20000

* File Compression : ☐

* Disk Monitor Major Threshold : 50

* Disk Monitor Critical Threshold : 75

* TCP/IP Enabled : ☐

TCP/IP IP Address : 0.0.0.0

TCP/IP Primary Host Port : 9000

TCP/IP Recovery Host Port : 9001

* FTP Push Enabled : ☐

Primary FTP Directory :

Recovery FTP Directory :

Remote FTP Node ID : 0.0.0.0

FTP User ID :

FTP USER Password :

Reset

Service Component Name:

Apply Cancel

The table below describes the configuration properties of the CAM:

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	The Logical IP address for the Accounting Module that would be written into the IPDR. Note: The default value must be updated in order for the functionality to work correctly.
Primary CAM Port	Type: Integer Range: 1025-65535 Default: 17667	Designates the network communications port number on the Accounting Module used by the Primary Stream. Note: The default value is recommended.
Recovery CAM Port	Type: Integer Range: 1025-65535 Default: 17668	Designates the network communications port number on the Accounting Module used by the Recovery Stream. Note: The default value is recommended.

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
File Rotation Size	Type: Integer (bytes) Range: 0 (disabled) 1-300000 Default: 100000	Designates the maximum file size allowable for accounting files to reach - after which file rotation takes place. A value of zero indicates no rotation based on file size. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
File Rotation Time	Type: Integer (milliseconds) Range: 0 (disabled), 1-3600000 (1 millisecond to 60 minutes) Default: 20000 (20 seconds)	Designates the maximum time interval for rotating accounting files from active to closed. A value of zero indicates no rotation based on time. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
File Compression	Type: Boolean Range: True/False Default: False	Enables/disables compression of the IPDR formatted accounting information. The compressed files are stored with a ".zip" extension.

Table 2 Configuration properties of the CAM

CAM Field name	Format	Description
Disk Monitor Major Threshold	Type: Integer Range: 0-100 Default: 50	Percentage of the accounting partition that can be used before a DiskMajorAlarm is raised. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
Disk Monitor Critical Threshold	Type: Integer Range: 0-100 Default: 75	Percentage of the accounting partition that can be used before a DiskCriticalAlarm is raised. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
TCP/IP Enabled	Type: Boolean Range: True/False Default: False	Enable/disable TCP/IP stream.
TCP/IP IP Address	Type: String Range: N/A Default: 0.0.0.0	Hostname or IP address of the destination server that will be receiving the TCP/IP stream. Note: The default value must be updated in order for the functionality to work correctly.
TCP/IP Primary Host Port	Type: Integer Range: 1025-65535 Default: 9000	The TCP port on the destination server that will receive the near-real-time flow for the Primary Stream accounting information.

Table 2 Configuration properties of the CAM

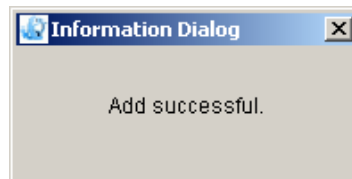
CAM Field name	Format	Description
TCP/IP Recovery Host Port	Type: Integer Range: 1025-65535 Default: 9001	The TCP port on the destination server that will receive the flow for the Recovery Stream accounting information.
FTP Push Enabled	Type: Boolean Range: True/False Default: False	Specifies whether or not automatic FTP transfer is enabled.
Primary FTP Directory	Type: String Range: 1-500 characters Default: N/A	Specifies the top-level directory on the remote FTP server where the IPDR files should be stored for the Primary Stream.
Recovery FTP Directory	Type: String Range: 1-500 characters Default: N/A	Specifies the top-level directory on the remote FTP server where the IPDR files should be stored for the Recovery Stream.
Remote FTP Node ID	Type: String Range: 1-500 characters Default: 0.0.0.0	Specifies the hostname for the destination server of the FTP stream. Note: The default value must be updated in order for the functionality to work correctly.
FTP User ID	Type: String Range: 1-500 characters Default: N/A	Specifies the login name for the remote host for FTP transfers.
FTP User Password	Type: String Range: 1-500 characters Default: N/A	Specifies the password used for FTP transfers.

- 7** After entering the appropriate configuration information, enter a label (six characters or less) in the Service Component Name field. This label is the name that appears in the System tree.

Click on the **Apply** button. A progress screen appears while it deploys.

- 8 When deployment completes, there is a screen showing that the component was added successfully.

Figure 17 Add Successful dialog box



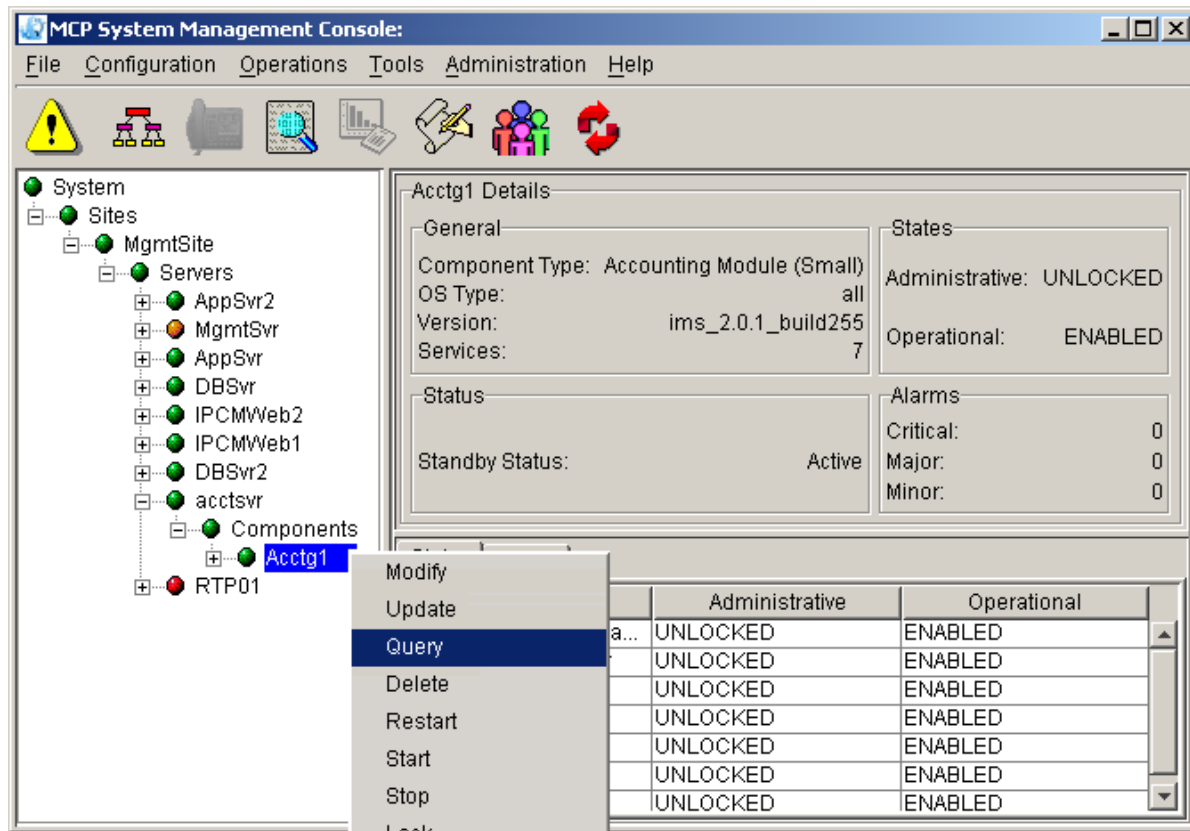
- 9 Within a redundant architecture, repeat this procedure to add the secondary Accounting Module to another server.

Querying or modifying Accounting Module configuration properties

Use the following procedure to query or modify the configuration properties for the Accounting Module component:

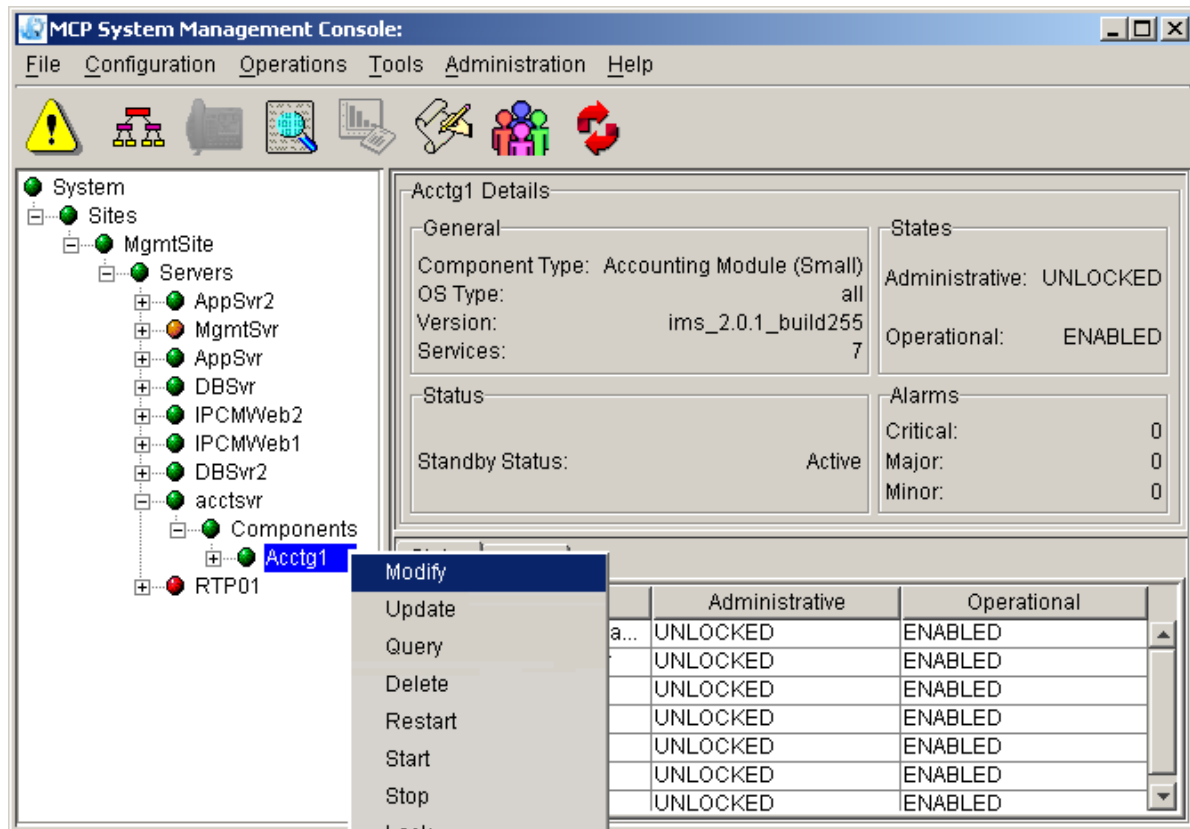
From the System Management Console

- 1 In the System tree, find the appropriate Accounting Module component to be queried or modified.
Note: In a redundant architecture, there are two Accounting Modules deployed.
- 2 To query the configuration properties, right-click the root level Accounting Module component and select **Query**.

Figure 18 Query Accounting Module configuration properties

The Query Accounting Module window displays the properties. However, no configuration changes are permitted in the window.

- 3 To modify the configuration properties of an Accounting Module component, do the following:
 - a Right-click the root level Accounting Module component and click **Lock** to lock the component while you modify the settings.
 - b A confirmation dialog box prompts you to confirm that you want to lock the Accounting Module. Click **Yes**.
 - c Right-click the root level Accounting Module component and click **Modify**.

Figure 19 Modify Accounting Module configuration properties

- d Modify the properties as required and click **OK**. For information on the configuration properties, please refer to [Table 2. Configuration properties of the CAM, on page 36.](#)

Configuring the LAM on the SIP Application Module

When adding or modifying a SIP Application Module component, LAM configuration is required. For more details on how this is achieved, as well as how to query configuration information for the SIP Application Module, refer to *MCS 5100 SIP Application Module Basics*. [Figure 20. LAM configuration tab, on page 43](#) shows the LAM properties requiring configuration during the addition or modification of a SIP Application Module component.

Figure 20 LAM configuration tab

Authentication	Data Synchronization	Long Call Service	Overload Controls
SIP TCF Base	Registration	SipFwdAdapter	Prov Sync Service
Database Base	Presence	Application Server	Server Properties
Local Accounting Manager	In Memory Database	Media Portal	Location Service Manager

* Primary CAM IP Address :	0.0.0.0
* Primary CAM Port :	17667
* Recovery CAM IP Address :	0.0.0.0
* Recovery CAM Port :	17668
* File Rotation Size :	100000
* File Rotation Time :	300
* Disk Monitor Major Threshold :	50
* Disk Monitor Critical Threshold :	75

Service Component Name:

The table below describes the configuration properties of the LAM:

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
Primary CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	Designates the logical IP address of the Primary Stream associated with the active Accounting Module. This is used to set up the connection for the Primary Stream between the Local Accounting Manager and the Central Accounting Manager. The address entered here should be the same as that which was entered for the "CAM IP Address" property during the configuration of the CAM on the Accounting Module. Note: The default value must be updated in order for the functionality to work correctly.
Primary CAM Port	Type: Integer Range: 1025-65535 Default: 17667	Designates the port number of the Accounting Module used to set up the connection for the Primary Stream between the Local Accounting Manager and the Central Accounting Manager. The port entered here should be the same as that which was entered for the "Primary CAM Port" property during the configuration of the CAM on the Accounting Module.

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
Recovery CAM IP Address	Type: String Range: 1-15 characters Default: 0.0.0.0	Designates the logical IP address of the Recovery Stream associated with the active Accounting Module. This is used to set up the connection for the Recovery Stream between the Local Accounting Manager and the Central Accounting Manager. The address entered here should be the same as that which was entered for the "CAM IP Address" property during the configuration of the CAM on the Accounting Module. Note: The default value must be updated in order for the functionality to work correctly.
Recovery CAM Port	Type: Integer Range: 1025-65535 Default: 17668	Designates the port number of the Accounting Module used to set up the connection for the Recovery Stream between the Local Accounting Manager and the Central Accounting Manager. The port entered here should be the same as that which was entered for the "Recovery CAM Port" property during the configuration of the CAM on the Accounting Module.
File Rotation Size	Type: Integer (bytes) Range: 0-300000 Default: 100000	Specifies the maximum file size for the accounting file stored on the disk of the SIP Application Module. A value of zero indicates no rotation based on file size. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. This field is only used for the Recovery Stream. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.

Table 3 Configuration properties of the LAM

LAM Field name	Format	Description
File Rotation Time	Type: Integer (seconds) Range: 0 (disabled), 1-3600 (1 second – 60 minutes) Default: 300 (5 minutes)	Designates the amount of time a file is writable. A value of zero indicates no rotation based on time. When both File Rotation Size and File Rotation Time are set to values greater than 0, then files are rotated based on the first condition met, either size or time. This field is only used for the Recovery Stream. Note: The System Management Console will not allow you to set both the File Rotation Size and File Rotation Time to zero.
Disk Monitor Major Threshold	Type: Integer (percentage) Range: 1-100 Default: 50	Specifies the threshold of used disk space for the accounting disk partition when the Local Accounting Manager raises a DiskMajor alarm. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.
Disk Monitor Critical Threshold	Type: Integer (percentage) Range: 1-100 Default: 75	Specifies the threshold of used disk space for the accounting disk partition when the Local Accounting Manager raises a DiskCritical alarm. This property is used to help reduce the chance of losing accounting records by notifying customers when accounting disk space is getting low.



Accounting management

How this chapter is organized

This chapter is organized as follows:

- [Accounting naming conventions on page 47](#)
 - [LAM output file directory on page 47](#)
 - [LAM recovery file naming convention on page 48](#)
 - [CAM output file directory on page 48](#)
 - [CAM file naming convention on page 49](#)
 - [Accessing accounting files on the CAM on page 49](#)
 - [Deleting accounting files on the CAM on page 50](#)
- [Accounting file format on page 51](#)
 - [General format on page 51](#)
 - [Accounting Files on page 52](#)
 - [IPDR elements and attributes on page 59](#)
 - [Example accounting file on page 60](#)
- [Accounting record format on page 62](#)
 - [Record types on page 62](#)
 - [Accounting record schema on page 63](#)
 - [Element/Field definition on page 77](#)
 - [Record formats on page 85](#)
 - [Sample accounting records on page 99](#)

Accounting naming conventions

LAM output file directory

The directory where the RU Block file is located is:

/billing/LAM/RUblock/<AppModName>

where:

<AppModName> is the Component Name provided by the administrator when deploying the SIP Application Module through the System Management Console. For further information, refer to the *MCS 5100 SIP Application Module Basics*.

LAM recovery file naming convention

When writing recovery files to the directory structure built from the information in the previous section, the LAM uses the following file naming convention:

RUblocks_<date>@<time>.<extension>

where:

<date> is the date the file was created in <year><month><day> format

For example, 20010309 represents March 9, 2001

<time> is the time the file was created in
<hours><minutes><seconds> <milliseconds> format

For example, 141700143 represents 14 hours 17 minutes 0 seconds and 143 milliseconds

<extension> is in one of the following strings:

- .active—represents an open RU Blocks file that is currently being written by the LAM
- .closed—represents a closed RU Blocks file that has been written, but has not yet been sent to the CAM
- .reading—represents an RU Blocks file that is currently being transferred to the CAM through the recovery stream

CAM output file directory

The actual directory containing the accounting information for the primary stream is:

/billing/CAM/accounting/Primary

and the directory for the recovery stream is:

/billing/CAM/accounting/Recovery

CAM file naming convention

When writing IPDR formatted files to the directory structure built from the information in the previous section, the CAM uses the following file naming convention:

IPDR_<date>@<time>.<extension>

where:

<date> is the date the file was created in <year><month><day> format

For example, 20010309 represents March 9, 2001

<time> is the time the file was created in
<hours><minutes><seconds><milliseconds> format

For example, 141700143 represents 14 hours 17 minutes 0 seconds and 143 milliseconds

<extension> is in one of the following strings:

- .active—represents an open accounting file that is currently being written by the CAM
- .closed—represents a closed accounting file, which is available for retrieval by the OSS
- .incomplete—represents an accounting file which was not properly closed due to a failure (e.g. failover, shutdown, etc.) on the previously active instance of the Accounting Module.
- .zip—represents a file which was compressed, if this option was chosen during configuration. For more information on how to choose this option, please refer to [Table 2. Configuration properties of the CAM, on page 36](#).
- .transferred—represents a transferred file via FTP Push (e.g. file has been sent via FTP to the customer OSS successfully).

Note: Some extensions listed above can be used in conjunction with each other. For example, a file which was closed, compressed, and then transferred via FTP Push would have the following extension: .closed.zip.transferred.

Accessing accounting files on the CAM

To access files on the CAM, you need to establish a telnet session to the server:

From the telnet session

- 1 Establish a remote login session to the server. You will need a Login ID and Password. Contact your next level of support.
- 2 To access the primary stream directory on the CAM:
type: **cd /billing/CAM/accounting/Primary**
To access the recovery stream directory on the CAM:
type: **cd /billing/CAM/accounting/Recovery**
- 3 Type **ls** to see all the files in the directory.
- 4 To view a file:
type: **more <filename>**
- 5 To exit out of the session, type **exit**.

Deleting accounting files on the CAM**CAUTION**

Ensure all information has been transferred to a back-end billing system prior to deletion.

It is recommended that the oldest files be deleted first.

To delete files on the CAM, you need to establish a telnet session to the server:

From the telnet session

- 1 Establish a remote login session to the server. You will need a Login ID and Password. Contact your next level of support.
- 2 To access the primary stream directory on the CAM:
type: **cd /billing/CAM/accounting/Primary**
To access the recovery stream directory on the CAM:
type: **cd /billing/CAM/accounting/Recovery**
- 3 Type **ls** to see all the files in the directory.
- 4 To delete a file:
type: **rm <filename>**
- 5 To exit out of the session, type **exit**.

Accounting file format

General format

In the Accounting Module, Extensible Markup Language (XML) is used to format accounting data into accounting records. XML is a standard created by the W3C (World Wide Web Consortium). It is a subset of SGML (Structured Generalized Markup Language), and is used to store data in a machine-independent way through the use of tags.

XML tags look similar to HTML (Hyper Text Markup Language) bracketed strings which delimit each piece of data. Each accounting field has a unique markup tag that allows any XML parser to recognize it.

XML was chosen due to its generic format, flexible structure, and human+machine readability. It serves the same purpose as arbitrarily formatted tags while adding the weight of a standard.

The XML format is based on Version 2.0 of the IPDR specification ("Network Data Management - Usage (NDM-U) For IP-Based Services"). The IPDR specification defines what is termed an IPDR document, which encompasses many IPDR records. An IPDR record, in turn, is also made up of categorized accounting information. This accounting information is categorized into a Service Session (SS) (composed of Service Consumer (SC) and Service Element (SE) information) and Usage Event (UE) information.

In this document, an accounting file is synonymous to an IPDR document; while accounting records are synonymous to IPDR records.

In order to describe the outputted XML format, Version 2.0 of the IPDR specification uses the XML Schema language defined by the W3C. The IPDR document is described using a Master Schema defined within the IPDR specification.

Service Schemas further define the IPDR document by defining the IPDR records within the document. Each type of service has a service schema associated with it which defines the accounting information that is captured in order to bill end-users (Service Consumers) for that service. The IPDR specification also provides schemas for some example services, including VoD (Video on Demand) and VoIP (Voice over IP).

Although the IPDR specification is in its infancy and requires expansion in some areas, it was chosen due to its ability to provide a good base and general standard for building accounting/detail records for IP-type services.

Accounting Files

When accounting records are written to a file, they are written in the form of IPDR documents. The format of the accounting file is based on the structure laid out in the Master Schema. The following figures show the IPDR Master Schema:

Figure 21 IPDR Master Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<!--Generated by XML Authority. Conforms to w3c
http://www.w3.org/2001/XMLSchema-->
<schema xmlns="http://www.w3.org/2001/XMLSchema" targetNam-
espace="http://www.ipdr.org/namespaces/ipdr"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr">
  <annotation>
    <documentation> This is the base type for the Service Consumer
      element. The service specific schema can extend
      this by deriving from it.
    </documentation>
    <documentation> This is the base type for the SE (Service
      Element)element. The service specific schema can extend
      this by deriving from it.
    </documentation>
    <documentation> This is the base type for the UE (Usage Entry)
      element. The service specific schema can extend
      this by deriving from it.
    </documentation>
  </annotation>
  <element name="IPDRDoc">
    <annotation>
      <documentation> The IPDRDoc element is the top-level container
        of a set of IPDRs. The document will also define the entity
        which recorded these IPDRs via the IPDRRec element.
      </documentation>
    </annotation>
    <complexType>
      <sequence>
        <element ref="ipdr:IPDRRec"/>
        <element ref="ipdr:IPDRRecList" minOccurs="0"/>
        <element ref="ipdr:IPDR" maxOccurs="unbounded"/>
        <element ref="ipdr:IPDRDoc.End" minOccurs="0"/>
      </sequence>
      <attribute name="seqNum" type="integer"/>
      <attribute name="version" type="string"/>
      <attribute name="startTime" type="dateTime"/>
      <attribute name="info" type="string"/>
    </complexType>
  </element>
</schema>

```

Figure 22 IPDR Master Schema, cont'd

```
</element>
<element name="IPDRDoc.End">
  <annotation>
    <documentation> The IPDRDoc.End element optionally marks the
      end of the IPDR block. It may contain some check
      information like a count of IPDRs.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="count" type="integer"/>
    <attribute name="endTime" type="dateTime"/>
  </complexType>
</element>
<element name="IPDRRec">
  <annotation>
    <documentation> The IPDRRec element describes the entity that
      is responsible for creating (recording) the IPDRDoc.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="id" type="ID"/>
    <attribute name="startTime" type="dateTime"/>
    <attribute name="info" type="string"/>
  </complexType>
</element>
<element name="IPDRRecRef">
  <annotation>
    <documentation> The IPDRRecRef element may be used to associate
      common references to the same IPDRRec element without
      repeating its other usage attributes.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
```

Figure 23 IPDR Master Schema, cont'd

```
<element name="IPDRRecList">
  <annotation>
    <documentation> The IPDRRecList identifies contributing IPDR
      recording entities which were used in the construction
      of the current IPDR Document. A typical example use
      would be for an aggregator of IPDR documents to
      identify the set of initial recorders presenting
      IPDRs.
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <element ref="ipdr:IPDRRec" maxOccurs="unbounded"/>
    </sequence>
  </complexType>
</element>
<element name="IPDR">
  <annotation>
    <documentation> An IPDR describes an event between a Service
      Consumer (SC) and a Service Element (SE). The SC and SE
      elements are contained beneath an entity called the
      Service Session (SS). Details of the event is contained
      in the Usage Entry (UE) element. All IPDRs have a time
      indicating when the event occurred.
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <choice minOccurs="0">
        <element ref="ipdr:IPDRRec"/>
        <element ref="ipdr:IPDRRecRef"/>
      </choice>
      <choice>
        <element ref="ipdr:SS"/>
        <element ref="ipdr:SSRef"/>
      </choice>
      <element ref="ipdr:UE"/>
      <element ref="ipdr:BaseIPDR" minOccurs="0"/>
    </sequence>
  </complexType>
</element>
```

Figure 24 IPDR Master Schema, cont'd

```

    <attribute name="id" type="ID"/>
    <attribute name="time" use="required" type="dateTime"/>
    <attribute name="seqNum" type="integer"/>
  </complexType>
</element>
<element name="SS">
  <annotation>
    <documentation> The Service Session (SS) element groups the
      Service Consumer and Service Element information. This
      grouping allows an SC/SE pair to be associated with other
      IPDRs via a single reference (the SSRef).
    </documentation>
  </annotation>
  <complexType>
    <sequence>
      <choice>
        <element ref="ipdr:SC"/>
        <element ref="ipdr:SCRef"/>
      </choice>
      <choice>
        <element ref="ipdr:SE"/>
        <element ref="ipdr:SERef"/>
      </choice>
    </sequence>
    <attribute name="id" type="ID"/>
    <attribute name="service" type="string"/>
  </complexType>
</element>
<complexType name="SCType" final="restriction">
  <sequence/>
  <attribute name="id" type="ID"/>
</complexType>
<element name="SC" type="ipdr:SCType">
  <annotation>
    <documentation> This element describes the Service Consumer.
  </documentation>
  </annotation>
</element>

```

Figure 25 IPDR Master Schema, cont'd

```
<complexType name="SEType" final="restriction">
  <sequence/>
  <attribute name="id" type="ID"/>
</complexType>
<element name="SE" type="ipdr:SEType">
  <annotation>
    <documentation> This element describes the Service Element.
  </documentation>
  </annotation>
</element>
<complexType name="UEType" final="restriction">
  <sequence/>
  <attribute name="type" default="Start-Stop">
    <simpleType>
      <restriction base="string">
        <enumeration value="Start"/>
        <enumeration value="Stop"/>
        <enumeration value="Start-Stop"/>
        <enumeration value="Interim"/>
      </restriction>
    </simpleType>
  </attribute>
</complexType>
<element name="UE" type="ipdr:UEType">
  <annotation>
    <documentation> This element describes the Usage Entry.
  </documentation>
  </annotation>
</element>
<element name="SSRef">
  <annotation>
    <documentation> The SSRef element may be used to associate common
      references to the same pairing of a Service Consumer
      and a Service Element.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
```

Figure 26 IPDR Master Schema, cont'd

```
</element>
<element name="SRef">
  <annotation>
    <documentation> The SRef element may be used to associate
      common references to the Service Element.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
<element name="SCRef">
  <annotation>
    <documentation> The SCRef element may be used to associate
      common references to the Service Consumer.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="ref" use="required" type="IDREF"/>
  </complexType>
</element>
<element name="BaseIPDR">
  <annotation>
    <documentation> The BaseIPDR element allows reference to be
      made to IPDRs which contributed to the construction of the
      current IPDR element.
    </documentation>
  </annotation>
  <complexType>
    <attribute name="refs" use="required" type="IDREFS"/>
  </complexType>
</element>
</schema>
```

IPDR elements and attributes

Within the IPDR Master Schema, there are many elements, and attributes for these elements, defined. However, only a subset of these are actually used within the accounting file. This subset is shown in the following table:

Table 4 IPDR elements and attributes used

Element Name (XML tag) Used	Element Name Located Within	Attribute Name(s) Used	Description
IPDRDoc	N/A (root element)	seqNum	Indicates the accounting file sequence number.
		version	Indicates the IPDR version and Accounting Module release used to create the accounting file.
IPDRRec	IPDRDoc	id	Identifies the Accounting Module producing the accounting file.
		startTime	Indicates the time when the accounting file was created.
IPDR	IPDRDoc	time	Indicates the time when the accounting record was created in the file.
		seqNum	Indicates the accounting record sequence number.
SS	IPDR	service	Indicates the type of the accounting record.
SC	SS	N/A (none used)	N/A
SE	SS	N/A (none used)	N/A
UE	IPDR	N/A (none used)	N/A

Table 4 IPDR elements and attributes used

Element Name (XML tag) Used	Element Name Located Within	Attribute Name(s) Used	Description
IPDRDoc.End	IPDRDoc	count	Indicates the number of accounting/IPDR records held within the accounting file.
		endTime	Indicates the time when the accounting file was closed.

Example accounting file

[Figure 27, Example accounting file structure, on page 61](#) shows an example of a basic accounting file without any service specific information.

Figure 27 Example accounting file structure

```
<?xml version="1.0"?>
<ipdr:IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance" xsi:noNamespace-
SchemaLocation="NortelIMS2.0_VoIPschema.xsd" seqNum="24" ver-
sion="IPDR2.0/NortelIMS2.0">
  <ipdr:IPDRRec id="CAM-32.124.26.125" startTime="2000-02-01T06:35:00Z"/>
  <ipdr:IPDR seqNum="1" time="2000-02-01T07:05:00Z">
    <ipdr:SS service="ConnectEgress">
      <ipdr:SC xsi:type="SC-VoIP-Type"/>
      <ipdr:SE xsi:type="SE-VoIP-Type"/>
    </ipdr:SS>
    <ipdr:UE xsi:type="UE-VoIP-Type"/>
  </ipdr:IPDR>
  <ipdr:IPDR seqNum="2" time="2000-02-01T07:06:00Z">
    <ipdr:SS service="ConnectIngress">
      <ipdr:SC xsi:type="SC-VoIP-Type"/>
      <ipdr:SE xsi:type="SE-VoIP-Type"/>
    </ipdr:SS>
    <ipdr:UE xsi:type="UE-VoIP-Type"/>
  </ipdr:IPDR>
  <ipdr:IPDR seqNum="3" time="2000-02-01T07:07:00Z">
    <ipdr:SS service="SDP">
      <ipdr:SC xsi:type="SC-VoIP-Type"/>
      <ipdr:SE xsi:type="SE-VoIP-Type"/>
    </ipdr:SS>
    <ipdr:UE xsi:type="UE-VoIP-Type"/>
  </ipdr:IPDR>
  <ipdr:IPDRDoc.End count="3" endTime="2000-02-01T09:05:00Z"/>
</ipdr:IPDRDoc>
```

Accounting record format

Record types

Accounting records are produced based on events that occur during service/session processing. In response to these events, the following types of records are produced:

- Connect Ingress record - holds information regarding the setup/abandon/reject/answer portion of the session for the originating call model (OCM). This covers accounting for the following services: Authentication, and SDP (including Video, Collaboration, and CODEC information).
- Connect Egress record - holds information regarding the setup/abandon/reject/answer portion of the terminating session for the terminating call model (TCM). This also covers accounting for the following services: Routing (including Simultaneous Ringing, Sequential Ringing, Call Forwarding, and Redirection).
- Long Call Ingress - holds information regarding sessions for the OCM when a Long Call audit is performed. For information regarding when a Long Call audit is performed on the SIP Application Module, please refer to *MCS 5100 SIP Application Module Basics*.
- Long Call Egress - holds information regarding sessions for the TCM when a Long Call audit is performed. For information regarding when a Long Call audit is performed on the SIP Application Module, please refer to *MCS 5100 SIP Application Module Basics*.
- SDP record - holds SDP information which is received for the session during the middle of the call (between answer and disconnect). This covers accounting for the following services: Call Hold, Call Retrieve, and WebPush.

Note 1: An SDP record for WebPush is only created when originating from any 1.0 Nortel client or a 1.1 Multimedia Web Client.

Note 2: The system will only create an SDP record for call hold or call retrieve when the H.323 endpoint sends notification to the H.323 Gatekeeper that it has placed a call on hold or retrieved a call.

- REFER record - holds information regarding the transfer of calls during the middle of the call.

Note: The system will not create a REFER record for call transfers when the request originates from supported H.323 endpoints through the H.323 Gatekeeper. This is because the

H.323 endpoint does not send notification to the H.323 Gatekeeper that it has transferred a call.

- Disconnect Ingress record - holds information regarding the disconnection of the session for the OCM.
- Disconnect Egress record - holds information regarding the disconnection of the session for the TCM.

The order in which these records are produced and written to the accounting file is undeterminable since it is dependent on the services, etc. encountered during the course of a SIP session.

For service diagrams and descriptions of call flows for the services encountered to produce these records, please refer to Appendix A of the *MCS 5100 SIP Application Module Basics*. This information is useful for understanding what events trigger the production of the accounting records as well as provide insight into the Method of Population for the majority of fields within the records.

Accounting record schema

The accounting record format is based on the VoIP (Voice over IP) service schema (which references the Master Schema) as defined within the IPDR specification. A schema (called NortelIMS2.0_VoIPschema.xsd) has been developed based on the VoIP service schema in order to hold all of the Nortel accounting record information. The following figures show the current version of the Nortel Service Schema as of the release of this document:

Note: The latest Nortel Service Schema can be retrieved from the `\billing` directory on the server where the Accounting Module was deployed.

Figure 28 Nortel Service Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- DOCTYPE xs:schema PUBLIC "-//W3C//DTD XMLSCHEMA 200102//EN"
"XMLSchema.dtd" [
    <!ENTITY % schemaAttrs "xmlns:ipdr CDATA #IMPLIED
                                xmlns:nortel CDATA #IMPLIED">
]-->
<!--Generated by XML Authority. Conforms to w3c
http://www.w3.org/2001/XMLSchema-->
<xs:schema targetNamespace="http://www.nortelnetworks.com/namespaces/ipdr"
xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns:ipdr="http://www.ipdr.org/namespaces/ipdr"
xmlns:nortel="http://www.nortelnetworks.com/namespaces/ipdr">
    <xs:import namespace="http://www.ipdr.org/namespaces/ipdr" schemaLoca-
tion="ipdr2.0.xsd"/>
    <!-- Nortel types -->
    <xs:simpleType name="boolean">
        <xs:annotation>
            <xs:documentation>
                String enumeration for boolean true or false values.
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="string">
            <xs:enumeration value="true"/>
            <xs:enumeration value="false"/>
        </xs:restriction>
    </xs:simpleType>
    <!-- Element definitions and documentation -->
    <xs:element name="corrID" type="string">
        <xs:annotation>
            <xs:documentation>
                The unique ID used to correlate ingress and egress accounting
                records within the IMS network.
            </xs:documentation>
        </xs:annotation>
    </xs:element>

```

Figure 29 Nortel Service Schema, cont'd

```
<xs:element name="notifyArrival" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time when the "NOTIFY" message is received during the call
      transfer.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="recTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time the accounting information was captured at the SIP
      application server.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="uID" type="string">
  <xs:annotation>
    <xs:documentation>
      Identifies a session in the IMS network.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referBy" type="string">
  <xs:annotation>
    <xs:documentation>
      The address of the party which transferred a session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referTo" type="string">
  <xs:annotation>
    <xs:documentation>
      The address of the party to which a session is transferred.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 30 Nortel Service Schema, cont'd

```
<xs:element name="referArrival" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The time the "REFER" message is received during a call transfer.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="referStatus" type="integer">
  <xs:annotation>
    <xs:documentation>
      This indicates if a successful "NOTIFY" message has been received
      for the "REFER" message during a transfer.
      0 is unknown status, 1 indicates a failure, 2 indicates success.
      No other values are valid.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="protocol" type="string">
  <xs:annotation>
    <xs:documentation>
      The session protocol used during the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="origDest" type="string">
  <xs:annotation>
    <xs:documentation>
      The first address the session was originally routed to.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="subscriberID" type="string">
  <xs:annotation>
    <xs:documentation>
      The SIP address of the originator for a session or a mid-call
      request.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 31 Nortel Service Schema, cont'd

```
</xs:annotation>
</xs:element>
<xs:element name="callingPSTN" type="string">
  <xs:annotation>
    <xs:documentation>
      The PSTN number for the calling party (originator) of the session.
    </xs:documentation>
    <xs:appinfo>
      Found in SC records only.
    </xs:appinfo>
  </xs:annotation>
</xs:element>
<xs:element name="oUA" type="string">
  <xs:annotation>
    <xs:documentation>
      The originating User Agent that was used for the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="startTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      When the SIP Application server received an initial "INVITE"
      request message issued by the originator.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="endTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      Indicates when a session has ended.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="destinationPhoneNumber" type="string">
  <xs:annotation>
```

Figure 32 Nortel Service Schema, cont'd

```
<xs:documentation>
  The SIP address of the terminator being attempted.
</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="proprietaryErrorCode" type="integer">
  <xs:annotation>
    <xs:documentation>
      The SIP response type when a failed session occurs.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="aband" type="nortel:boolean">
  <xs:annotation>
    <xs:documentation>
      Indicates if a call was abandoned before answering.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="ansInd" type="nortel:boolean">
  <xs:annotation>
    <xs:documentation>
      Indicates if a call was answered.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="webURI" type="string">
  <xs:annotation>
    <xs:documentation>
      The URI of the web page being pushed.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="tUA" type="string">
  <xs:annotation>
```

Figure 33 Nortel Service Schema, cont'd

```
<xs:documentation>
The terminating user agent.
</xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="tMG" type="string">
  <xs:annotation>
    <xs:documentation>
The terminating media gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="oMG" type="string">
  <xs:annotation>
    <xs:documentation>
The originating media gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sdpPort" type="integer">
  <xs:annotation>
    <xs:documentation>
      The sdp port used in the media connection.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sdpProtocol" type="string">
  <xs:annotation>
    <xs:documentation>
      The protocol used in the media connection.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="sessionName" type="string">
  <xs:annotation>
    <xs:documentation>
      The name of the session.
    </xs:documentation>
  </xs:annotation>
</xs:documentation>
```

Figure 34 Nortel Service Schema, cont'd

```
</xs:annotation>
</xs:element>
<xs:element name="mediaPortal" type="nortel:boolean">
  <xs:annotation>
    <xs:documentation>
      A flag indicating the use of a media portal during the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<!-- Media block elements -->
<xs:element name="succStatus" type="string">
  <xs:annotation>
    <xs:documentation>
      The success status.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="failRsn" type="string">
  <xs:annotation>
    <xs:documentation>
      The failure reason.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="fromAddr" type="string">
  <xs:annotation>
    <xs:documentation>
      The from address.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="fromPSTNnum" type="string">
  <xs:annotation>
    <xs:documentation>
      The PSTN number from which the call/action came.
    </xs:documentation>
  </xs:annotation>
```

Figure 35 Nortel Service Schema, cont'd

```
</xs:element>
<xs:element name="toAddr" type="string">
  <xs:annotation>
    <xs:documentation>
      The to address.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="attemptList" type="string">
  <xs:annotation>
    <xs:documentation>
      The list of addresses attempted for a SimRing or SeqRing request.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="connParty" type="string">
  <xs:annotation>
    <xs:documentation>
      The party connected to.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="phoneNo" type="string">
  <xs:annotation>
    <xs:documentation>
      The phone number used in the call.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="ansTime" type="dateTime">
  <xs:annotation>
    <xs:documentation>
      The date and time the call was answered.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

Figure 36 Nortel Service Schema, cont'd

```

<xs:element name="outpulsedDigits" type="string">
  <xs:annotation>
    <xs:documentation>
      The digits outpulsed to the gateway.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<!-- Routing complex type -->
<xs:simpleType name="RouteSimpleType">
  <xs:annotation>
    <xs:documentation>
      There are two types of route blocks.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="string">
    <xs:enumeration value="SIM"/>
    <xs:enumeration value="SEQ"/>
  </xs:restriction>
</xs:simpleType>
<xs:complexType name="routeBlock-Type">
  <xs:sequence>
    <xs:element name="type" type="nortel:RouteSimpleType"/>
    <!-- Remove <xs:element name="numAttempts" type="integer"/> -->
    <xs:element name="routes" type="nortel:Routes-Complex-Type"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="Routes-Complex-Type">
  <xs:sequence>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element name="route" type="string"/>
      <xs:element name="routing" type="nortel:routing-Type"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="routing-Type">
  <xs:annotation>

```

Figure 37 Nortel Service Schema, cont'd

```

    <xs:documentation>
      The routing used for the session.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="routingDest" type="string"/>
    <xs:element name="routeBlock" type="nortel:routeBlock-Type" maxOc-
curs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<!-- Now glue it all together -->
<xs:complexType name="SC-VoIP-Type">
  <xs:complexContent>
    <xs:extension base="ipdr:SCType">
      <xs:sequence>
        <xs:element name="subscriberID" type="string" minOccurs="0"/>
        <xs:element name="callingPSTN" type="string" minOccurs="0"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="SE-VoIP-Type">
  <xs:complexContent>
    <xs:extension base="ipdr:SEType">
      <xs:sequence>
        <xs:element name="appSrvID" type="string"/>
        <xs:element name="appSrvVer" type="string"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
<xs:complexType name="Codec-List-Type">
  <xs:sequence>
    <xs:element name="codec" type="string" minOccurs="1" maxOc-
curs="unbounded"/>
  </xs:sequence>
</xs:complexType>

```

Figure 38 Nortel Service Schema, cont'd

```

<xs:complexType name="Media-List-Type">
  <xs:annotation>
    <xs:documentation>This describes the media block.</xs:documenta-
tion>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="mediaName" type="string"/>
    <xs:element name="sdpProtocol" type="string"/>
    <xs:element name="origSdpPort" type="integer"/>
    <xs:element name="origConnAddr" type="string" minOccurs="0"/>
    <xs:element name="termSdpPort" type="integer"/>
    <xs:element name="termConnAddr" type="string" minOccurs="0"/>
    <xs:element name="codecList" type="nortel:Codec-List-Type" minOc-
curs="0"/>
  </xs:sequence>
</xs:complexType>
<!-- servType is an enumeration -->
<xs:simpleType name="Service-Type">
  <xs:annotation>
    <xs:documentation>Enumerate the valid service types.</xs:documenta-
tion>
  </xs:annotation>
  <xs:restriction base="string">
    <xs:enumeration value="SDP"/>
    <xs:enumeration value="Authentication"/>
    <xs:enumeration value="RoutingActions"/>
  </xs:restriction>
</xs:simpleType>
<xs:complexType name="supplementaryService-Type">
  <xs:annotation>
    <xs:documentation>
      This is a superset of all the supplementaryService varieties that
      the IMS system can present.
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="servType" type="nortel:Service-Type"/>

```

Figure 39 Nortel Service Schema, cont'd

```

<xs:element ref="nortel:corrID" minOccurs="0"/>
<xs:element ref="nortel:referBy" minOccurs="0"/>
<xs:element ref="nortel:referTo" minOccurs="0"/>
<xs:element ref="nortel:referArrival" minOccurs="0"/>
<xs:element ref="nortel:referStatus" minOccurs="0"/>
<xs:element ref="nortel:subscriberID" minOccurs="0"/>
<xs:element ref="nortel:succStatus" minOccurs="0"/>
<xs:element ref="nortel:failRsn" minOccurs="0"/>
<xs:element ref="nortel:fromAddr" minOccurs="0"/>
<xs:element ref="nortel:fromPSTNnum" minOccurs="0"/>
<xs:element ref="nortel:toAddr" minOccurs="0"/>
<xs:element ref="nortel:sessionName" minOccurs="0"/>
<xs:element ref="nortel:mediaPortal" minOccurs="0"/>
<xs:element ref="nortel:phoneNo" minOccurs="0"/>
<xs:element name="media" type="nortel:Media-List-Type" minOccurs="0" maxOccurs="unbounded"/>
<xs:element name="routing" type="nortel:routing-Type" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<!-- UE group type -->
<xs:complexType name="UE-VoIP-Type">
  <xs:annotation>
    <xs:documentation>
      This is a superset of all the UE combinations.
    </xs:documentation>
  </xs:annotation>
  <xs:complexContent>
    <xs:extension base="ipdr:UEType">
      <xs:sequence>
        <xs:element ref="nortel:uID"/>
        <xs:element ref="nortel:corrID"/>
        <xs:element ref="nortel:recTime"/>
        <!-- all else are expressed as optional -->
        <xs:element ref="nortel:protocol" minOccurs="0"/>
        <xs:element ref="nortel:notifyArrival" minOccurs="0"/>
        <xs:element ref="nortel:startTime" minOccurs="0"/>

```

Figure 40 Nortel Service Schema, cont'd

```

<xs:element ref="nortel:endTime" minOccurs="0"/>
<xs:element ref="nortel:tUA" minOccurs="0"/>
<xs:element ref="nortel:tMG" minOccurs="0"/>
<xs:element ref="nortel:oMG" minOccurs="0"/>
<xs:element ref="nortel:ansTime" minOccurs="0"/>
<xs:element ref="nortel:origDest" minOccurs="0"/>
<xs:element ref="nortel:referBy" minOccurs="0"/>
<xs:element ref="nortel:oUA" minOccurs="0"/>
<xs:element ref="nortel:destinationPhoneNumber" minOc-
curs="0"/>
<xs:element ref="nortel:proprietaryErrorCode" minOccurs="0"/>
<xs:element ref="nortel:aband" minOccurs="0"/>
<xs:element ref="nortel:ansInd" minOccurs="0"/>
<xs:element ref="nortel:sessionName" minOccurs="0"/>
<xs:element ref="nortel:mediaPortal" minOccurs="0"/>
<xs:element ref="nortel:phoneNo" minOccurs="0"/>
<xs:element ref="nortel:webURI" minOccurs="0"/>
<xs:element name="media" type="nortel:Media-List-Type" minOc-
curs="0" maxOccurs="unbounded"/>
<xs:element ref="nortel:outpulsedDigits" minOccurs="0"/>
<!-- The following supplementary service is really only the
RoutingActions service -->
<xs:element name="supplementaryService" type="nortel:supple-
mentaryService-Type" minOccurs="0" maxOccurs="1"/>
<xs:element ref="nortel:connParty" minOccurs="0"/>
<xs:element ref="nortel:failRsn" minOccurs="0"/>
<xs:element ref="nortel:referTo" minOccurs="0"/>
<xs:element ref="nortel:referArrival" minOccurs="0"/>
<xs:element ref="nortel:referStatus" minOccurs="0"/>
<xs:element name="supplementaryService" type="nortel:supple-
mentaryService-Type" minOccurs="0" maxOccurs="2"/>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>

```

Element/Field definition

The following table lists the elements and fields used in the IPDR records:

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Answer Indicator	ansInd	ConnectIngress, ConnectEgress	UE	Indicates whether the call was answered.
Answer Time	ansTime	ConnectIngress, ConnectEgress	UE	If the call was answered, indicates the time of answer (in Greenwich Mean Time (GMT)).
Application Server ID	appSrvID	ALL	SE	Indicates the SIP Application Module which is producing the accounting record.
Application Server Version	appSrvVer	ALL	SE	Indicates the software Load Version of the SIP Application Module producing the accounting record. Note: This information is important when reporting problems to your next level of support.
Call Abandoned	aband	ConnectIngress, ConnectEgress	UE	Indicates whether the call was abandoned before the call was answered.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Calling Party PSTN Number	callingPSTN	ConnectIngress	SC	Indicates the telephony number for the calling party (originator) of the session.
CODEC	codec	ConnectIngress, SDP	codecList	Indicates the CODEC chosen based on negotiation with the terminator.
CODEC List	codecList	ConnectIngress, SDP	media	Contains a list of CODEC(s).
Connected Party	connParty	ConnectEgress	UE	Indicates the address of the party that a session was finally connected to.
Correlation ID	corrID	ALL	UE	Indicates a unique ID used to correlate ingress and egress accounting records within the network. This correlation ID can also be used to correlate accounting records with accounting records from the CS 2000 network.
Destination Phone Number	destinationPhoneNumber	ConnectIngress	UE	Indicates the terminating address being attempted.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
End Time	endTime	ConnectIngress, ConnectEgress, DisconnectIngress, DisconnectEgress	UE	Indicates the time (in Greenwich Mean Time (GMT)) when a session has ended, either based on disconnection, abandonment or error.
Failure Reason	failRsn	ConnectIngress, LongCallIngress, LongCallEgress	SupplementaryService; UE	Indicates the reason a failure has occurred (either during authentication or a long call audit).
Media	media	ConnectIngress, SDP	SupplementaryService; UE	Contains other elements/fields which provide information regarding a negotiated media during the session.
Media Name	mediaName	ConnectIngress, SDP	media	Indicates the type of media being transported during the session (i.e. audio, video).
Media Portal	mediaPortal	ConnectIngress, SDP	SupplementaryService; UE	Indicates whether an RTP Media Portal was used during the session.
Notify Arrival Time	notifyArrival	REFER	UE	Indicates the time (in Greenwich Mean Time (GMT)) the "NOTIFY" message is received during a call transfer.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Original Destination Address	origDest	ConnectIngress	UE	Indicates the first address the session was originally routed to.
Originating Connection Address	origConnAddr	ConnectIngress, SDP	media	When set to 0.0.0.0, it indicates a session is on hold. Otherwise, it indicates the address of the originating party.
Originating SDP Port	origSdpPort	ConnectIngress, SDP	media	Indicates the originating port which was used to transport the media for the session.
Originating User Agent	oUA	ConnectIngress	UE	Identifies the originating User Agent that was used for the session.
Outpulsed Digits	outpulsedDigits	ConnectEgress	UE	Indicates the terminator's address, which was used to route the call on the outbound side of the session.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Phone Number	phoneNo	ConnectIngress, SDP	Supplementary Service; UE	Indicates the phone number associated with the SDP sent during the session initiation. In the case of WebPush, it indicates that a WebPush was performed. Note: This field is only created when originating from a Multimedia PC Client or Web Client.
Proprietary Error Code	proprietaryErrorCode	ConnectIngress, ConnectEgress	UE	Indicates the SIP response type when a failed session occurs. For more information on the SIP response types, please refer to the SIP Draft RFC 2543 (see note in Record formats on page 85 for specific reference).
Protocol	protocol	ConnectIngress, ConnectEgress	UE	Indicates the signaling protocol (SIP) that was used during the session.
Record Time	recTime	ALL	UE	Indicates the time (in Greenwich Mean Time (GMT)) an accounting record is produced at the SIP Application Module.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Refer Arrival Time	referArrival	REFER	UE	Indicates the time (in Greenwich Mean Time (GMT)) when the request to transfer the call is received by the party being transferred.
Refer Status	referStatus	REFER	UE	Indicates if the call transfer was successful.
Refer to	referTo	REFER	UE	Indicates the address of the party to which a session is transferred.
Referred by	referBy	ConnectIngress, REFER	UE	Indicates the address of the party which transferred a session.
Route	route	ConnectEgress	routes	Resolved destination route with IP address and port number (i.e. user@25.106.53.96).
Route Block	routeBlock	ConnectEgress	routing	Contains other elements/fields which provides a set of routes that are attempted sequentially or simultaneously based on the service provided.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Routes	routes	ConnectEgress	routeBlock	Contains other elements/fields to indicate a resolved route(s) and/or an unresolved destination(s).
Routing	routing	ConnectEgress	SupplementaryService; routes	Contains other elements/fields which provide information regarding routing information for each well-known destination. Well-known destinations are destinations which need to be resolved further (i.e. user@domain.com).
Routing Destination Address	routingDest	ConnectEgress	routing	Indicates the unresolved destination address.
Routing Type	type	ConnectEgress	routeBlock	Indicates the type of routing used to traverse the route(s) identified in the Route Block.
SDP Protocol	sdpProtocol	ConnectIngress, SDP	media	Indicates the protocol used to transport the media for the session.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Service Type	servType	ConnectIngress, ConnectEgress	SupplementaryService	Indicates the type of service information captured within the Supplementary Service field (i.e. Authentication, RoutingActions, SDP).
Session Name	sessionName	ConnectIngress, SDP	SupplementaryService; UE	Indicates the session name. In the case of collaboration, it indicates that it is a collaboration session.
Start Time	startTime	ConnectIngress, ConnectEgress	UE	Indicates the time (in Greenwich Mean Time (GMT)) when the session begins.
Subscriber ID	subscriberID	ConnectIngress, ConnectEgress, REFER, SDP, DisconnectIngress, DisconnectEgress	SC	Indicates the SIP address of the user who initiated an event (i.e. Connect, Disconnect, Hold, Retrieve, Media Change, etc.).
Success Status	succStatus	ConnectIngress	SupplementaryService	Indicates whether authentication was successful.
Supplementary Service	supplementaryService	ConnectIngress, ConnectEgress	UE	Contains other elements/fields which provide information regarding a service provided during a session.

Table 5 Element/Field list

Field Name	Element Name (XML tag)	Record Type	Element Name Located Within	Description
Terminating Connection Address	termConnAddr	ConnectIngress, SDP	media	When set to 0.0.0.0, it indicates a session is on hold. Otherwise, it indicates the address of the terminating party.
Terminating Media Gateway	tMG	ConnectEgress	UE	Identifies the terminating Media Gateway that was used for the session.
Terminating SDP Port	termSdpPort	ConnectIngress, SDP	media	Indicates the terminating port which was used to transport the media for the session.
Terminating User Agent	tUA	ConnectEgress	UE	Identifies the terminating user agent for the session.
Unique Session Identifier	uID	ALL	UE	Identifies a session in the network.
Web URI Indicator	webURI	SDP	UE	Indicates the URI which was specified as part of the WebPush service.

Record formats

In order to provide a different layout of the accounting record information, each record and its fields are detailed. The “Method of Population” information for each field is provided as insight into the values that are recorded in each field. Since the majority of the accounting information is gathered from the SIP messaging used during session processing, it is recommended that the SIP Draft RFC

2543 (see note for specific reference) be referenced for more information.

Note 1: J. Rosenberg et al, SIP: Session Initiation Protocol, Internet Draft draft-ietf-sip-rfc2543-bis09.txt, IETF, Feb 27, 2002.

Note 2: Your next level of support should be contacted regarding third party interoperability prior to implementing the SIP Draft RFC 2543 specification.

The following table lists the ConnectIngress record fields:

Table 6 ConnectIngress record fields

Field Name	Method of Population
Answer Indicator	Set when the SIP Application Module receives a "200 OK" Response message from the terminator after the originator issued the "INVITE" Request message.
Answer Time	Based on a timestamp taken when the Originating Call Model (OCM) of the SIP Application Module receives a "200 OK" response message from the terminator after the originator issued the "INVITE" request message.
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Call Abandoned	Set by the SIP Application Module when the call was cancelled without the call being answered.
Calling Party PSTN Number	Determined based on provisioning for the subscriber in the Provisioning Client or information received from PRI gateways/PSTN. The precedence order for populating this field is the following: • Taken from the provisioned public charge ID of the calling subscriber. • Taken from the provisioned private charge ID of the calling subscriber • Taken from the Remote-Party-ID header in the "INVITE" Request message from a PRI gateway.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
Destination Phone Number	Taken from the URL in the initial "INVITE" Request message issued by the originator.
End Time	Based on the timestamp taken when a call is abandoned or an internal failure occurs.
Original Destination Address	Taken from the addr-spec portion of "TO" field in the initial "INVITE" Request message issued by the originator.
Originating User Agent	Taken from the "User-Agent" header of the "INVITE" Request message received by the SIP Application Module.
Proprietary Error Code	Derived from various response messages received by the SIP Application Module when a session failed.
Protocol	Based on the protocol used to initiate the session.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Referred by	Taken from the "Referred-By" header of the "INVITE" message received when the transferred call is initiated.
Start Time	Based on a timestamp taken when an Initial "INVITE" Request message is received for the OCM by the SIP Application Module.
Subscriber ID	Taken from the addr-spec portion of the "FROM" field in the initial "INVITE" Request message issued by the originator. When the "FROM" field user name portion of the addr-spec is "Anonymous," it is taken from the Remote Party ID header calling parameter if one is provided in the "INVITE" Request message.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Supplementary Service: Authentication (servType)	Contains information/elements regarding authentication. This information includes: • Service Type - Indicates the type of service. In this case, it is Authentication. • Success Status - Indicates if authentication for the "INVITE" was successful or not. • Failure Reason - Based on the signal "407 Authentication Required" in response to the original "INVITE" issued by the originator.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Supplementary Service: SDP (servType)	Contains information/elements regarding SDP. This information includes: • Service Type - Indicates the type of service. In this case, it is SDP. • Media - contains information/elements regarding the media. This information includes: — CODEC List - contains a list of CODEC(s) as follows: – CODEC - Based on a portion of the media attributes field (a=) within the SDP header of the “200 OK” or “ACK” message. — Media Name - Based on a portion of the media description field (m=) within the SDP header of the “INVITE” message. — Media Portal - Determined based on whether or not an RTP Media Portal was involved in a session. — Originating Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the “INVITE” or “ACK” message. — Originating SDP Port - Based on a portion of the media description field (m=) within the SDP header of the “INVITE” or “ACK” message. — SDP Protocol - Based on a portion of the media description field (m=) within the SDP header of the “INVITE” message. — Terminating Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the “200 OK” message. — Terminating SDP Port - Based on a portion of the media description field (m=) within the SDP header of the “200 OK” message. • Phone Number - Based on a portion of the phone number field (p=) within the SDP header of the “200 OK” or “ACK” message. • Session Name - Based on a portion of the session name field (s=) within the SDP header of the “200 OK” or “ACK” message.

Table 6 ConnectIngress record fields

Field Name	Method of Population
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the ConnectEgress record fields:

Table 7 ConnectEgress record fields

Field Name	Method of Population
Answer Indicator	Set when the SIP Application Module receives a "200 OK" Response message from the terminator after the originator issued the "INVITE" Request message.
Answer Time	Based on a timestamp taken when the Terminating Call Model (TCM) of the SIP Application Module receives a "200 OK" response message from the terminator after the originator issued the "INVITE" request message.
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Call Abandoned	Set by the SIP Application Module when the call was cancelled without the call being answered.
Connected Party	Determined during Session Processing, it indicates the SIP address of the party who answers the session. It will match the last route displayed in the RoutingActions Supplementary Service block.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a call is abandoned or an internal failure occurs.

Table 7 ConnectEgress record fields

Field Name	Method of Population
Outpulsed Digits	Determined during Session Processing, it is the SIP address specified in the translated request URI field of the outgoing "INVITE" message from the SIP Application Module.
Proprietary Error Code	Derived from various response messages received by the SIP Application Module when a session failed.
Protocol	Based on the protocol used to terminate the session.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Start Time	Based on a timestamp taken when an Initial "INVITE" Request message is received for the TCM by the SIP Application Module.
Subscriber ID	Taken from the addr-spec portion of the "FROM" field in the initial "INVITE" Request message issued by the originator. When the "FROM" field user name portion of the addr-spec is "Anonymous," it is taken from the Remote Party ID header calling parameter if one is provided in the "INVITE" Request message.

Table 7 ConnectEgress record fields

Field Name	Method of Population
Supplementary Service: RoutingActions (servType)	Contains information/elements regarding routing. This information includes: • Service Type - Indicates the type of service. In this case, it is RoutingActions. • Routing - Contains information/elements regarding routing. This information includes: — Routing Destination Address - Derived based on routing and translations of the URL in the initial "INVITE" Request message issued by the originator. — Route Block - Contains information/elements regarding routing for sessions encountering the simultaneous or sequential ringing service. This information includes: – Routing Type - Indicates whether the simultaneous ringing or sequential ringing service was used to route and terminate the session. The possible values for this field include "SIM" for Simultaneous Ringing or "SEQ" for Sequential Ringing. – Routes - Contains information/elements regarding the routes attempted, either resolved destinations or routing due to call forwarding or redirection. This information includes: – Route - Resolved route derived based on translating the corresponding Routing Destination Address. – Routing - Contains information/elements as described above. Thus, this information is recursive in nature and indicates call forwarding or redirection.
Terminating Media Gateway	Taken from the translated request URI field of the forwarding message sent by the SIP Application Module.

Table 7 ConnectEgress record fields

Field Name	Method of Population
Terminating User Agent	Taken from the "User-Agent" header of the terminator's 200/OK message.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the LongCallIngress record fields:

Table 8 LongCallIngress record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on a timestamp taken when the Long Call audit determines that a call should be taken down.
Failure Reason	Error code given by the Long Call audit when it has been determined that a call should be taken down.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the LongCallEgress record fields:

Table 9 LongCallEgress record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on a timestamp taken when the Long Call audit determines that a call should be taken down.
Failure Reason	Error code given by the Long Call audit when it has been determined that a call should be taken down.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the SDP record fields:

Table 10 SDP record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during the deployment of the SIP Application Module.

Table 10 SDP record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
Media	Contains information/elements regarding a negotiated media. This information includes: • CODEC List - contains a list of CODEC(s) as follows: — CODEC - Based on a portion of the media attributes field (a=) within the SDP header of the "200 OK" or "ACK" message. • Originating Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the "INVITE" or "ACK" message. When the value is set to 0.0.0.0, it indicates the session is on hold. Otherwise, it indicates the address of the originating party. • Originating SDP Port - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" or "ACK" message. • Media Name - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. • Media Portal - Determined based on whether or not an RTP Media Portal was involved in a session. • SDP Protocol - Based on a portion of the media description field (m=) within the SDP header of the "INVITE" message. • Terminating Connection Address - Based on a portion of the connection data field (c=) within the SDP header of the "200 OK" message. When the value is set to 0.0.0.0, it indicates the session is on hold. Otherwise, it indicates the address of the terminating party. • Terminating SDP Port - Based on a portion of the media description field (m=) within the SDP header of the "200 OK" message.

Table 10 SDP record fields

Field Name	Method of Population
Phone Number	Based on a portion of the phone number field (p=) within the SDP header of the “200 OK” or “ACK” message. In the case of WebPush, it indicates that a WebPush was performed.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Session Name	Based on a portion of the session name field (s=) within the SDP header of the “200 OK” or “ACK” message.
Subscriber ID	Based on who initiated the media change. If the originator initiated the media change, then the Method of Population is the same as that used to populate the Subscriber ID within the Connect Ingress record. If the terminator initiated the media change, then the Method of Population is the same as that used to populate the Outpulse Digits within the Connect Egress record.
Unique Session Identifier	Taken from the “Call-ID” field in the “INVITE” message issued by the originator.
Web URI	Based on a portion of the web URI field (w=) within the SDP header of the “INFO” message.

The following table lists the REFER record fields:

Table 11 REFER record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.

Table 11 REFER record fields

Field Name	Method of Population
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
Notify Arrival Time	Based on a timestamp taken when the "NOTIFY" message is received by the SIP Application Module during a call transfer.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Refer Arrival Time	Based on a timestamp taken when the "REFER" message is received by the SIP Application Module during a call transfer.
Refer Status	Based on whether a successful "NOTIFY" is received for a "REFER" message during a call transfer. The possible values for this field include: 0 (unknown), 1 (failure), or 2 (success).
Refer to	Taken from the "Refer-To" header of the "REFER" message received during a call transfer.
Referred by	Taken from the "Referred-By" header of the "REFER" message received during a call transfer.
Subscriber ID	Based on who initiated the transfer. If the originator initiated the transfer, then the Method of Population is the same as that used to populate the Subscriber ID within the Connect Ingress record. If the terminator initiated the transfer, then the Method of Population is the same as that used to populate the Outpulse Digits within the Connect Egress record.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the DisconnectIngress record fields:

Table 12 DisconnectIngress record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a "BYE" message is received by the Originating Call Module (OCM) of the SIP Application Module or when an internal failure occurs.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Subscriber ID	Based on who initiated the disconnect. If the originator initiated the disconnect, then the Method of Population is the same as that used to populate the Subscriber ID within the Connect Ingress record. If the terminator initiated the disconnect, then the Method of Population is the same as that used to populate the Outpulse Digits within the Connect Egress record.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

The following table lists the DisconnectEgress record fields:

Table 13 DisconnectEgress record fields

Field Name	Method of Population
Application Server ID	Based on the SIP Application Module name being provided by the customer during the deployment of the SIP Application Module.
Application Server Version	Based on the software load version selected by the customer during deployment of the SIP Application Module.
Correlation ID	Taken from the x-nt-corr-id header in the initial "INVITE" Request message issued by the originator. If the header is not present, it uses the Unique Session Identifier for the Ingress Session.
End Time	Based on the timestamp taken when a "BYE" message is received by the Terminating Call Model (TCM) of the SIP Application Module or when an internal failure occurs.
Record Time	Based on a timestamp taken when the services portion of the SIP Application Module produces an accounting record (i.e. RU).
Subscriber ID	Based on who initiated the disconnect. If the originator initiated the disconnect, then the Method of Population is the same as that used to populate the Subscriber ID within the Connect Ingress record. If the terminator initiated the disconnect, then the Method of Population is the same as that used to populate the Outpulse Digits within the Connect Egress record.
Unique Session Identifier	Taken from the "Call-ID" field in the "INVITE" message issued by the originator.

Sample accounting records

The following figures provide sample accounting records for the record types described in [Record types on page 62](#) and the common billable services provided by the SIP Application Module. These accounting records are the current samples as of the release of this document.

Note: The latest sample accounting records can be retrieved from the `\billing\Sample` directory on the server where the Accounting Module was deployed.

Figure 41 Connect Ingress Record

```
<ipdr:IPDR seqNum="8" time="2003-07-24T11:54:34.815Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>bab55ad_f6953bb2cc@test2_ipcmweb</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:34.808Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T11:54:33.440Z</startTime>
    <ansTime>2003-07-24T11:54:34.808Z</ansTime>
    <origDest>8080@lab2.org</origDest>
    <oUA>IMS Nortel IPCM 2.0</oUA>
    <destinationPhoneNumber>8080@lab2.org</destinationPhoneNumber>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Nortel Networks</sessionName>
      <mediaPortal>false</mediaPortal>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <origSdpPort>50078</origSdpPort>
        <origConnAddr>32.118.116.65</origConnAddr>
        <termSdpPort>50030</termSdpPort>
        <termConnAddr>32.118.116.154</termConnAddr>
        <codecList>
          <codec>0 PCMU/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 42 Connect Ingress Record, cont'd

```
</supplementaryService>  
</ipdr:UE>  
</ipdr:IPDR>
```

Figure 43 Connect Ingress Record with multiple media

```
<ipdr:IPDR seqNum="6879" time="2003-07-24T09:37:49.922Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>1972@yamaha.com</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>656142795@yamaha.com</uID>
    <corrID>656142795@32.124.12.166</corrID>
    <recTime>2003-07-24T09:37:49.143Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T09:37:36.567Z</startTime>
    <ansTime>2003-07-24T09:37:49.143Z</ansTime>
    <origDest>1962@yamaha.com</origDest>
    <oUA>IMS2.0 Nortel Networks IP RAIDer/2.0.63</oUA>
    <destinationPhoneNumber>1962@yamaha.com</destinationPhoneNumber>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>nortelnetworks</sessionName>
      <mediaPortal>false</mediaPortal>
      <phoneNo>p=+972-684-1000</phoneNo>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <origSdpPort>50038</origSdpPort>
        <origConnAddr>32.124.18.77</origConnAddr>
        <termSdpPort>50014</termSdpPort>
        <termConnAddr>32.124.18.93</termConnAddr>
        <codecList>
          <codec>0 PCMU/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 44 Connect Ingress Record with multiple media, cont'd

```
</media>
<media>
  <mediaName>video</mediaName>
  <sdpProtocol>RTP/AVP</sdpProtocol>
  <origSdpPort>50040</origSdpPort>
  <origConnAddr>32.124.18.77</origConnAddr>
  <termSdpPort>50016</termSdpPort>
  <termConnAddr>32.124.18.93</termConnAddr>
  <codecList>
    <codec>96 X-NNVC/10</codec>
  </codecList>
</media>
</supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 45 Connect Ingress Record with Authentication

```
<ipdr:IPDR seqNum="8" time="2003-07-21T12:01:36.958Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>436190b1_f685cecc37@test2_ipcmweb</uID>
    <corrID>436190b1_f685cecc37@32.124.12.139</corrID>
    <recTime>2003-07-21T12:01:36.190Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-21T12:01:18.020Z</startTime>
    <ansTime>2003-07-21T12:01:36.190Z</ansTime>
    <origDest>69047710011@lab2.org</origDest>
    <oUA>IMS Nortel IPCM 2.0</oUA>
    <destinationPhoneNumber>69047710011@lab2.org</destinationPhoneNumber>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Nortel Networks</sessionName>
      <mediaPortal>true</mediaPortal>
      <phoneNo>p=+972-684-1000</phoneNo>
      <media>
        <mediaName>audio</mediaName>
        <sdpProtocol>RTP/AVP</sdpProtocol>
        <origSdpPort>50044</origSdpPort>
        <origConnAddr>32.118.116.65</origConnAddr>
        <termSdpPort>30228</termSdpPort>
        <termConnAddr>32.124.24.66</termConnAddr>
        <codecList>
          <codec>0 PCMU/8000</codec>
        </codecList>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 46 Connect Ingress Record with Authentication, cont'd

```
    </media>
  </supplementaryService>
  <supplementaryService>
    <servType>Authentication</servType>
    <succStatus>true</succStatus>
  </supplementaryService>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 47 Connect Ingress Record with Collaboration

```
<ipdr:IPDR seqNum="121" time="2003-07-24T12:37:42.970Z">
  <ipdr:SS service="ConnectIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8082@lab2.org</subscriberID>
      <callingPSTN>9876@lab2.org</callingPSTN>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>705962703@32.124.18.97</uID>
    <corrID>705962703@32.124.12.139</corrID>
    <recTime>2003-07-24T12:37:42.961Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T12:37:36.463Z</startTime>
    <ansTime>2003-07-24T12:37:42.961Z</ansTime>
    <origDest>8081@lab2.org</origDest>
    <oUA>IMS2.0 Nortel Networks IP RAIDer/2.0.67</oUA>
    <destinationPhoneNumber>8081@lab2.org</destinationPhoneNumber>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <supplementaryService>
      <servType>SDP</servType>
      <sessionName>Collaboration</sessionName>
      <mediaPortal>false</mediaPortal>
      <media>
        <mediaName>application</mediaName>
        <sdpProtocol>udp</sdpProtocol>
        <origSdpPort>50093</origSdpPort>
        <origConnAddr>32.124.18.97</origConnAddr>
        <termSdpPort>50095</termSdpPort>
        <termConnAddr>32.124.18.93</termConnAddr>
      </media>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 48 Connect Egress Record with Sequential Ringing

```

<ipdr:IPDR seqNum="7" time="2003-07-24T11:54:34.813Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>615ef877_f6953bb6ef@test2_app2</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:34.789Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T11:54:33.547Z</startTime>
    <tUA>Nortel IMS IPCM 2.0</tUA>
    <ansTime>2003-07-24T11:54:34.789Z</ansTime>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <outpulsedDigits>8080@lab2.org:5070</outpulsedDigits>
    <supplementaryService>
      <servType>RoutingActions</servType>
      <routing>
        <routingDest>8080@lab2.org</routingDest>
        <routeBlock>
          <type>SEQ</type>
          <routes>
<route>sip:8080@lab2.org:5070;nt-im=nt-im-2.0;maddr=32.124.12.145;ntguid=La
b2Cluster1_209014</route>
          </routes>
        </routeBlock>
      </routing>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 49 Connect Egress Record with Sequential Ringing, cont'd

```
<con-  
nParty>sip:8080@lab2.org:5070;nt-im=nt-im-2.0;maddr=32.124.12.145;ntguid=La  
b2Cluster1_209014</connParty>  
  </ipdr:UE>  
</ipdr:IPDR>
```

Figure 50 Connect Egress Record with Simultaneous Ringing

```

<ipdr:IPDR seqNum="69" time="2003-07-24T12:12:52.908Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>6279bd59_f6954c68e0@test2_app2</uID>
    <corrID>2e16aa36_f6954c61ca@32.124.12.139</corrID>
    <recTime>2003-07-24T12:12:52.870Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T12:12:47.588Z</startTime>
    <tUA>IMS2.0 Networks IP Nortel RAIDer/2.0.67</tUA>
    <ansTime>2003-07-24T12:12:52.869Z</ansTime>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <outputPulsedDigits>8081@32.118.117.196:5070</outputPulsedDigits>
    <supplementaryService>
      <servType>RoutingActions</servType>
      <routing>
        <routingDest>8081@lab2.org</routingDest>
        <routeBlock>
          <type>SIM</type>
          <routes>
            <route>sip:8081@32.118.117.196:5070
;trans-
port=udp;nt-im=nt-im-2.0;ntguid=f6624ae6eb3f4ebd16eb46435f26ae52f5da89</rou
te>
            <route>sip:8081@lab2.org:5070;ntfwa
ddr=32.124.12.148:5070;nt_server_host=32.124.24.37;nt-im=nt-im-2.0;maddr=32
.124.12.148;nt_disposition=firew
all_client;ntguid=Lab2Cluster1_209015</route>
          </routes>
        </routeBlock>
      </routing>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 51 Connect Egress Record with Simultaneous Ringing, cont'd

```
</routeBlock>
</routing>
</supplementaryService>
<connParty>sip:8081@32.118.117.196:5070;transport=udp;nt-im=nt-im-2
.0;ntguid=f6624ae6eb3f4ebd16eb46435f26ae52f5da89</connParty>
</ipdr:UE>
</ipdr:IPDR>
```

Figure 52 Connect Egress Record with Redirection

```

<ipdr:IPDR seqNum="447" time="2003-07-24T14:39:50.845Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8081@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>44499f1d_f695d2dab4@test2_app1</uID>
    <corrID>224192315@32.124.12.139</corrID>
    <recTime>2003-07-24T14:39:50.706Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-24T14:39:44.006Z</startTime>
    <tUA>Nortel IMS IPCM 2.0</tUA>
    <ansTime>2003-07-24T14:39:50.706Z</ansTime>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <outpulsedDigits>8080@lab2.org:5070</outpulsedDigits>
    <supplementaryService>
      <servType>RoutingActions</servType>
      <routing>
        <routingDest>8084@lab2.org</routingDest>
        <routeBlock>
          <type>SEQ</type>
          <routes>
<route>sip:8084@lab2.org:5070;nt-im=nt-im-2.0;maddr=32.124.12.148;ntguid=La
b2Cluster1_191657</route>
          <routing>
            <routingDest>8080@lab2.org</routingDest>
            <routeBlock>
              <type>SEQ</type>

```

Figure 53 Connect Egress Record with Redirection, cont'd

```
        <route>
<route>sip:8080@lab2.org:5070;nt-im=nt-im-2.0;maddr=32.124.12.145;ntguid=La
b2Cluster1_209014</route>
        </route>
    </routeBlock>
</routing>
</routes>
</routeBlock>
</routing>
</supplementaryService>
<con-
nParty>sip:8080@lab2.org:5070;nt-im=nt-im-2.0;maddr=32.124.12.145;ntguid=La
b2Cluster1_209014</connParty>
    </ipdr:UE>
</ipdr:IPDR>
```

Figure 54 Connect Egress Record with SimRing > Redirection > SeqRing

```

<ipdr:IPDR seqNum="829" time="2003-07-22T13:38:35.725Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>norma6@nortelnetworks.com</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>Proxy</appSrvID>
      <appSrvVer>ims_2.0_build182</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>36ddefd_f68b4e2615@zpvcs104</uID>
    <corrID>2062083850@32.124.23.58</corrID>
    <recTime>2003-07-22T13:38:34.701Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-22T13:38:29.401Z</startTime>
    <tUA>Nortel IMS IPCM 2.0</tUA>
    <ansTime>2003-07-22T13:38:34.701Z</ansTime>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <outpulsedDigits>normal@nortelnetworks.com:5070</outpulsedDigits>
    <supplementaryService>
      <servType>RoutingActions</servType>
      <routing>
        <routingDest>norma3@nortelnetworks.com</routingDest>
        <routeBlock>
          <type>SIM</type>
          <routes>
            <routing>
              <routingDest>normal@nortelnetworks.com</routingDest>
              <routeBlock>
                <type>SEQ</type>
                <routes>
                  <route>sip:normal@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83410</route>
                </routes>
              </routeBlock>
            </routing>
          </routes>
        </routeBlock>
      </routing>
    </supplementaryService>
  </ipdr:UE>
</ipdr:IPDR>

```

Figure 55 Connect Egress Record with SimRing > Redirection > SeqRing, cont'd

```
        <route>sip:norma3@32.118.117.48:5065;trans-  
port=udp;nt-im=nt-im-2.0;ntguid=f66165c61e67047916eab24aa648e375285d0</route>  
e>  
    </routes>  
  </routeBlock>  
</routing>  
</supplementaryService>  
<connParty>sip:normal@nortelnet-  
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83410</conn-  
Party>  
  </ipdr:UE>  
</ipdr:IPDR>
```

Figure 56 Connect Egress Record with variation of services (Redirection, SimRing, SeqRing)

```

<ipdr:IPDR seqNum="824" time="2003-07-22T13:33:19.560Z">
  <ipdr:SS service="ConnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>norma6@nortelnetworks.com</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>Proxy</appSrvID>
      <appSrvVer>ims_2.0_build182</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>480dd052_f68b490628@zpvcs104</uID>
    <corrID>1938723354@32.124.23.58</corrID>
    <recTime>2003-07-22T13:33:18.525Z</recTime>
    <protocol>sip</protocol>
    <startTime>2003-07-22T13:33:13.717Z</startTime>
    <tUA>Nortel IMS IPCM 2.0</tUA>
    <ansTime>2003-07-22T13:33:18.525Z</ansTime>
    <aband>false</aband>
    <ansInd>true</ansInd>
    <outpulsedDigits>normal@nortelnetworks.com:5070</outpulsedDigits>
    <supplementaryService>
      <servType>RoutingActions</servType>
      <routing>
        <routingDest>norma3@nortelnetworks.com</routingDest>
        <routeBlock>
          <type>SIM</type>
          <routes>
            <routing>
              <routingDest>norma2@nortelnetworks.com</routingDest>
              <routeBlock>
                <type>SIM</type>
                <routes>
                  <route>sip:norma2@32.118.117.48:5065;trans-
port=udp;nt-im=nt-im-2.0</route>
                  <route>sip:norma2@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83411</route>

```

Figure 57 Connect Egress Record with variation of services (Redirection, SimRing, SeqRing), cont'd

```

        </routes>
      </routeBlock>
    </routing>
    <routing>
      <routingDest>norma4@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SEQ</type>
        <routes>
          <route>sip:norma4@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83413</route>
        </routes>
      </routeBlock>
    </routing>
  </routes>
</routeBlock>
<routeBlock>
  <type>SEQ</type>
  <routes>
    <routing>
      <routingDest>norma5@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SEQ</type>
        <routes>
          <route>sip:norma5@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83415</route>
        </routes>
      </routeBlock>
    </routing>
  </routes>
</routeBlock>
<routeBlock>
  <type>SEQ</type>
  <routes>
    <routing>
      <routingDest>norma1@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SIM</type>

```

Figure 58 Connect Egress Record with variation of services (Redirection, SimRing, SeqRing), cont'd

```

        </routes>
      </routeBlock>
    </routing>
    <routing>
      <routingDest>norma4@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SEQ</type>
        <routes>
          <route>sip:norma4@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83413</route>
        </routes>
      </routeBlock>
    </routing>
  </routes>
</routeBlock>
<routeBlock>
  <type>SEQ</type>
  <routes>
    <routing>
      <routingDest>norma5@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SEQ</type>
        <routes>
          <route>sip:norma5@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83415</route>
        </routes>
      </routeBlock>
    </routing>
  </routes>
</routeBlock>
<routeBlock>
  <type>SEQ</type>
  <routes>
    <routing>
      <routingDest>norma1@nortelnetworks.com</routingDest>
      <routeBlock>
        <type>SIM</type>

```

Figure 59 Connect Egress Record with variation of services (Redirection, SimRing, SeqRing), cont'd

```
        <route>
          <route>sip:normal@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83410</route>
          <route>sip:normal@32.118.117.48:5065;trans-
port=udp;nt-im=nt-im-2.0;ntguid=f66165c61e67047916eab24aa648e375285d0</route>
        </route>
      </routes>
    </routeBlock>
  </routing>
</routes>
</routeBlock>
</routing>
</supplementaryService>
<connParty>sip:normal@nortelnet-
works.com:5070;nt-im=nt-im-2.0;maddr=32.124.23.58;ntguid=ipcm_83410</conn-
nParty>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 60 Long Call Ingress Record with success

```
<ipdr:IPDR seqNum="73" time="2003-07-24T11:20:40.115Z">
  <ipdr:SS service="LongCallIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type"/>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>7ef198e6_f69510ef27@test2_ipcmweb</uID>
    <corrID>7ef198e6_f69510ef27@32.124.12.139</corrID>
    <recTime>2003-07-24T11:09:25.558Z</recTime>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 61 Long Call Egress Record with failure

```
<ipdr:IPDR seqNum="6489" time="2003-07-23T16:11:24.397Z">
  <ipdr:SS service="LongCallEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type"/>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App1</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>1c9263da_f690ff13a0@test2_app1</uID>
    <corrID>5796c601_f690ff0fac@32.124.12.139</corrID>
    <recTime>2003-07-23T16:11:23.387Z</recTime>
    <endTime>2003-07-23T16:11:23.385Z</endTime>
    <failRsn>408</failRsn>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 62 SDP Record with Hold

```
<ipdr:IPDR seqNum="9" time="2003-07-24T11:54:39.856Z">
  <ipdr:SS service="SDP">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>bab55ad_f6953bb2cc@test2_ipcmweb</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:39.548Z</recTime>
    <sessionName>Nortel Networks</sessionName>
    <mediaPortal>>false</mediaPortal>
    <media>
      <mediaName>audio</mediaName>
      <sdpProtocol>RTP/AVP</sdpProtocol>
      <origSdpPort>50078</origSdpPort>
      <origConnAddr>0.0.0.0</origConnAddr>
      <termSdpPort>50030</termSdpPort>
      <termConnAddr>0.0.0.0</termConnAddr>
      <codecList>
        <codec>0 PCMU/8000</codec>
      </codecList>
    </media>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 63 SDP Record with Retrieve

```
<ipdr:IPDR seqNum="10" time="2003-07-24T11:54:39.857Z">
  <ipdr:SS service="SDP">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>bab55ad_f6953bb2cc@test2_ipcmweb</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:39.852Z</recTime>
    <sessionName>Nortel Networks</sessionName>
    <mediaPortal>>false</mediaPortal>
    <media>
      <mediaName>audio</mediaName>
      <sdpProtocol>RTP/AVP</sdpProtocol>
      <origSdpPort>50078</origSdpPort>
      <origConnAddr>32.118.116.65</origConnAddr>
      <termSdpPort>50030</termSdpPort>
      <termConnAddr>32.118.116.154</termConnAddr>
      <codecList>
        <codec>0 PCMU/8000</codec>
      </codecList>
    </media>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 64 REFER Record

```
<ipdr:IPDR seqNum="74" time="2003-07-24T12:13:23.503Z">
  <ipdr:SS service="REFER">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8081@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>6279bd59_f6954c68e0@test2_app2</uID>
    <corrID>2e16aa36_f6954c61ca@32.124.12.139</corrID>
    <recTime>2003-07-24T12:13:23.481Z</recTime>
    <notifyArrival>2003-07-24T12:13:23.480Z</notifyArrival>
    <referBy>sip:8081@lab2.org</referBy>
    <referTo>sip:8084@lab2.org</referTo>
    <referArrival>2003-07-24T12:13:21.707Z</referArrival>
    <referStatus>2</referStatus>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 65 Disconnect Ingress Record

```
<ipdr:IPDR seqNum="11" time="2003-07-24T11:54:45.969Z">
  <ipdr:SS service="DisconnectIngress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>bab55ad_f6953bb2cc@test2_ipcmweb</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:45.960Z</recTime>
    <endTime>2003-07-24T11:54:45.960Z</endTime>
  </ipdr:UE>
</ipdr:IPDR>
```

Figure 66 Disconnect Egress Record

```
<ipdr:IPDR seqNum="12" time="2003-07-24T11:54:45.970Z">
  <ipdr:SS service="DisconnectEgress">
    <ipdr:SC xsi:type="SC-VoIP-Type">
      <subscriberID>8090@lab2.org</subscriberID>
    </ipdr:SC>
    <ipdr:SE xsi:type="SE-VoIP-Type">
      <appSrvID>App2</appSrvID>
      <appSrvVer>ims_2.0_build179</appSrvVer>
    </ipdr:SE>
  </ipdr:SS>
  <ipdr:UE xsi:type="UE-VoIP-Type">
    <uID>615ef877_f6953bb6ef@test2_app2</uID>
    <corrID>bab55ad_f6953bb2cc@32.124.12.139</corrID>
    <recTime>2003-07-24T11:54:45.964Z</recTime>
    <endTime>2003-07-24T11:54:45.964Z</endTime>
  </ipdr:UE>
</ipdr:IPDR>
```



Performance management

Functional description

Accounting performance is monitored through the System Management Console by viewing Operational Measurements (OMs) for the CAM and LAM. Refer to the *MCS 5100 System Management Console User Guide* for information on OMs and viewing OMs.



Security and Administration

How this chapter is organized

This chapter is organized as follows:

- [Security on page 127](#)
- [User administration on page 127](#)

Security

The Accounting Module is located on the private managed network, which is located behind a firewall. The Management Module manages the security functions for the Accounting Module. For additional information, refer to the *MCS 5100 Management Module Basics* and the *MCS 5100 System Management Console User Guide*.

User administration

Basic administrative tasks not defined in the other sections of this document, are detailed in the *MCS 5100 System Management Console User Guide*.

Multimedia Communication Portfolio

Multimedia Communication Server 5100

Accounting Module Basics

Copyright © 2004 Nortel Networks,

All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the MCS 5100 Accounting Module without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, and Nortel are trademarks of Nortel Networks.

*Sun Fire and Netra are trademarks of Sun Microsystems, Inc.

Publication number: NN10279-111
Product release: MCS 5100 2.0
Document version: Standard (02.02)
Date: February 2004

